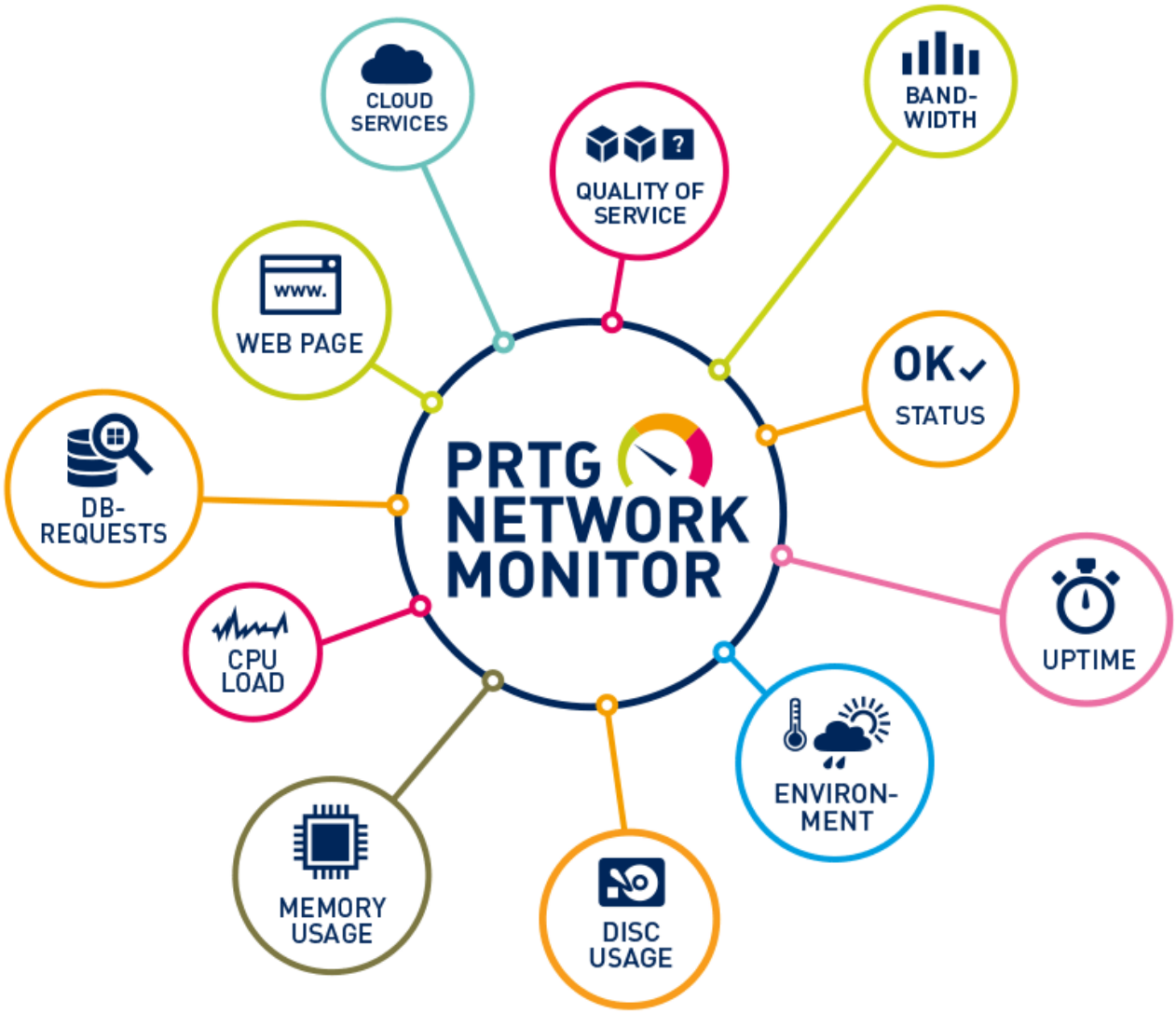
PAESSLER
THE NETWORK MONITORING COMPANY

USER MANUAL



USER MANUAL

COMPREHENSIVE IT MONITORING TO SIMPLIFY THE ADMIN'S DAILY WORK

PRTG NETWORK MONITOR

PRTG Network Monitor User Manual

© 2017 Paessler AG

All rights reserved. No parts of this work may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems—without the written permission of the publisher.

Products that are referred to in this document may be either trademarks and/or registered trademarks of the respective owners. The publisher and the author make no claim to these trademarks.

While every precaution has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. In no event shall the publisher and the author be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by this document.

Printed: June 2017 in Nuremberg

Table of Contents

Part 1 Welcome to PRTG Network Monitor 14

1 About this Document 16
2 Key Features 17
3 New in This Version 20
4 Available Licenses 21
5 System Requirements 23
Detailed System Requirements 25
6 Introduction: Monitoring with PRTG 33

Part 2 Quick Start Guide 44

1 ONE—Download, Installation, and First Login 46
2 TWO—Smart Setup 50

Part 3 Using PRTG on Demand 62

1 Create a PRTG on Demand Instance 63
2 Manage a PRTG on Demand Subscription 69

Part 4 Installing the Software 76

1 Download PRTG 77
2 Update From Previous Versions 79
3 Install a PRTG Core Server 84
4 Install a PRTG Cluster 88
5 Enter a License Key 89
6 Activate the Product 91
7 Install a PRTG Remote Probe 93
8 Install the Enterprise Console 100
9 Uninstall PRTG Products 106

Part 5 Understanding Basic Concepts 110

1 Architecture and User Interfaces 111
2 Clustering 116
3 Object Hierarchy 118
4 Inheritance of Settings 122
5 Tags 124
6 Dependencies 126
7 Scheduling 127
8 Notifying 128
9 User Access Rights 129
10 Data Reporting 132
11 IPv6 133

Part 6 Ajax Web Interface—Basic Procedures 136

1 Login 138
2 SSL Certificate Warning 142
3 Welcome Page 145
Customer Service 149
4 General Layout 151
5 Sensor States 163
6 Review Monitoring Data 166
7 Compare Sensors 172
8 Historic Data Reports 175
9 Similar Sensors 180
10 Recommended Sensors 184
11 Object Settings 188
12 Alarms 190
13 System Information 193
14 Logs 198
15 Tickets 200
16 Working with Table Lists 207
17 Object Selector 210
18 Priority and Favorites 211
19 Pause 214
20 Context Menus 215
21 Hover Popup 230
22 Main Menu Structure 231

Part 7 Ajax Web Interface—Device and Sensor Setup 248

1 Auto-Discovery 249
2 Create Objects Manually 267
Add a Group 268
Add a Device 275
Add a Sensor 288
3 Manage Device Tree 292
4 Root Group Settings 294
5 Probe Settings 312
6 Group Settings 334
7 Device Settings 360
8 Sensor Settings 384
List of Available Sensor Types 385
Active Directory Replication Errors Sensor 407
ADO SQL v2 Sensor 418
Amazon CloudWatch Alarm Sensor 433
Amazon CloudWatch EBS Sensor 443
Amazon CloudWatch EC2 Sensor 455
Amazon CloudWatch ElastiCache Sensor 467
Amazon CloudWatch ELB Sensor 479
Amazon CloudWatch RDS Sensor 491

Amazon CloudWatch SNS Sensor 504
Amazon CloudWatch SQS Sensor 516
Business Process Sensor 528
Cisco IP SLA Sensor 540
Citrix XenServer Host Sensor 550
Citrix XenServer Virtual Machine Sensor 561
Cloud HTTP Sensor 571
Cloud Ping Sensor 580
Cluster Health Sensor 589
Common SaaS Sensor 594
Core Health Sensor 602
Dell PowerVault MDi Logical Disk Sensor 609
Dell PowerVault MDi Physical Disk Sensor 618
DHCP Sensor 628
DNS Sensor 638
Docker Container Status Sensor 646
Dropbox Sensor 656
Enterprise Virtual Array Sensor 666
Event Log (Windows API) Sensor 677
Exchange Backup (Powershell) Sensor 687
Exchange Database (Powershell) Sensor 697
Exchange Database DAG (Powershell) Sensor 707
Exchange Mail Queue (Powershell) Sensor 717
Exchange Mailbox (Powershell) Sensor 727
Exchange Public Folder (Powershell) Sensor 737
EXE/Script Sensor 747
EXE/Script Advanced Sensor 759
File Sensor 770
File Content Sensor 779
Folder Sensor 789
FTP Sensor 800
FTP Server File Count Sensor 808
GitLab Build Status Sensor 818
Google Analytics Sensor 827
Google Drive Sensor 839
HTTP Sensor 848
HTTP Advanced Sensor 858
HTTP Apache ModStatus PerfStats Sensor 874
HTTP Apache ModStatus Totals Sensor 884
HTTP Content Sensor 894
HTTP Data Advanced Sensor 906
HTTP Full Web Page Sensor 918
HTTP Push Count Sensor 929
HTTP Push Data Sensor 939
HTTP Push Data Advanced Sensor 951
HTTP Transaction Sensor 962
HTTP XML/REST Value Sensor 976
Hyper-V Cluster Shared Volume Disk Free Sensor 991
Hyper-V Host Server Sensor 1001
Hyper-V Virtual Machine Sensor 1009
Hyper-V Virtual Network Adapter Sensor 1020

Hyper-V Virtual Storage Device Sensor 1031
IMAP Sensor 1040
IP on DNS Blacklist Sensor 1054
IPFIX Sensor 1063
IPFIX (Custom) Sensor 1075
IPMI System Health Sensor 1085
jFlow V5 Sensor 1095
jFlow V5 (Custom) Sensor 1107
LDAP Sensor 1118
Microsoft OneDrive Sensor 1125
Microsoft SQL v2 Sensor 1135
MySQL v2 Sensor 1151
NetApp cDOT Aggregate (SOAP) Sensor 1166
NetApp cDOT I/O (SOAP) Sensor 1176
NetApp cDOT Physical Disk (SOAP) Sensor 1187
NetApp cDOT System Health (SOAP) Sensor 1197
NetFlow V5 Sensor 1207
NetFlow V5 (Custom) Sensor 1219
NetFlow V9 Sensor 1230
NetFlow V9 (Custom) Sensor 1242
Oracle SQL v2 Sensor 1253
Oracle Tablespace Sensor 1268
Packet Sniffer Sensor 1278
Packet Sniffer (Custom) Sensor 1289
PerfCounter Custom Sensor 1299
PerfCounter IIS Application Pool Sensor 1309
Ping Sensor 1319
Ping Jitter Sensor 1328
POP3 Sensor 1337
Port Sensor 1346
Port Range Sensor 1355
PostgreSQL Sensor 1363
Probe Health Sensor 1378
Python Script Advanced Sensor 1385
QoS (Quality of Service) One Way Sensor 1395
QoS (Quality of Service) Round Trip Sensor 1403
RADIUS v2 Sensor 1413
RDP (Remote Desktop) Sensor 1422
Share Disk Free Sensor 1430
Sensor Factory Sensor 1438
sFlow Sensor 1457
sFlow (Custom) Sensor 1469
SFTP Secure File Transfer Protocol Sensor 1481
SIP Options Ping Sensor 1490
SMTP Sensor 1499
SMTP&IMAP Round Trip Sensor 1508
SMTP&POP3 Round Trip Sensor 1519
SNMP APC Hardware Sensor 1530
SNMP Buffalo TS System Health Sensor 1539
SNMP Cisco ADSL Sensor 1548
SNMP Cisco ASA VPN Connections Sensor 1556

SNMP Cisco ASA VPN Traffic Sensor 1566
SNMP Cisco ASA VPN Users Sensor 1577
SNMP Cisco CBQoS Sensor 1587
SNMP Cisco System Health Sensor 1596
SNMP Cisco UCS Blade Sensor 1605
SNMP Cisco UCS Chassis Sensor 1614
SNMP Cisco UCS Physical Disk Sensor 1623
SNMP Cisco UCS System Health Sensor 1632
SNMP CPU Load Sensor 1641
SNMP Custom Sensor 1649
SNMP Custom Advanced Sensor 1658
SNMP Custom String Sensor 1668
SNMP Custom String Lookup Sensor 1679
SNMP Custom Table Sensor 1689
SNMP Dell EqualLogic Logical Disk Sensor 1701
SNMP Dell EqualLogic Member Health Sensor 1710
SNMP Dell EqualLogic Physical Disk Sensor 1720
SNMP Dell Hardware Sensor 1729
SNMP Dell PowerEdge Physical Disk Sensor 1738
SNMP Dell PowerEdge System Health Sensor 1747
SNMP Disk Free Sensor 1757
SNMP Hardware Status Sensor 1766
SNMP HP BladeSystem Blade Sensor 1775
SNMP HP BladeSystem Enclosure System Health Sensor 1783
SNMP HP LaserJet Hardware Sensor 1791
SNMP HP ProLiant Logical Disk Sensor 1800
SNMP HP ProLiant Memory Controller Sensor 1809
SNMP HP ProLiant Network Interface Sensor 1818
SNMP HP ProLiant Physical Disk Sensor 1827
SNMP HP ProLiant System Health Sensor 1836
SNMP IBM System X Logical Disk Sensor 1845
SNMP IBM System X Physical Disk Sensor 1854
SNMP IBM System X Physical Memory Sensor 1863
SNMP IBM System X System Health Sensor 1872
SNMP interSeptor Pro Environment Sensor 1881
SNMP Juniper NS System Health Sensor 1889
SNMP LenovoEMC Physical Disk Sensor 1897
SNMP LenovoEMC System Health Sensor 1905
SNMP Library Sensor 1912
SNMP Linux Disk Free Sensor 1924
SNMP Linux Load Average Sensor 1936
SNMP Linux Meminfo Sensor 1944
SNMP Linux Physical Disk Sensor 1952
SNMP Memory Sensor 1961
SNMP NetApp Disk Free Sensor 1970
SNMP NetApp Enclosure Sensor 1979
SNMP NetApp I/O Sensor 1988
SNMP NetApp License Sensor 1997
SNMP NetApp Logical Unit Sensor 2005
SNMP NetApp Network Interface Sensor 2014
SNMP NetApp System Health Sensor 2022

SNMP Poseidon Environment Sensor 2031
SNMP Printer Sensor 2039
SNMP QNAP Logical Disk Sensor 2047
SNMP QNAP Physical Disk Sensor 2056
SNMP QNAP System Health Sensor 2065
SNMP RMON Sensor 2073
SNMP SonicWALL System Health Sensor 2083
SNMP SonicWALL VPN Traffic Sensor 2091
SNMP Synology Logical Disk Sensor 2100
SNMP Synology Physical Disk Sensor 2108
SNMP Synology System Health Sensor 2116
SNMP System Uptime Sensor 2124
SNMP Traffic Sensor 2132
SNMP Trap Receiver Sensor 2143
SNMP Windows Service Sensor 2155
SNTP Sensor 2163
SSH Disk Free Sensor 2170
SSH INodes Free Sensor 2183
SSH Load Average Sensor 2193
SSH Meminfo Sensor 2203
SSH Remote Ping Sensor 2213
SSH SAN Enclosure Sensor 2223
SSH SAN Logical Disk Sensor 2233
SSH SAN Physical Disk Sensor 2244
SSH SAN System Health Sensor 2255
SSH Script Sensor 2266
SSH Script Advanced Sensor 2278
SSL Certificate Sensor 2289
SSL Security Check Sensor 2299
Syslog Receiver Sensor 2309
System Health Sensor 2321
TFTP Sensor 2327
Traceroute Hop Count Sensor 2335
VMware Datastore (SOAP) Sensor 2344
VMware Host Hardware (WBEM) Sensor 2354
VMware Host Hardware Status (SOAP) Sensor 2362
VMware Host Performance (SOAP) Sensor 2372
VMware Virtual Machine (SOAP) Sensor 2382
Windows CPU Load Sensor 2393
Windows IIS 6.0 SMTP Received Sensor 2403
Windows IIS 6.0 SMTP Sent Sensor 2412
Windows IIS Application Sensor 2421
Windows MSMQ Queue Length Sensor 2430
Windows Network Card Sensor 2441
Windows Pagefile Sensor 2452
Windows Physical Disk I/O Sensor 2461
Windows Print Queue Sensor 2472
Windows Process Sensor 2483
Windows System Uptime Sensor 2493
Windows Updates Status (Powershell) Sensor 2502
WMI Custom Sensor 2512

WMI Custom String Sensor 2522
WMI Event Log Sensor 2533
WMI Exchange Server Sensor 2544
WMI Exchange Transport Queue Sensor 2554
WMI File Sensor 2564
WMI Free Disk Space (Multi Disk) Sensor 2573
WMI HDD Health Sensor 2585
WMI Logical Disk I/O Sensor 2596
WMI Memory Sensor 2606
WMI Microsoft SQL Server 2005 Sensor (Deprecated) 2615
WMI Microsoft SQL Server 2008 Sensor 2628
WMI Microsoft SQL Server 2012 Sensor 2640
WMI Microsoft SQL Server 2014 Sensor 2652
WMI Microsoft SQL Server 2016 Sensor 2664
WMI Remote Ping Sensor 2676
WMI Security Center Sensor 2685
WMI Service Sensor 2695
WMI Share Sensor 2705
WMI SharePoint Process Sensor 2715
WMI Terminal Services (Windows 2008+) Sensor 2724
WMI Terminal Services (Windows XP/Vista/2003) Sensor 2732
WMI UTC Time Sensor 2740
WMI Vital System Data (V2) Sensor 2748
WMI Volume Sensor 2758
WSUS Statistics Sensor 2767
9 Additional Sensor Types (Custom Sensors) 2778
10 Sensor Channels Settings 2782
11 Sensor Notifications Settings 2791

Part 8 Ajax Web Interface—Advanced Procedures 2804

1 Toplists 2806
2 Arrange Objects 2811
3 Clone Object 2812
4 Multi-Edit 2814
5 Create Device Template 2818
6 Show Dependencies 2822
7 Geo Maps 2824
8 Notifications 2829
Setting up Notifications Based on Sensor Limits: Example 2832
Setting up Notifications Based on Libraries: Example 2840
9 Libraries 2845
Libraries Step By Step 2848
Management 2852
Libraries and Node Settings 2855
Context Menus 2861
10 Reports 2862
Reports Step By Step 2866
View and Run Reports 2870
Report Settings 2873

11 Maps 2885
Maps Step By Step 2890
Map Designer 2893
Maps Settings 2902
12 Setup 2907
Account Settings—My Account 2909
Account Settings—Notifications 2916
Account Settings—Notification Contacts 2934
Account Settings—Schedules 2938
System Administration—User Interface 2943
System Administration—Monitoring 2955
System Administration—Notification Delivery 2961
System Administration—Core & Probes 2967
System Administration—User Accounts 2975
System Administration—User Groups 2982
System Administration—Administrative Tools 2987
System Administration—Cluster 2992
PRTG Status—System Status 2994
PRTG Status—Auto-Update 3005
PRTG Status—Cluster Status 3010
PRTG Status—Licensing Status and Settings 3012
Optional Downloads and Tools 3018
Desktop Notifications 3020
Support—Contact Support 3022

Part 9 Enterprise Console 3028

1 First Start 3031
2 General Layout 3033
3 Menu Tabs and Page Content 3037
Devices 3038
Libraries 3045
Sensors 3047
Alarms 3049
Maps 3051
Reports 3053
Logs 3055
Tickets 3057
Setup 3059
Search Results 3061
4 PRTG Servers 3062
5 Options 3065
6 Windows Menu Structure 3071
7 Context Menus 3079
8 Shortcuts Overview 3080

Part 10 PRTG Apps for Mobile Network Monitoring 3082

Part 11 Sensor Technologies 3086

1 Monitoring via SNMP 3087

2 Monitoring via WMI 3092
3 Monitoring via SSH 3095
4 Monitoring Bandwidth via Packet Sniffing 3097
5 Monitoring Bandwidth via Flows 3099
6 Bandwidth Monitoring Comparison 3102
7 Monitoring Quality of Service and VoIP 3104
8 Monitoring Email Round Trip 3109
9 Monitoring Backups 3111
10 Monitoring Virtual Environments 3112
11 Monitoring Databases 3120
12 Monitoring Syslogs and SNMP Traps 3125

Part 12 PRTG Administration Tool 3134

1 PRTG Administration Tool on Core Server System 3135
2 PRTG Administration Tool on Remote Probe Systems 3157

Part 13 Advanced Topics 3170

1 Active Directory Integration 3171
2 Application Programming Interface (API) Definition 3174
3 Filter Rules for xFlow, IPFIX and Packet Sniffer Sensors 3175
4 Channel Definitions for xFlow, IPFIX, and Packet Sniffer Sensors 3180
5 Define IP Ranges 3182
6 Define Lookups 3183
7 Regular Expressions 3193
8 Calculating Percentiles 3194
9 Add Remote Probe 3195
Remote Probes and Multiple Probes 3196
Remote Probe Quick Setup 3199
Remote Probe Setup Using Installer 3206
10 Failover Cluster Configuration 3212
Failover Cluster Step by Step 3219
11 Data Storage 3226
12 Using Your Own SSL Certificate with PRTG's Web Server 3228

Part 14 Appendix 3232

1 Glossary 3233
2 List of Abbreviations 3237
3 List of Icons 3242
4 Support and Troubleshooting 3243
5 Differences between PRTG on Premises and PRTG on Demand 3244
6 Legal Notices 3254

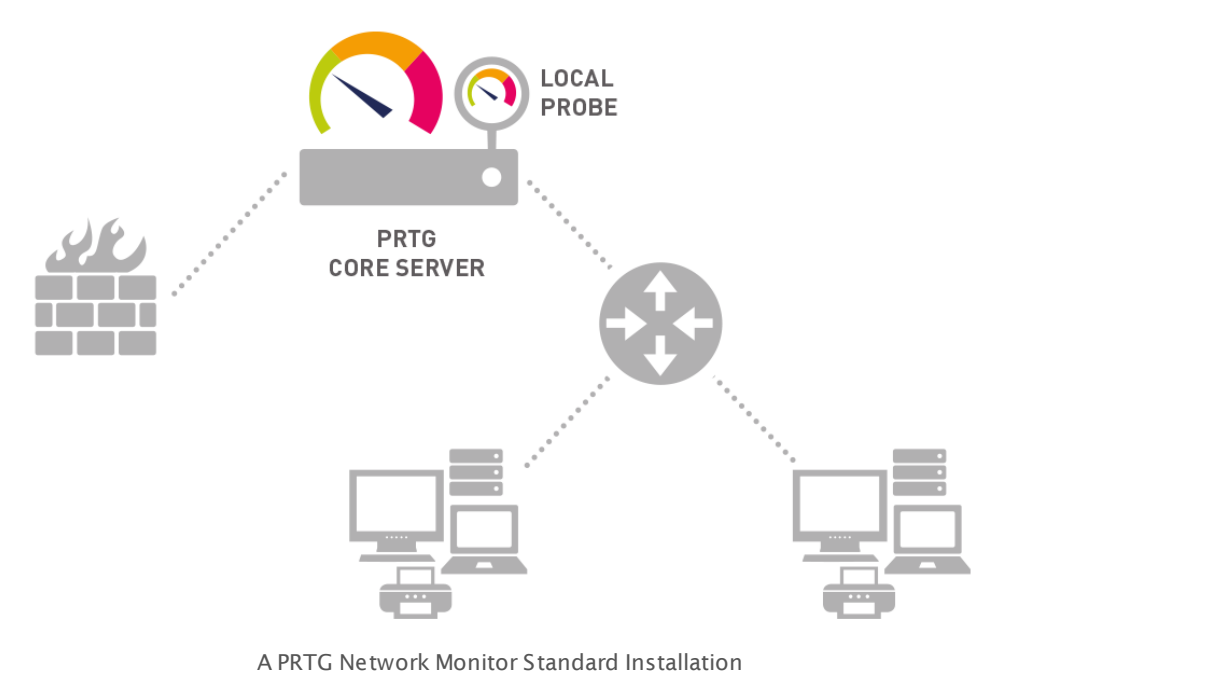
Index 0

Part 1

Welcome to PRTG Network Monitor

1 Welcome to PRTG Network Monitor

Welcome to PRTG Network Monitor! You have chosen an easy-to-use software product that comes with a powerful set of features to monitor your entire network.



A PRTG Network Monitor Standard Installation

Why Network Monitoring is Important

Today, nearly every business relies on a computer and network infrastructure for internet, internal management, telephone, and email. A complex set of servers and network equipment is required to ensure that business data flows seamlessly between employees, offices, and customers. The economic success of an organization is tightly connected to a hitch-free flow of data.

That's why your computer network has to work successfully: reliability, speed, and efficiency are crucial. But, like all other technical objects, network devices may fail from time to time—potentially causing trouble and loss of sales, no matter what migration efforts have been made up-front.

So network administrators need to take three key steps to maintain network uptime, reliability, and speed:

1. Set up a well-planned network with reliable components.
2. Create recovery plans for the event of device failure.
3. Monitor the network to get informed about failures when they build up or actually happen.

PRTG Network Monitor, the software described in this document, is a complete solution for monitoring small, medium, and large networks.

Monitoring Networks with PRTG Network Monitor

PRTG Network Monitor is a powerful network monitoring application for Windows-based systems. It is suitable for small, medium, and large networks and capable of LAN, WAN, WLAN, and VPN monitoring. You can also monitor physical or virtual web, mail, and file servers, Linux systems, Windows clients, routers, and many more. PRTG monitors network availability and bandwidth usage, as well as various other network parameters such as quality of service, memory load, and CPU usages, even on remote machines. It provides system administrators with live readings and periodical usage trends to optimize the efficiency, layout, and setup of leased lines, routers, firewalls, servers, and other network components.

The software is easy to set up and use and monitors a network using Simple Network Management Protocol (SNMP), Windows Management Instrumentation (WMI), packet sniffer, Cisco NetFlow (as well as IPFIX, sFlow, and jFlow), and many other industry standard protocols. It runs on a Windows-based machine in your network for 24 hours every day. PRTG Network Monitor constantly records the network usage parameters and the availability of network systems. The recorded data is stored in an internal database for later analysis.

BETA PRTG Network Monitor offers two options to monitor your network: PRTG on premises and PRTG on demand. With PRTG on premises, the core server and local probe run within your network. PRTG on demand is the PRTG cloud solution, where we at Paessler run the core server and local probe for you. The PRTG web interface 136 for monitoring configuration and reviewing monitoring data is the same for both, PRTG on demand and PRTG on premises.

Do you want to get an overview of PRTG in 90 seconds? See this video on our website: PRTG Network Monitor in 90 Seconds

More

Video Demo: PRTG Network Monitor in 90 Seconds

- https://www.paessler.com/support/videos/about-paessler/prtg-90-sec

Video Demo: What is Unified Monitoring?

- https://www.paessler.com/support/videos/all-about-monitoring

1.1 About this Document

This document introduces you to the system concepts of **PRTG Network Monitor** and explains how to set up the software to achieve the best monitoring results. You will learn how to plan your monitoring setup, how to set up your devices and sensors, dependencies, reports, notifications, maps, user accounts, and clustering for fail-safe monitoring.

This document is also meant to be a reference for all available settings in PRTG. Short contextual help is already provided within the Ajax web interface of PRTG. In this manual you often get some more help regarding the different options that are available. No matter whether you use PRTG on demand or PRTG on premises, you will find all of the information that you need in this document.

This document does not explain monitoring protocols and file formats in-depth. Also, the use of the Application Programming Interface (API) built into PRTG is only briefly addressed. Whenever possible, hyperlinks to more detailed resources are provided, such as articles in the **Paessler Knowledge Base**.

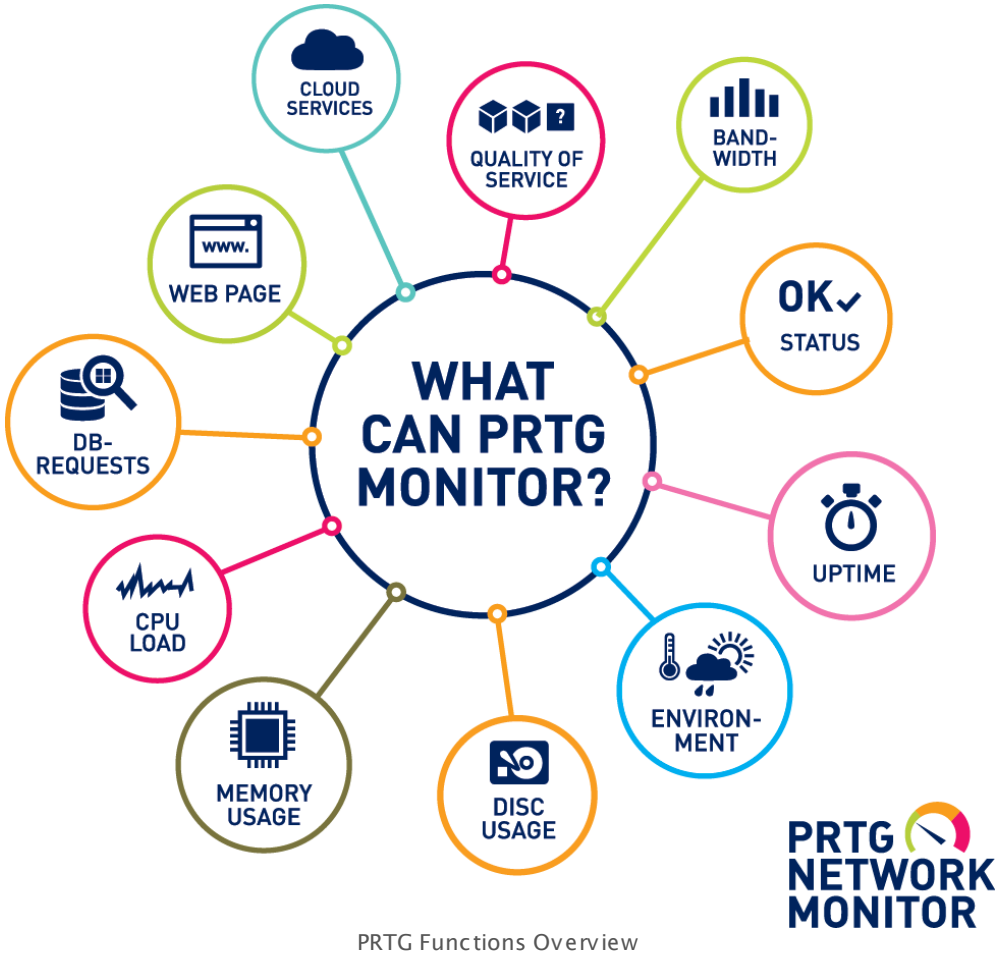
To start using PRTG right away, please see the **Quick Start Guide** 44 section. For more detailed instructions, browse the manual content and choose the section you want to read.

For an overview of the icons and abbreviations that are used in this document, please see the **Appendix** 3232 section.

1.2 Key Features

PRTG Network Monitor follows and analyzes your network and requires no third-party software. It's quick to download and install. PRTG will be up and running in a just a few minutes including a first auto-configuration. **Smart Setup** [50], the built-in interactive guidance dialog, will lead you through the whole process.

What is PRTG for?



PRTG Functions Overview

Click here to enlarge: https://media-s3.paessler.com/prtg-screenshots/PRTG-Schaubild.png

- Monitoring and alerting you to up and downtimes or slow servers
- System health monitoring of your various hardware devices
- Network device monitoring, bandwidth accounting
- Application monitoring
- Monitoring virtual servers
- Service Level Agreement (SLA) monitoring

- System usage monitoring (for example, CPU loads, free memory, free disk space)
- Database performance and table values monitoring
- Email server monitoring and reviewing various backup solutions
- Monitoring the network's physical environment
- Classifying network traffic by source or destination as well as content
- Discovering unusual, suspicious, or malicious activity with devices or users
- Measuring Quality of Service (QoS) and Voice over IP (VoIP) parameters
- Cloud monitoring services
- Discovering and evaluating network devices
- Collecting system information for various hardware types
- Finding unexpected relationships between your network components to detect potential security issues and assessing the real usage of your network and hardware
- Fail-safe monitoring using a failover cluster setup

What is Included in PRTG?

The PRTG on premises installer or a PRTG on demand instance contains everything necessary to run your monitoring system immediately without any third-party modules.

- High performance — PRTG's own fast and efficient database system stores the raw monitoring results, as well as logs, toplists, and tickets (outperforms SQL servers for monitoring data), accessible through the Application Programming Interface (API). You can distribute high loads on multiple probes.
- Low system requirements: For PRTG on premises an average PC (not older than 2 years) is sufficient and even a netbook can monitor over a thousand sensors. For detailed system requirements see here 23. PRTG on demand does not even require any hardware for the PRTG core server!
- High security standards: SSL encryption for connections and web servers, a personalized user rights management, and much more.
- A built-in SSL-secured web server with HTTP and HTTPS support for the user interface.
- Fast web interface, works as Single Page Application (SPA) to avoid time-extensive reloading of pages.
- A built-in email relay server for automatic email delivery.
- Customizable, personalized alerting
  - Various notification technologies, for example, email, push, SMS text messages, syslog and SNMP traps, HTTP requests, event logs, Amazon SNS, executing scripts.
  - Multiple triggers, for example, status alerts, limit alerts, threshold alerts, multiple condition alerts, escalation alerts.
  - Gradual dependencies to avoid alarm floods, acknowledging certain alarms to avoid further notifications for this alarm, and alert scheduling.

- In-depth report generator to create reports on-the-fly as well as scheduled reports in HTML, PDF, and as CSV or XML data files. Several report templates are available by default.
- Graphics engines for user-friendly live and historic data graphs.
- Network analysis modules to automatically discover network devices and sensors.
- Distributed monitoring to monitor several networks in different locations.
- Special features for Managed Service Provider (MSP) to monitor customer networks and increase the quality of service.
- Data publishing with real time dashboards—private and public—including live performance and status information. You can design these maps as you like with many different objects, as well as integrate external custom objects.
- Multiple languages such as English, German, Spanish, French, Portuguese, Dutch, Czech, Japanese, Russian, and Simplified Chinese.
- Customization: The PRTG Application Programming Interface (API) allows you to develop your own features. Additionally, you can create custom sensors, notifications, and device templates according to your specific requirements.

PRTG Network Monitor supports monitoring up to several thousand sensors per installation, depending on various parameters. It can optionally work with multiple remote probes to monitor multiple sites or network segments from one central core installation, and to distribute high loads. You can also configure fail-safe monitoring using a cluster installation to perform automatic failovers. Single failover installations are allowed with every PRTG license.

BETA PRTG Network Monitor offers two options to monitor your network: PRTG on premises and PRTG on demand. With PRTG on premises, the core server and local probe run within your network. PRTG on demand is the PRTG cloud solution, where we at Paessler run the core server and local probe for you. The PRTG web interface 136 for monitoring configuration and reviewing monitoring data is the same for both, PRTG on demand and PRTG on premises.

The software is based on Paessler's reliable monitoring technology that has been constantly improving since 1997. There are already more than 200,000 PRTG installations running all over the world. Our outstanding support ensures your inquiries are answered within one business day for best possible network monitoring. Attractive licensing packages from freeware (up to 100 sensors) to enterprise level (with thousands of sensors) and the free choice between PRTG on premises and PRTG on demand make sure every user finds the best-possible solution.

1.3 New in This Version

Our continuous development and rollout constantly improves and expands the functionalities provided by PRTG. Instead of delivering only a few versions each year with massive changes in every update, PRTG is automatically and seamlessly enhanced with new features and fixes—fast and with high quality.

We provide three release channels for PRTG on premises:

- **Stable**: Best tested version of PRTG for live systems; updated about once or twice a month; for use on live systems.
- **Preview**: Offering the latest features and fixes; updated several times a month; consider this version as "beta", so **do not use** this version on live systems you depend on!
- **Canary**: Providing "nightly builds"; updated very often; not tested extensively; **never use** on live systems you depend on!

Via these three channels, you can choose either maximum stability, early access to new features, or a mix of both.

For an overview of all recent changes in the current version, visit the release notes for the stable release channel on our website.

More

Paessler Website: Release Notes for the "Stable" Release Channel

- https://www.paessler.com/prtg/history/stable

Paessler Website: PRTG Network Monitor Version History

- https://www.paessler.com/prtg/history

Paessler Blog: Version 12 of PRTG will introduce "Continuous Rollout"

- https://www.paessler.com/blog/prtg-12-introduces-continuous-rollout

1.4 Available Licenses

Our licenses count by sensors. We define one sensor as one aspect that you monitor on a device.

There are three different PRTG flavors available.

Freeware Edition

The Freeware Edition is a good solution to get started with PRTG or for private use:

- Free for personal and commercial use.
- Can monitor up to 100 sensors.
- Supports all available sensor types.

If you want to use the Freeware Edition, please first install the **Trial Edition** 21 and get a free trial key. After the trial period has ended, your Trial Edition automatically turns into a Freeware Edition.

This option is not available in PRTG on demand.

Trial Edition

The Trial Edition is intended for evaluation purposes for customers who are interested in purchasing commercial licenses:

- Can monitor an unlimited number of sensors.
- Supports all available sensor types.
- For PRTG on premises you have to request the temporary license key from our website. Usually you see the license details including the key if you click the free download button on paessler.com
- The trial period of PRTG on premises is limited to 30 days and automatically reverts to Freeware Edition 21 afterwards.
- PRTG on demand provides a 10 days trial. Afterwards, your instance will be deleted if you do not purchase a commercial edition.
- Each PRTG on premises license includes one single failover cluster setup 116, consisting of two nodes. Cluster installations with two and three failover nodes will require one additional trial license key; a cluster installation with four failover nodes will require two additional trial license keys.

After the trial period has ended, a Trial Edition automatically turns into a Freeware Edition, allowing you to monitor up to 100 sensors for free.

Commercial Editions

There are several licenses of PRTG Network Monitor available to suit the demands of smaller as well as larger customers and organizations:

- Can monitor a maximum number of sensors (please consider our recommendations 27).
- Supports all available sensor types.
- Each PRTG on premises license includes one single failover cluster setup 116, consisting of two nodes. Cluster installations with two and three failover nodes will require one additional license of the same size. A cluster installation with four failover nodes will require two additional licenses of the same size.

For more information about available commercial licenses, please see the Paessler FAQs: What is the difference between the PRTG Network Monitor licenses?

More

Paessler Website: Get a Free PRTG Trial Key and Download PRTG for Evaluation

- https://www.paessler.com/prtg/trial

Paessler FAQs: What is the difference between the PRTG Network Monitor licenses?

- https://www.paessler.com/support/faqs#e1912

1.5 System Requirements

PRTG Network Monitor consists of two main system parts, the PRTG core server and one or more probes (for details, see section Architecture and User Interfaces 111). If you want to use PRTG on premises, you need to install the PRTG server on a computer that meets the System Requirements for PRTG Core Server (PRTG on Premises) 23. If you want to use PRTG on demand, you need to install at least one remote probe on a computer the meets the System Requirements for PRTG Remote Probes 23.

System Requirements for PRTG Core Server (PRTG on Premises)

To install a PRTG on premises server and work with it, you need to meet the following requirements:

- A current PC or server with at least a dual core CPU and a minimum of 2048 MB RAM memory is sufficient for the PRTG server.
- We recommend that you use the operating system Microsoft Windows Server 2012 R2 for best performance.
- A web browser to access the web interface. The following browsers are supported:
  - Google Chrome 57 or later (recommended)
  - Mozilla Firefox 52 or later
  - Microsoft Internet Explorer 11

PRTG on demand does not require any hardware for the PRTG server, but at least one remote probe installation is necessary to monitor your local network when using PRTG on demand.

System Requirements for PRTG Remote Probes

You can extend your monitoring by installing one or more Remote Probes 3196. A remote probe installation is required to monitor your local network with a PRTG on demand instance. Remote probes also allow you to monitor different sub-networks that are separated by a firewall from your PRTG on premises core server, to keep an eye on remote locations, and are useful in several other scenarios.

- **Hardware**
  A current PC or server with at least a dual core CPU and a minimum of 2048 MB RAM memory is sufficient for remote probes.
- **Operating system**
  We recommend that you use the operating system Microsoft Windows Server 2012 R2 for best performance. Microsoft Windows 7 and Microsoft Windows 10 are also good options for remote probes.
- **Stable network connection**
  Remote probes require a stable network connection between the PRTG server and the remote probe. Remote probes that connect to a PRTG on demand server need a reliable internet connection. Unstable connections, for example via 3G, might work but it is possible that you lose monitoring data if the connection is non-reliable.

Planning a PRTG on Premises Installation With Hundreds of Sensors or More?

The maximum number of sensors you can monitor with one PRTG on premises installation mainly depends on the monitoring technology and the monitoring intervals you use. In general, we recommend that you use a dedicated physical machine to run both the PRTG core server and PRTG remote probes. For more information, please see section **Detailed System Requirements** 25.

PRTG on demand is restricted to max. 5,000 sensors, more sensors are not possible. This number of sensors is available in the PRTG-5000 subscription.

More

- **Update From Previous Versions** 79

Paessler Website: System Requirements for PRTG Network Monitor—Recommended Setup for Most PRTG Users

- https://www.paessler.com/prtg/requirements

Knowledge Base: Planning Large Installations of PRTG Network Monitor

- https://kb.paessler.com/en/topic/26383

Knowledge Base: How can I speed up PRTG—especially for large installations?

- https://kb.paessler.com/en/topic/2733

Knowledge Base: Checklist for Running PRTG on VMware

- https://kb.paessler.com/en/topic/49193

Knowledge Base: Which ports does PRTG use on my system?

- https://kb.paessler.com/en/topic/61462

Knowledge Base: Which servers does PRTG connect to for Software Auto-Update, Activation, etc.?

- https://kb.paessler.com/en/topic/32513

Knowledge Base: Which .NET version does PRTG require?

- https://kb.paessler.com/en/topic/60543

PRTG on demand: Enter a New Era of Monitoring

- https://my-prtg.com

1.5.1 Detailed System Requirements

This section shows different aspects of system requirements for PRTG. Please consider these requirements to avoid issues while monitoring your network.

- Supported Operating Systems 25
- Hardware Requirements 26
- Network Size: Recommendations 27
- Running PRTG on Virtual Machines 29
- Running PRTG in a Failover Cluster 29
- Web Browser Requirements 30
- Screen Resolution 30
- Requirements for Monitored Devices 30
- Requirements for the Enterprise Console 31
- Requirements for Smartphones 31
- More 31

PRTG on demand does not require any hardware for the PRTG server, but at least one remote probe installation is necessary to monitor your local network when using PRTG on demand.

Supported Operating Systems for PRTG Server and Remote Probes

The 32-bit and 64-bit versions of the following operating systems are officially supported for PRTG **Core Service** and **Probe Service**:

- Microsoft Windows Server 2012 R2* (recommended)
- Microsoft Windows Server 2012*
- Microsoft Windows 10**
- Microsoft Windows 8.1
- Microsoft Windows 8
- Microsoft Windows 7
- Microsoft Windows Server 2008 R2*
- Microsoft Windows Server 2016*
- Microsoft Windows Server 2008 (not recommended)

* Windows servers in Core mode or Minimal Server Interface are not officially supported.

** The PRTG Enterprise Console is not fully compatible with Windows 10.

The version (32-bit or 64-bit) of the PRTG Core Server depends on the version of your operating system. The 64-bit version of the PRTG Core Server will be installed if

- the operating system is a 64-bit Windows system, and
- the system provides 6 GB RAM or more.

Otherwise the 32-bit version of the PRTG Core Server will be installed.

- For best performance of VMware sensors, EXE/Script sensors, and some other sensor types, we recommend Windows Server 2012 R2 on the computer running the PRTG probe: This is either on the local system (on every node, if on a cluster probe), or on the system running a remote probe 3196.

- For best performance of hybrid sensors using Windows Performance Counters and Windows Management Instrumentation (WMI), we recommend Windows 2008 R2 or higher on the computer running the PRTG probe: This is either on the local system (on every node, if on a cluster probe), or on the system running a remote probe 3196.

- **Microsoft .NET Framework**: We recommend that you provide Microsoft .NET Framework versions 4.0 or 4.5 (with latest updates) on all systems running a PRTG probe.

The .NET framework is imperatively needed for monitoring VMware and XenServer virtual environments.
More details: Some sensor types need the Microsoft .NET Framework to be installed on the computer running the PRTG probe. This is either on the local system (on every node, if on a cluster probe), or on the system running a remote probe 3196. Depending on the sensor type, the required versions are 4.0 or 4.5. For details, see the Knowledge Base: Which .NET version does PRTG require?

- **Disabled FIPS Mode**: Please ensure the FIPS (Federal Information Processing Standards) mode (Windows security option "System Cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing.") is disabled on Windows systems running the PRTG core or probe service. FIPS-compliant encryption may cause errors of sensors which use the .NET framework. For details, see the Knowledge Base: Why should I disable the FIPS mode under Windows?

Hardware Requirements for PRTG Server and Remote Probes

Hardware requirements for PRTG **Core Service** and **Probe Service** mainly depend on the sensor types and intervals used. The following values are provided as reference for common usage scenarios of PRTG (based on a default sensor interval of 60 seconds).

- **CPU**
  A current PC or server with at least a dual core CPU can easily monitor up to 2,000 sensors (see sensor type specific notes below). PRTG supports native x86/x64 architectures.
- **RAM memory**
  Minimum requirement: 2048 MB RAM. You need about 150 KB of RAM per sensor.
- In general, we recommend at least 1 additional CPU core and 1 GB RAM per additional 1,000 sensors.
- **Hard Disk Drive**
  You need about 200 KB of disk space per sensor per day (for sensors with 60 second interval).

- **Internet connection**
  An internet connection is required for license activation (via HTTP or email).
- **Stable network connection for remote probes**
  Remote probes require a stable network connection between the PRTG core server and the remote probe. Unstable connections, for example via 3G, might work but it could be possible that you lose monitoring data if the connection is non-reliable.

There are also non-hardware dependent limitations for some sensor types, for example, WMI and SNMP V3 sensors. These limitations can be overcome by distributing the sensors across multiple remote probes. For clusters we recommend that you stay below 2,500 sensors per cluster.

It is crucial for a properly working PRTG server to have a certain amount of hardware resources available. Because of this PRTG sends according warning and emergency messages to the primary email address of the **PRTG System Administrator** user if disk space or memory on the PRTG core server system is running out. You will get warning messages if available disk space falls below 1 GB or memory below 500 MB, and emergency messages if available disk space or memory falls below 50 MB. Please react immediately in this case and free your system resources!

Network Size: Recommendations

- Rule of thumb: Typical PRTG installations almost never run into performance issues when they stay under 2,000 sensors, under 30 remote probes, and under 30 user accounts.
- PRTG can scale much higher when the installation is planned well. Please read on if you plan to go beyond these numbers and/or if you plan elevated use of resource intensive features like reporting, xFlow sensors, or clustering.
- If you plan an installation that monitors more than 10,000 sensors from one instance of PRTG on a physical device or more than 5,000 sensors with PRTG running on a virtual machine we ask you to contact our pre-sales team for consultation.
- For your information: To monitor 5,000 sensors in a 1-minute interval, PRTG takes 7.2 million measurements and evaluates, notifies, and stores them—this adds 700 MB of additional data to the database every single day.

PRTG on demand is restricted to max. 5,000 sensors, more sensors are not possible. This number of sensors is available in the PRTG-5000 subscription.

Apart from the processing power required for the monitoring itself, several aspects can affect the number of sensors that you can use with PRTG. The following recommendations are for a PRTG single core setup (without clustering) on a physical machine. You can overcome some of these limitations if you distribute the sensors across multiple remote probes.

SIZE RECOMMENDATIONS

Operating System	We recommend that you use Windows Server 2012 R2 to run the PRTG core server and probes. This offers superior performance for monitoring, especially if you have more than 2,000 sensors.

SIZE RECOMMENDATIONS

Sensor Types	Ping 1319 and SNMP sensors 387 create much less load than complex sensors like xFlow sensors 3099, VMware sensors 391, Sensor Factory sensors 1438, WMI sensors 389, or Syslog 2309/Trap receiver 2143 sensors, for example.
Scanning Interval	We recommend that you mainly use 1-minute scanning intervals 307 for up to 2,000 sensors and 5-minute intervals if you have more sensors.
Number of Users	We recommend that you stay below 30 active user accounts 2975 for each PRTG core server. You can work well with more users if these do not all use the UI at the same time (including public dashboards).
Number of Remote Probes	Our general recommendation is to stay below 30 remote probes 3196 on one PRTG core server. PRTG still scales well up to 60 probes as long as you have less than 100 sensors per probe.
CPU Intensive Features	Try keeping the usage of the following features down: Many quickly refreshed dashboards 2885, frequent generation of huge sensor reports 2862, heavy usage of packet sniffing 3097, factory sensors 1438, and toplists 2806, frequent automatically scheduled auto-discoveries 249 for large network segments, constant queries of monitoring data via the API 3174, among others.
Network Connection Quality	The quality of your network also plays an important role. When monitoring via UDP, for example, a high packet loss rate can lead to frequent timeouts. Remote probes that connect via unstable (WAN) connections can lead to delays as well.

In general, consider the following rules for the performance impact of different sensor types:

- **SNMP V1** and **V2**, **Ping**, **Port**, and **HTTP**
  We recommend that you use these sensor types for scenarios with thousands of sensors.
- **SNMP V3**
  You can monitor about 5,000 SNMP V3 sensors with an interval of 60 seconds on a common two core computer, and about 10,000 sensors on a four core system (the main limiting factor is your CPU power).
- **WMI**
  Try to keep the number of WMI sensors per probe below 120 sensors (with 60s interval), or 600 sensors (with 300s interval).
- **xFlow (IPFIX, NetFlow, sFlow, jFlow)**
  Monitoring the maximum number of sensors depends on the traffic pattern, the number of xFlow packets per second received by the PRTG probe, as well as the performance of the probe system.

- **Packet Sniffer**
  These sensors create the highest CPU load on the probe system. This technology is only recommended for monitoring of low traffic connections (<50 Mbit/s steady stream). When traffic is often over 10 Mbit/s a dedicated remote probe should be used.
- **VMware Monitoring**
  Monitoring of VMware is limited to about 20 sensors at a 60 seconds monitoring interval, or 100 sensors at a 5 minutes interval. On probes running on Windows Server 2012 R2, you can use more VMware sensors. These limitations issue from the VMware platform. For details, see this Knowledge Base article: Increasing Maximum Connections for VMware sensors
- **Other sensor types**
  The impact of a specific sensor type on performance is indicated by a color range when adding a sensor to a device. It ranges from dark green (very low impact) to bold red (very high impact).

To overcome any limitations mentioned above you should distribute the sensors over two remote probes 3196 or more.

Running PRTG on Virtual Machines

You can run the PRTG core server as well as PRTG remote probes on virtualized platforms. However, we strongly recommend that you use a dedicated physical machine to run the PRTG core server or the PRTG remote probes 3196. There are several reasons why we recommend that you run PRTG (core server and remote probes) on real hardware, especially for thousands of sensors. Each sensor request will have to go through many virtualization layers, which costs performance and makes measurements less exact. In our experience, a physical machine simply works best for a thousand sensors and more.

Our recommendation to use real hardware is valid for the PRTG core server and for remote probes. If you must run PRTG on a virtual machine, please stay below 5,000 sensors per virtual machine and consider running several PRTG core server instances instead.

We cannot offer technical support regarding performance and stability problems for PRTG installations on virtual machines that run with more than 5,000 sensors. In this case, please migrate PRTG to one or more, preferably physical, machines.

When running PRTG on a virtual machine, do not use dynamic resource allocation, but please make sure that full resources are available to the virtual machine at any time. In our experience, dynamic resource allocation is not working efficiently for a monitoring software and can therefore lead to massive performance issues. Do not distribute CPU cores over different CPU sockets in your VM configuration. Scheduling threads does not work properly in this case, which results in performance issues.

For more details, see this Knowledge Base article: Checklist for Running PRTG on VMware

Running PRTG in a Failover Cluster

We recommend a single failover setup 116 if you need fail-safe monitoring. This consists of two PRTG core servers, each working as a cluster node.

In a PRTG failover cluster, the monitoring load doubles with each cluster node, so you will encounter half performance for each additional cluster node. In a single failover cluster, please divide our recommended numbers from above in half.

This feature is not available in PRTG on demand.

Web Browser Requirements

The following browsers are officially supported by the PRTG web interface (in order of performance and reliability):

- Google Chrome 57 or later (recommended)
- Mozilla Firefox 52 or later
- Microsoft Internet Explorer 11

For security and performance reasons, we strongly recommend that you always use the latest version of Google Chrome to access the PRTG web interface.

Firefox is potentially vulnerable for cross-site scripting (XSS) attacks. These XSS exploits are possible if you click phishing links that contain malicious code, for example, in emails, and you are currently logged in to PRTG with Firefox. For more information, see this Knowledge Base article: How secure is it to access the PRTG web interface with Firefox?

Microsoft Internet Explorer 11 and Microsoft Edge may have issues with some functionalities of the PRTG web interface.

Deprecated Internet Explorer versions as well as mobile browsers might not be able to display the full featured **Ajax web interface** 136.

Screen Resolution

A screen resolution of at least 1024x768 pixels is sufficient for most functions of PRTG. However, we recommend a screen resolution of 1200x800 or higher.

Requirements for Monitored Devices

- **SNMP monitoring**
  The monitored device(s) must be equipped with SNMP Version 1, 2c, or 3 (an SNMP-compatible software must be installed on the device). SNMP must be enabled on the device and the machine running PRTG must be granted access to the SNMP interface. For details, please see section **Monitoring via SNMP** 3087.
- **Windows/WMI monitoring**
  To use Windows Management Instrumentation (WMI) monitoring, you need a Windows network. For client PCs monitored with WMI, only the operating systems as given above 25 are officially supported, but do not use Windows 2008 for WMI monitoring (strong performance issues). For details, please see section **Monitoring via WMI** 3092.

- **xFlow (IPFIX, NetFlow, sFlow) monitoring**
  The device must be configured to send NetFlow data packets (NetFlow version 5, 9, or IPFIX) or sFlow packets (version 5) to the machine running the PRTG probe. For details, please see section **Monitoring Bandwidth via Flows** 3099.
- **Packet Sniffer monitoring**
  Only data packets passing the local machine's network card can be analyzed. Switches with so-called 'monitoring ports' are necessary for network-wide monitoring in switched networks. For details, please see section **Monitoring Bandwidth via Packet Sniffing** 3097.
- **Other sensor types**
  Depending on the specific sensor type, you can find requirements (for example, modules, components, device configurations) which may have to be fulfilled in the corresponding manual section, as well as when adding the sensor to a device.

Requirements for the Enterprise Console

The optional PRTG **Enterprise Console** 3028 (EC) runs under all supported Windows versions 25, but it is not fully compatible with Windows 10. Running the EC on Windows 10 results in several issues so please use another operating system. We will consider full Windows 10 support for future PRTG desktop clients.

PRTG on demand does not support connections from the Enterprise Console. If you want to use it, please connect the Enterprise Console to a PRTG on premises instance.

The EC has a built-in webkit browser engine and requires no specific browser installed on the system. See also **Enterprise Console—Requirements for Connections to PRTG Web Server (s)** 3029.

Requirements for Smartphones and Tablets

PRTG supports optional mobile apps for iOS and Android devices, as well as for Windows Phone. For more information and system requirements, please see section **PRTG Apps for Mobile Network Monitoring** 3082.

More

- **Update From Previous Versions** 79

Paessler Website: System Requirements for PRTG Network Monitor—Recommended Setup for Most PRTG Users

- https://www.paessler.com/prtg/requirements

Knowledge Base: How can I speed up PRTG—especially for large installations?

- https://kb.paessler.com/en/topic/2733

Knowledge Base: My WMI sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/1043

Knowledge Base: Frequent Questions about xFlow, Packet Sniffing, Traffic Monitoring and Cisco

- https://kb.paessler.com/en/topic/3733

Knowledge Base: Increasing Maximum Connections for VMware Sensors

- https://kb.paessler.com/en/topic/30643

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Knowledge Base: Checklist for Running PRTG on VMware

- https://kb.paessler.com/en/topic/49193

Knowledge Base: Which ports does PRTG use on my system?

- https://kb.paessler.com/en/topic/61462

Knowledge Base: Which .NET version does PRTG require?

- https://kb.paessler.com/en/topic/60543

Knowledge Base: How secure is it to access the PRTG web interface with Firefox?

- https://kb.paessler.com/en/topic/70192

Knowledge Base: Why should I disable the FIPS mode under Windows?

- https://kb.paessler.com/en/topic/71305

1.6 Introduction: Monitoring with PRTG

This manual section provides an overview of basic principles of PRTG Network Monitor. It shows you how you can prepare your IT infrastructure for monitoring with PRTG. Of course, you do not have to re-configure your whole network for PRTG, but there are several topics that are useful to consider before actually using PRTG.

You can immediately start monitoring without complicated configuration steps. See the **Quick Start Guide** 44 for details. If you want to know more details right from the beginning, read through the manual section below. It covers these topics:

- Overview 33
- What PRTG Does 33
- Where to Install PRTG 34
- How to Monitor 35
- What can PRTG Monitor 35
- How to Prepare 36
- What Hardware Do I Want to Monitor 36
- Types of Logins and Credentials 37
- Monitoring Technologies 38
- Notifications from PRTG 41
- Advanced Topics 42

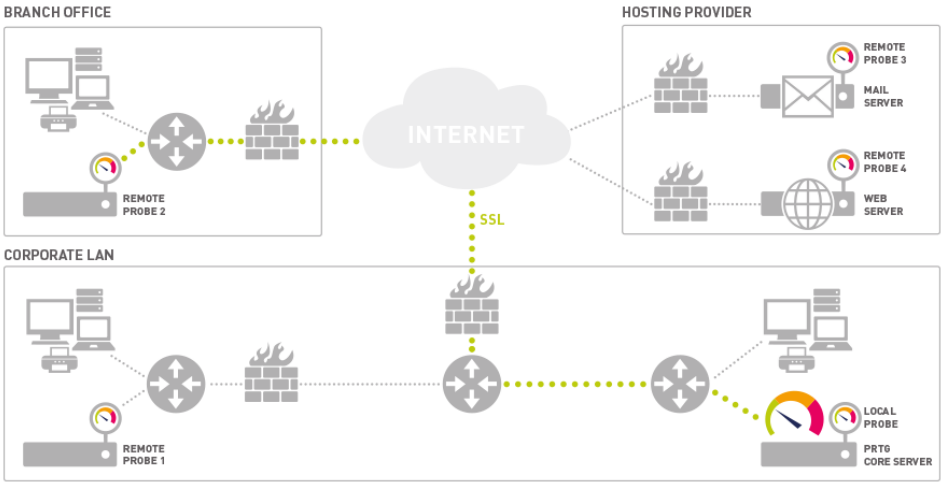
Overview

PRTG Network Monitor is a monitoring software that is flexible and easy to use. You can download, install, and configure 46 PRTG on premises or create a PRTG on demand instance 63 within minutes and start monitoring right away. That said, you will not immediately have full access to all relevant information unless your network is completely ready for monitoring—for example, PRTG needs credentials to access devices in your network. During the PRTG on premises install process, PRTG will automatically add devices with some default sensors, such as the **Ping sensor** 1319. But it will only add devices and sensors where no credentials or certain technologies are needed. For PRTG on demand you will need to install a remote probe in your LAN first.

We recommend that you run through the **Smart Setup** 50 which will ask you for most important credentials and auto-discover 249 the devices in your network.

What PRTG Does

PRTG is a Unified Monitoring Tool that allows you to monitor pretty much anything with an IP address. PRTG consists of a core server 112 which is responsible, for example, for the configuration, data management, and web server, and one or more probes 112 (local and remote 3196) which perform data collection and monitoring processes on devices 120 via sensors 120.



PRTG Architecture

Sensors are the basic building blocks of PRTG and are organized in an **Object Hierarchy** 118. A sensor can tell you about one or more aspects (referred to as channels 121) of a device or node. For example:

- Uptime
- Load
- Interface throughput
- Bandwidth usage (for example, flows)
- Loading times
- Speed
- Hardware status
- Temperature
- Quality
- Resource consumption
- User counts
- Record counts
- Log events
- Database requests

Where to Install PRTG

For best performance, we will always recommend that you install PRTG on premises on a physical machine. Any current PC or server with at least a dual core CPU and 2048 MB RAM will suffice for most average installations. PRTG can also run on a virtual machine (VM), but we have a recommended limit 29 on the number of sensors due to the hypervisor overhead.

For remote sites and for offloading work, you can use the PRTG Remote Probe 3196. Remote probes offer a smaller footprint data collector that reports back to the PRTG core server and so helps minimize performance impacts. At least one remote probe is required for PRTG on demand to monitor your local network.

PRTG on demand does not require any hardware for the PRTG server, but at least one remote probe installation is necessary to monitor your local network when using PRTG on demand.

How to Monitor

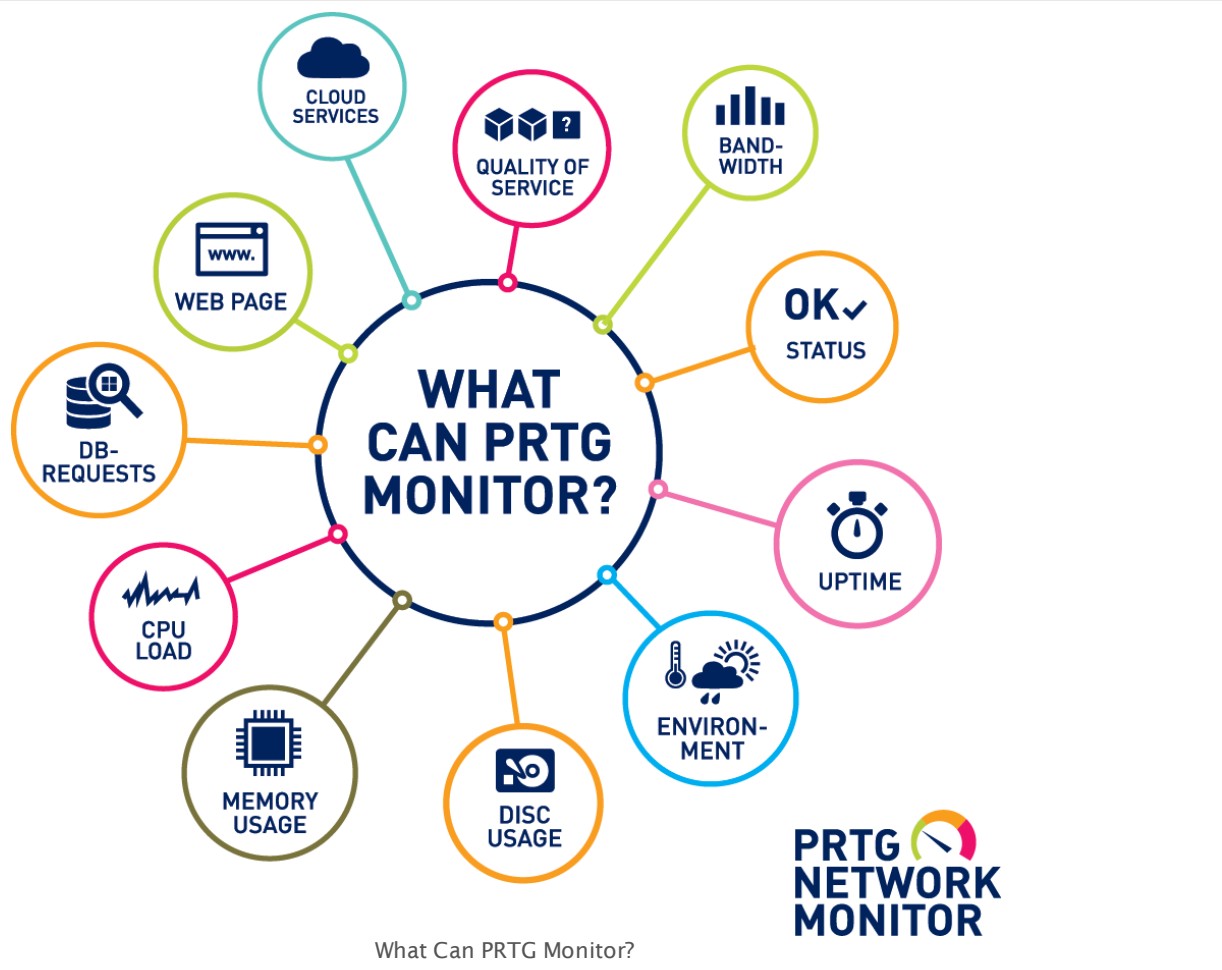
There are the following ways for PRTG to receive monitoring data from target devices:

- Polling or querying sensor data: PRTG actively obtains data from a device and refreshes it in regular intervals. This includes, for example, device status, resource usage, and performance metrics. Most sensor types use this method. PRTG can also consume and collect sensor data based on interface with, for example, HTTP(S) requests, port checks, email checks, FTP downloads, and database requests.
- Listening or receiving sensor data: PRTG passively receives data that is pushed to PRTG by a device or application. This includes, for example, unexpected events, Syslogs and SNMP traps, detailed data flow (bandwidth monitoring), and event log messages.

Most of the monitoring data that PRTG collects is actively queried. It is the basis for statistical sampling to see how a device or application is performing over time. For more information, see section **Monitoring Technologies** 38 below.

What Can PRTG Monitor

Out of the box, PRTG comes with more than 200 different sensor types 385 ranging from specific platform sensors over generic hardware and bandwidth sensors to custom scripts. Specific sensors that are pre-configured for common configurations allow you to quickly gather the information you need. Just add these sensors to the target devices they are designed for and receive monitoring data instantly. Additionally, PRTG provides the possibility to add custom sensors. For example, you can create individual sensors for devices that PRTG does not provide sensor types for out of the box, or write scripts that return data from some application.



What Can PRTG Monitor?

How to Prepare

Best practice for the first step in good monitoring is to make a plan. Think about the following questions.

1. What needs to be monitored in my IT infrastructure?
2. How can I retrieve the needed information? Which technologies and credentials are required?
3. Which notification methods do I want to use to get alerted if there is something wrong?

You can take the following sections as a basis for your monitoring planning.

What Hardware Do I Want to Monitor

When choosing what to monitor, we recommend that you add the most important devices within your infrastructure first. Start with the core network and other infrastructure that all network devices depend upon, your Business Critical Tier-1. This usually includes key infrastructure such as core routers, switches, Virtual Private Network (VPN), firewalls, and basic network services such as Dynamic Host Configuration Protocol (DHCP), Domain Name Service (DNS), and authentication like Lightweight Directory Access Protocol (LDAP).

As an example, if you are a web business, your web infrastructure is absolutely critical. You will want to add devices in order of importance to your business: file services, databases, and other systems. Usually, you would monitor devices from several perspectives, like hardware health, service availability, and performance. Please see also our video tutorial on webserver monitoring.

Hardware Overview

There is a huge number of different vendors with uncountable variations of hardware devices, so hardware details go beyond the scope of this article. Every IT infrastructure is individual, but here are the main points you should consider.

1. Core infrastructure
   a. Routers, switches, firewalls
   b. Core network services: DNS, Active Directory, LDAP servers
2. For your hardware devices, you need statistics on availability, usage, and performance.
3. PRTG will retrieve data using standard protocols:
   a. Ping, Simple Network Management Protocol (SNMP); web queries via HTTP and HTTPS; email via Post Office Protocol version 3 (POP3), Internet Message Access Protocol (IMAP), Simple Mail Transfer Protocol (SMTP)
   b. Hardware parameters via SNMP, SSH, Simple Object Access Protocol (SOAP)
   c. Bandwidth usage via xFlow (NetFlow, IPFIX, sFlow, jFlow), packet sniffing, SNMP
   d. Windows systems via Windows Management Instrumentation (WMI)
   e. Other interfaces via Secure Shell (SSH) and scripts (for example, PowerShell and Python)

PRTG will monitor, track, and chart data, as well as generate alarms.

Types of Logins and Credentials

Many of the sensors included in PRTG rely on access through logins to specific systems. You will need different credentials with sufficient permission for all the different devices, operating systems, and domains. The configuration may also be different if you want PRTG to act as a Syslog or SNMP trap receiver or for tracking flows.

In most cases, PRTG will use the following credential types to access the devices that you want to monitor.

- SNMP credentials
- Windows credentials (WMI)
- Linux, Solaris, and MacOS credentials (SSH/WBEM)
- VMware and XenServer credentials
- Database Management Systems (DBMS) credentials
- Other credentials (for example, Amazon CloudWatch keys, HTTP proxy)

Define your (administrative) credentials for all types of target devices that you want to monitor in the **Root** group of the device tree. Devices that you add to PRTG will inherit these automatically, so often you will not have to re-enter credentials, depending on the used monitoring technology.

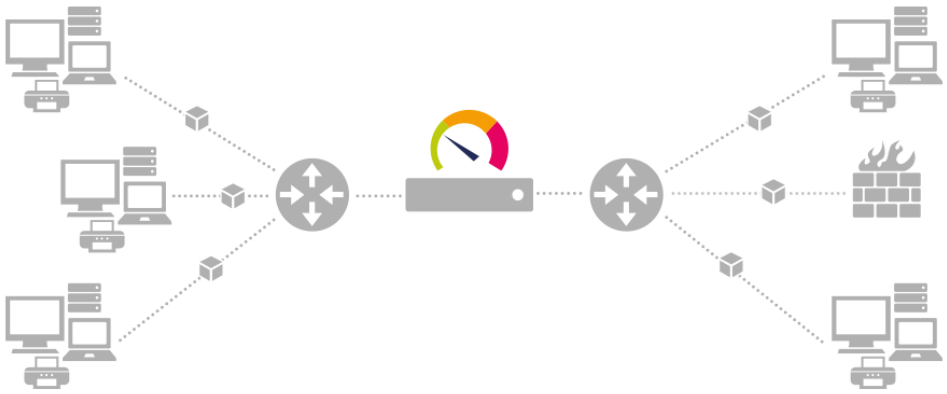
Monitoring Technologies

This section briefly describes the most common monitoring technologies. For details, please see manual section **Sensor Technologies** 3086.

Monitoring with Simple Network Management Protocol (SNMP)

SNMP is a set of standards for communication with devices in a TCP/IP network. SNMP monitoring is useful if you are responsible for servers and network devices such as hosts, routers, hubs, and switches. It enables you to keep an eye on network and bandwidth usage, and monitor important issues such as uptime and traffic levels.

You can use SNMP to monitor the bandwidth usage of routers and switches on a port-by-port basis, as well as device readings such as memory and CPU load. The target devices must support SNMP. Most devices with enabled SNMP require the same configuration like SNMP version and community string. To find out how to set up SNMP on a specific device, search in the internet for your device name or model and SNMP configuration. You will likely get plenty of information on how to configure SNMP.



Network Monitoring via SNMP

Click here to enlarge: http://media.paessler.com/prtg-screenshots/network-monitoring-via-snmp.png

When you use a sensor with this technology, PRTG sends small data packets to devices, for example, querying routers, switches, and servers for the traffic counters of each port. These queries trigger reply packets from the device. Compared to PRTG's other bandwidth monitoring technologies via flows, packet sniffing, or WMI, the SNMP option creates the least CPU and network load.

PRTG supports three versions of the SNMP protocol: Version 1, version 2c, and version 3.

SNMP Version 1

This is the oldest and most basic version of SNMP.

- Pro: Supported by most SNMP-compatible devices; simple to set up.
- Con: Limited security because it only uses a simple password (community string 3090) and sends data in clear text (unencrypted). Because of this, you should only use it inside LANs behind firewalls, but not in WANs. Version 1 only supports 32-bit counters which are not enough for high-load (gigabits/second) bandwidth monitoring.

SNMP Version 2c

This version adds 64-bit counters.

- Pro: Supports 64-bit counters to monitor bandwidth usage in networks with gigabits/second loads.
- Con: Limited security (same as with SNMP V1).

SNMP Version 3

This version adds authentication and encryption to SNMP.

- Pro: Offers user accounts and authentication for multiple users and optional data packet encryption, increasing available security; plus all advantages of Version 2c.
- Con: Difficult to configure and higher overhead for the probe, which will reduce the number of devices that you can monitor (see here 3089 for more information).

SNMP Traps

Various devices can send SNMP trap messages to notify you of system events.

- PRTG supports SNMP v1 and SNMP v2c traps.
- Destination for SNMP traps: IP address of the trap receiver, which is the IP of the PRTG probe system (server with either a local or remote probe running on it) to which you add the **SNMP Trap Receiver Sensor** 2143.

Which SNMP Version Should I Choose?

The SNMP version to choose depends on your environment, but as a guideline:

- If your network is publicly accessible, you may want to use SNMP v3, which has encryption and secure access. However security and encryption adds overhead, which results in less performance.
- If your network is isolated or well protected behind firewalls, the lower security of SNMP v1 or SNMP v2c may be sufficient.
- From the PRTG perspective, if you have a lot of devices to monitor, the SNMP v2c is preferable. It will allow you to monitor more devices on a shorter monitoring interval and supports 64-bit counters.

The most important thing is to set the same SNMP version in the PRTG settings (for example, on **Root** level) as you have configured in your target device. If you select an SNMP version that is not supported by the server or device you want to monitor, you receive an error message. Unfortunately, in most cases, these error messages do not explicitly point to the possibility that you use the incorrect SNMP version. These messages provide minimum information only, such as cannot connect or similar. Similar errors occur when community strings, usernames, or passwords do not match.

For basic requirements for SNMP monitoring, please see this Knowledge Base article: My SNMP sensors don't work. What can I do?

Monitoring Windows Systems

You can monitor Windows systems via Windows Management Instrumentation (WMI) 3092 and Windows Performance Counters 3092. WMI is the Microsoft base technology for monitoring and managing Windows based systems. PRTG uses this technology to access data of various Windows configuration parameters and status values. However, sensors using the WMI protocol generally have a high impact on system performance. In addition to strict WMI sensors, there are sensors that can use Performance Counters to monitor Windows systems.

To monitor via WMI and Performance Counters it is usually sufficient to provide **Credentials for Windows Systems** in PRTG. However, monitoring via WMI is not always trivial and often causes issues.

Please see this article in our Knowledge Base if you run into issues: My WMI sensors don't work. What can I do?

It is also possible to use Simple Network Management Protocol (SNMP) for Windows devices. The same information is often available using any of these protocols. From a performance perspective, the preference would be SNMP, and then WMI or Performance Counters.

Bandwidth and Traffic Monitoring: Flows and Packet Sniffing

Using flow protocols, you can monitor the bandwidth usage of all packets going through a device. In PRTG, you can view **Toplists** 2806 for all xFlow (NetFlow, IPFIX, sFlow, jFlow) sensors.

Flows are a type of monitoring data pushed from network devices to PRTG. You can use it to monitor where data is traveling from and to, and how much. This way it determines which machine, protocol, and user is consuming bandwidth. PRTG currently supports the following flow types:

- NetFlow v5/v9 and IPFIX: Originally introduced by Cisco and supported by several vendors
- jFlow: Traffic sampling technology introduced by Juniper networks
- sFlow: Short for sampled flow, introduced by HP. sFlow uses statistical sampling of the traffic at defined intervals to achieve scalability for high volume interfaces.

You can also use packet sniffing 3097 for bandwidth monitoring if your hardware does not support any of these flow versions.

Monitoring Passively Received Data

Another option to monitor data is to set up a device in a way that it automatically sends the data to PRTG. Specific sensor types can receive this data and alarm you based on your individual settings. Examples for this monitoring technology are HTTP push sensors 386, as well as Syslog and SNMP Trap receivers 3125.

For example, all Linux/Unix and most network devices support some form of remote Syslog or SNMP Trap server. Data from Syslog and traps is data that is generated by remote devices and has to be configured on each of the devices to send the messages to a PRTG probe system. Usually, only the destination IP and port are required. For more information, see our tutorial videos about the Syslog Receiver sensor and the SNMP Trap Receiver sensor.

Notifications from PRTG

PRTG can notify you in various ways 2921 if it detects that there is something wrong in your network. You can individually define in which case (for example, based on thresholds 2832 or on sensor states 163) and how you want to receive notifications from PRTG. The most common methods would be email 2922, SMS text message 2924, and push notifications 2923 to your smartphone which runs a PRTG mobile app 3082. For your critical infrastructure it is best practice to set up two redundant notifications with different delivery methods (for example, email and SMS via a gateway).

For more information about notifications, please see our video tutorials **PRTG – Notifications** and **Use Cases for PRTG Notifications**.

Email Notifications

The most common notification method is to send emails using a Simple Mail Transfer Protocol (SMTP) server built-in in PRTG. This means no SMTP server setup or configuration is required, but if you want to deliver through your email server, you will have to configure it in the PRTG SMTP settings 2961.

SMS Text Notifications

PRTG on premises can also notify you on your mobile phone. To deliver SMS text notifications 2964, you can select one of the SMS service providers that PRTG includes by default and use it with your credentials for this provider. Of course, you can also use any other service provider by defining a custom URL (look in your provider's documentation for the required format). You can also use an SMS gateway to receive messages even if your internet connection is down. See our Knowledge Base for a list of third-party tools.

Push Notifications

PRTG can send push notifications to iOS, Android, or Windows Phone when you run the according PRTG mobile app on your smartphone. Please see the article How can I use push notifications with PRTG? in our Knowledge Base for more details.

Advanced Topics

So, now that you are ready for monitoring with PRTG, enjoy having all important information about your IT infrastructure available at a glance. To dive deeper into network monitoring with PRTG we entrust you to have a look at our video tutorials for advanced topics. Of course, you will also find all relevant information about network monitoring in the PRTG User Manual!

More

Video Tutorials: PRTG Basics

- https://www.paessler.com/support/videos/prtg-basics

Video Tutorial: Webserver Monitoring

- https://www.paessler.com/support/videos/prtg-basics/webserver-monitoring

Video Tutorial: SNMP Trap Receiver

- https://www.paessler.com/support/videos/prtg-advanced/snmp-trap-receiver

Video Tutorial: Syslog Receiver

- https://www.paessler.com/support/videos/prtg-advanced/syslog-receiver

Video Tutorial: PRTG – Notifications

- https://www.paessler.com/support/videos/prtg-basics/notifications

Video Tutorial: Use Cases for PRTG Notifications

- https://www.paessler.com/support/videos/prtg-basics/notifications-use-cases

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Knowledge Base: My WMI sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/1043

Knowledge Base: How can I send SMS text message notifications via a modem or a mobile phone with PRTG?

- https://kb.paessler.com/en/topic/393

Knowledge Base: How can I use push notifications with PRTG?

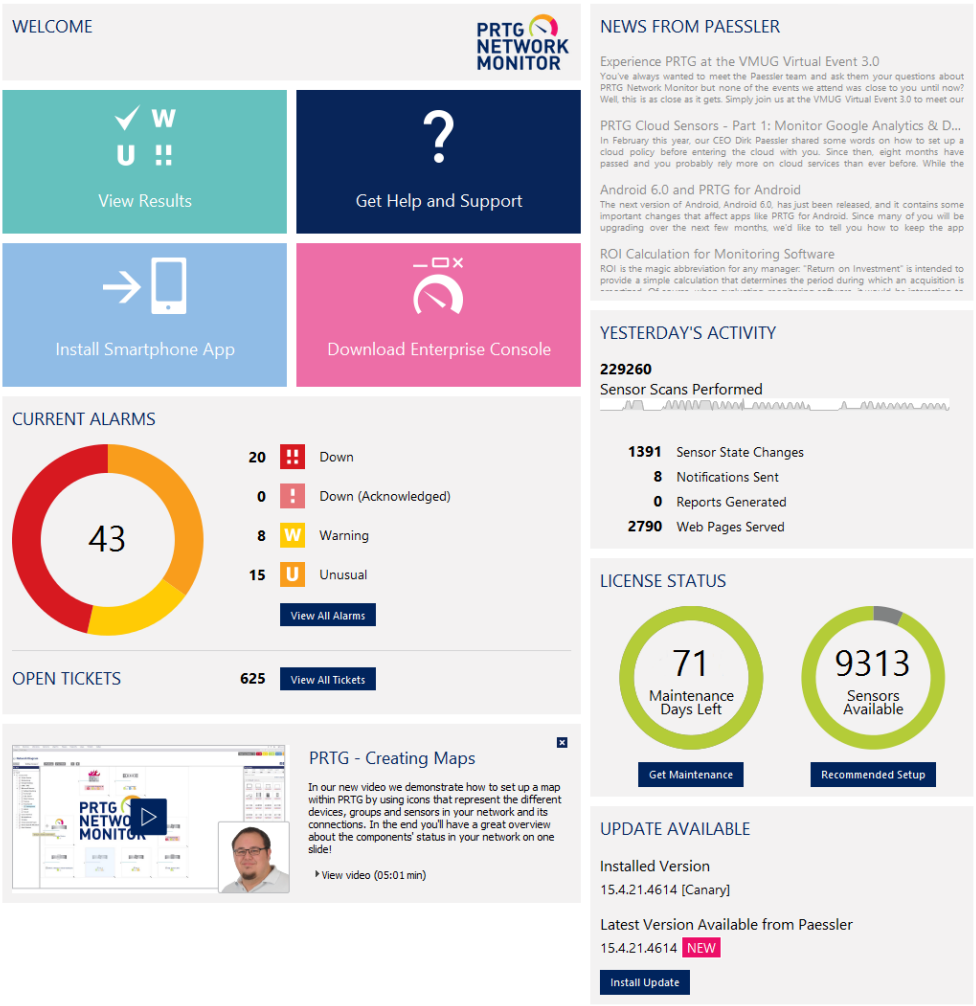
- https://kb.paessler.com/en/topic/60892

Part 2

Quick Start Guide

2 Quick Start Guide

Welcome to PRTG Network Monitor! This section gives a quick start into PRTG, so you can start monitoring your network right away!



Welcome Screen

Setting up monitoring for your network is easy! You only need to download the PRTG installer from the Paessler website and run through the installation wizard, or set up a PRTG on demand instance on https://my-prtg.com and install a remote probe in your LAN. Provide some information about your network in the **Smart Setup** 50 and PRTG will start monitoring your network immediately without any further complicated stumbling blocks! Of course, later on, you can still adjust everything to your needs.

Please see the following quick steps.

Quick Start Guide—Topics

- **ONE—Download, Installation, and First Login** 46

- TWO—Smart Setup 50

2.1 ONE—Download, Installation, and First Login

We offer two options to monitor your network with PRTG Network Monitor: use PRTG on premises to run the PRTG in your network, use PRTG on demand to run PRTG in the cloud.

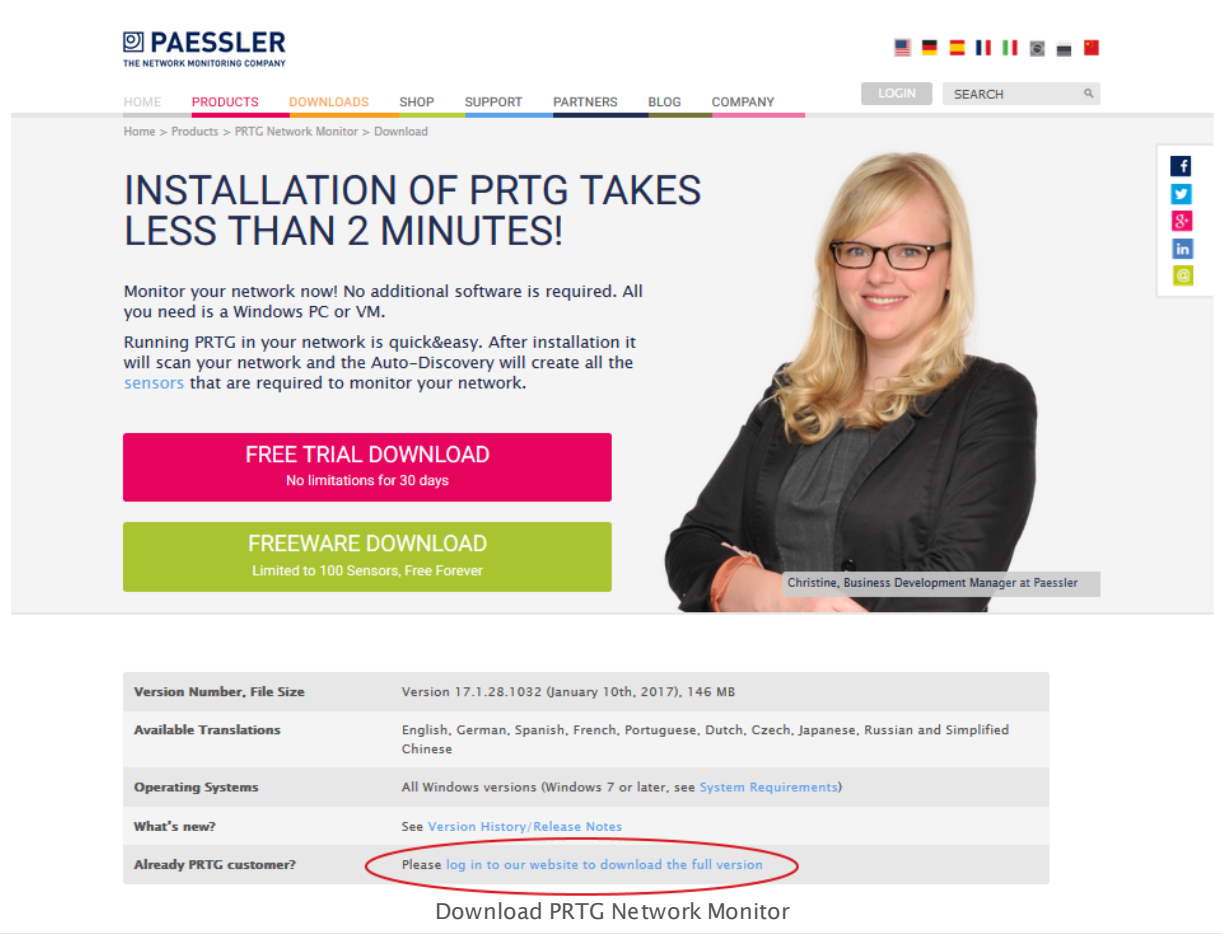
- If you want to use PRTG on premises, just download it from our website and install it on a Windows computer.
- PRTG on demand does not require a download or installation to set up the PRTG server, just create an instance on https://my-prtg.com

For video tutorials with PRTG basics, please see the video sections on paessler.com.

Download PRTG on Premises

You can find the installer for PRTG on our website https://www.paessler.com. There you can also login to the Paessler shop to buy or upgrade your license, or to renew your maintenance.

- This only applies to PRTG on premises instances, not to PRTG on demand.



Download PRTG Network Monitor

Downloading PRTG Network Monitor

Please download the latest publicly available program version from the Paessler website. Simultaneously, you will receive a trial key. Enter this license key during the installation of PRTG. If you have already purchased a commercial license, use your commercial key. Please log in to the Paessler website to find your license key,

- **https://www.paessler.com/prtg/download**
- **https://shop.paessler.com/accounts/login/**

Every freeware installation starts as a trial version that allows you to use an unlimited number of sensors for 30 days. After the trial period has expired, your installation automatically reverts to the freeware edition with 100 sensors. Please understand that customers with a commercial license get prioritized support.

To upgrade your running trial or freeware version to a commercial edition, please purchase a commercial license key on https://shop.paessler.com and enter this key on the license page 3012 in the PRTG web interface.

Updates are free to customers with an active maintenance contract. If you do not have an active maintenance contract, please log in to the Paessler shop to renew it or contact sales@paessler.com.

Once installed, the PRTG **Software Auto-Update** 3005 will automatically download and install new software versions. This helps you keep PRTG up to date without manually installing new PRTG versions.

Install PRTG on Premises

Double-click the setup file on the computer that you want to use as PRTG server. Follow the installation wizard and install the software.

This only applies to PRTG on premises instances, not to PRTG on demand.

At the end of the installation, PRTG opens a new browser window automatically. It connects to the PRTG web interface, shows the device tree 151, and starts the setup assistant 50. Please make sure you load the web interface with one of the supported browsers:

- Google Chrome 57 or later (recommended),
- Mozilla Firefox 52 or later, or
- Microsoft Internet Explorer 11.

We recommend that you use Google Chrome to access the PRTG web interface. Firefox has security issues and Internet Explorer as well as Microsoft Edge might have issues with some functionalities. See **Detailed System Requirements** 30 for more details.

Due to scripting incompatibilities, you might not be able to use all functionalities of the PRTG Ajax web interface with Internet Explorer 10 or earlier and other older browsers. If you cannot access the PRTG web interface, please open the URL of PRTG in another browser.

Create a PRTG on Demand Instance

PRTG on demand runs in the cloud, so setting up the PRTG server does not require a download or installation.

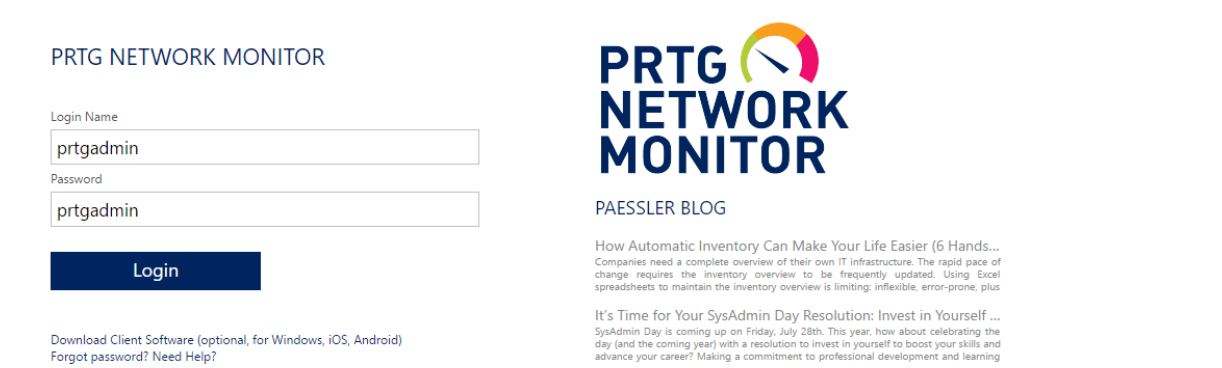
- Open https://my-prtg.com with a browser.
- You can directly start a free trial from there: enter your desired domain name (between 4 and 60 characters) and click **Start Free Trial Now**. You can reach your PRTG on demand instance with your browser under <yourdomain>.my-prtg.com later.
- A window where you have to sign in will appear. You can directly sign in using your Google, Facebook, Windows, or Amazon account (via Auth0). In this case, click the desired service and sign in with your credentials. Alternatively, you can register at my-prtg.com using dedicated credentials.
- After signing in, choose your subscription plan, for example, you can start with a free trial for 10 days. Click **Subscribe Now** and PRTG will create an instance for you.

As soon as your instance is ready, the PRTG web interface will open, show the device tree, and start the smart setup 50. You can also instantly monitor all servers, services, and devices that are publicly available via the internet.

Please make sure you load the web interface with one of the supported browsers 30. We recommend that you always use the latest version of Google Chrome.

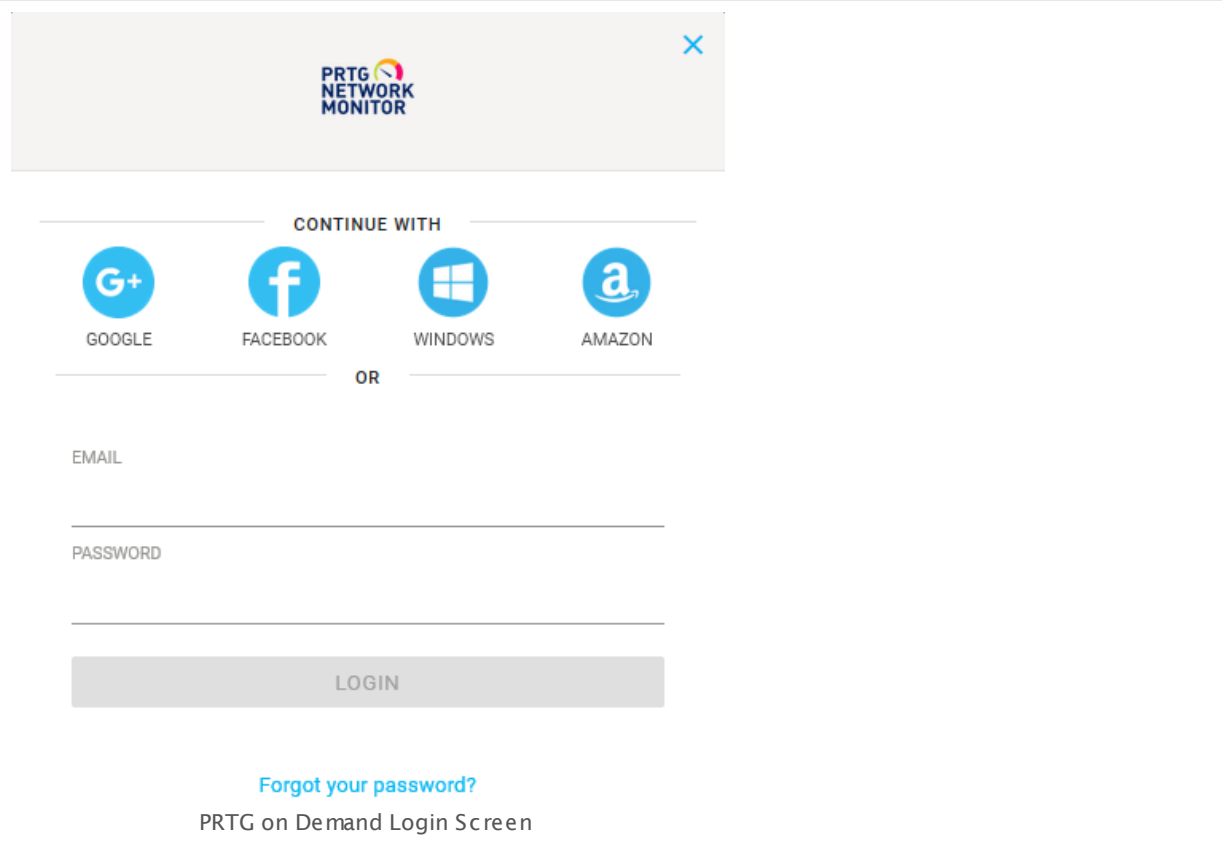
Login

If everything works fine, the first thing you will see will not be the login screen, but the device tree. You only have to log in manually if you use a different browser.



PRTG on Premises Login Screen

- The default administrator credentials (login name **prtgadmin** and password **prtgadmin**) are automatically filled in. Click **Login** to proceed if you use PRTG on premises.



PRTG on Demand Login Screen

- If you use PRTG on demand, click one of the social login buttons and log in with the according credentials using Auth0, or enter your dedicated my-prtg.com credentials and click **Login**. See section Create a PRTG on Demand Instance 63 for more information on how to get started with PRTG on demand.

Make sure you use a supported web browser when logging in to PRTG. Please use Google Chrome 57 or later (recommended), Mozilla Firefox 52 or later, or Microsoft Internet Explorer 11.

Please see the next step for more information about the initial configuration of PRTG using the Smart Setup 50!

More

Video tutorials for PRTG Network Monitor:

- https://www.paessler.com/support/videos

2.2 TWO—Smart Setup

PRTG will automatically start the **Smart Setup** on a new PRTG instance. This setup assistant, represented by some members of the Paessler team, will guide you through the initial setup of your network monitoring system. The Smart Setup will reappear until you have completed all steps. You can skip the introduction altogether right at the beginning.

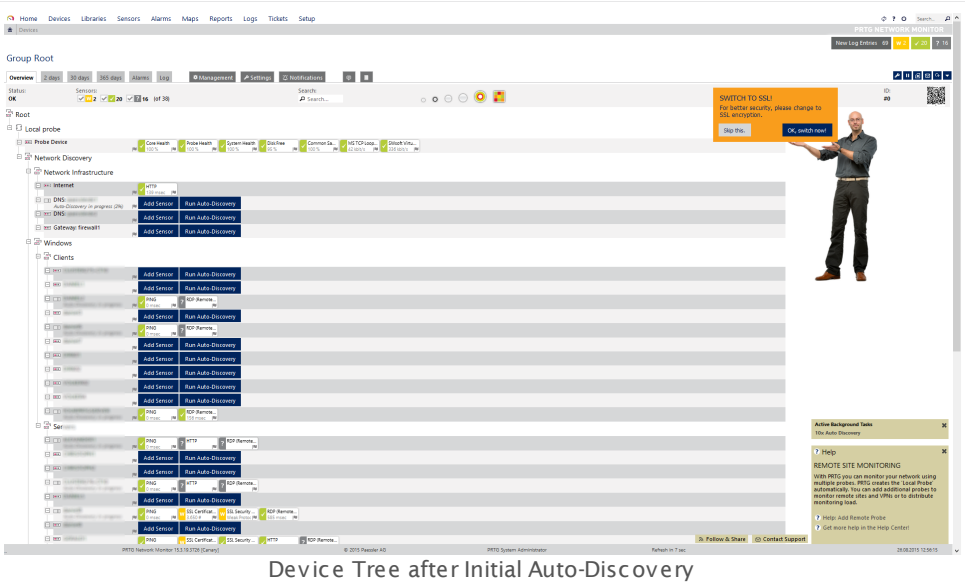
The Smart Setup in PRTG on demand differs in some details from the Smart Setup in PRTG on premises. For example, it will ask you right at the beginning to install a remote probe 93 in your local network. This is required to monitor your LAN, so we strongly recommend that you follow the smart setup!

First Start

When logging in for the first time, PRTG will show you the device tree 151. PRTG on premises already contains several devices 120 with sensors 120 that monitor your network, ordered in different suitable groups 119. PRTG automatically creates the device tree during the installation process by using its **Auto-Discovery** 249 function. You do not have to fill out any forms but will directly see the availability and first monitoring results of various devices in your network when you first start PRTG!

PRTG scans your network by pinging IP addresses in the subnet of your PRTG system and adds all reachable devices to your specific network monitoring structure.

The smart setup scans only for devices with IP addresses in private network ranges. You can manually start an Auto-Discovery for other subnets later.

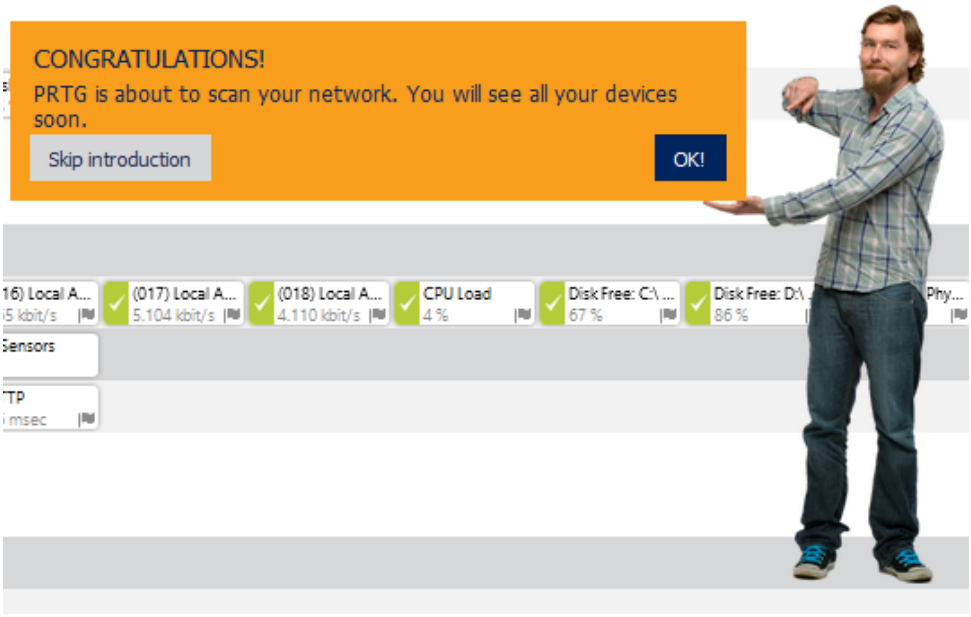


Device Tree after Initial Auto-Discovery

You will notice a Paessler employee in the upper-right corner of the PRTG web interface. He will guide you through 5 simple setup steps where you can enter more information about your network. PRTG will run another auto-discovery with this information to add additional devices and sensors to your monitoring. Of course, you can still edit the monitoring settings provided during the Smart Setup later on. And you can always adjust the monitoring to your needs.

Click **OK!** to start a guided tour, follow the instructions, and discover your network with PRTG!

If you choose **Skip introduction** now, then the Smart Setup assistant will never appear again! We strongly recommend that you take the guided tour if you are new to PRTG.



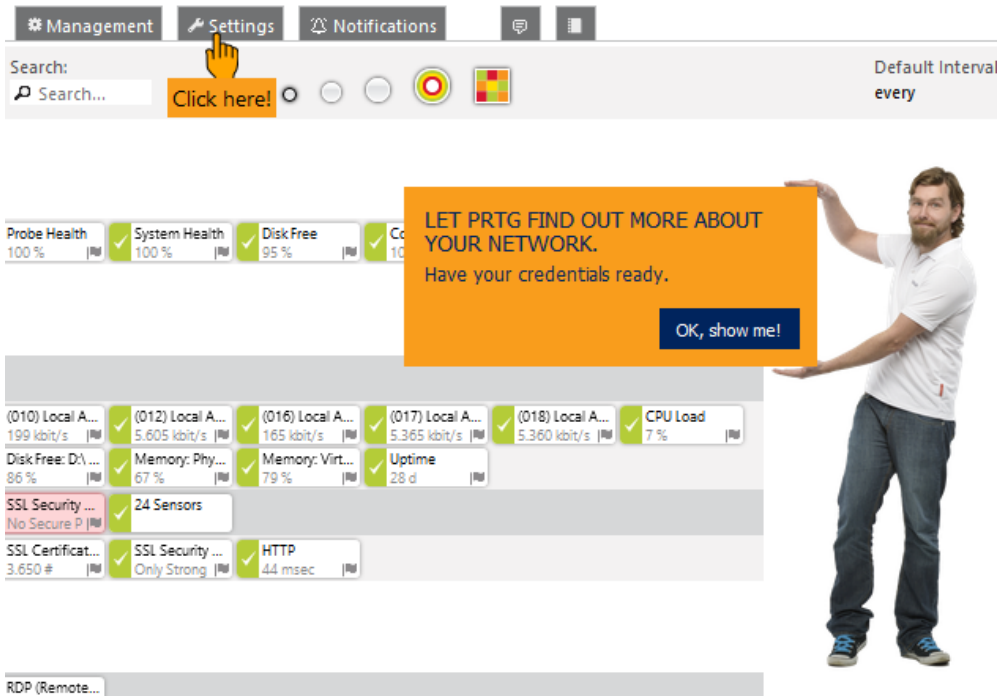
Start Your Introduction to PRTG

The steps to take are:

- Provide Credentials 51
- Enter Location Information 54
- Change Your PRTG Login Password 55
- Confirm Your Email Address 57
- Switch to SSL 58 (if you access PRTG from another computer)

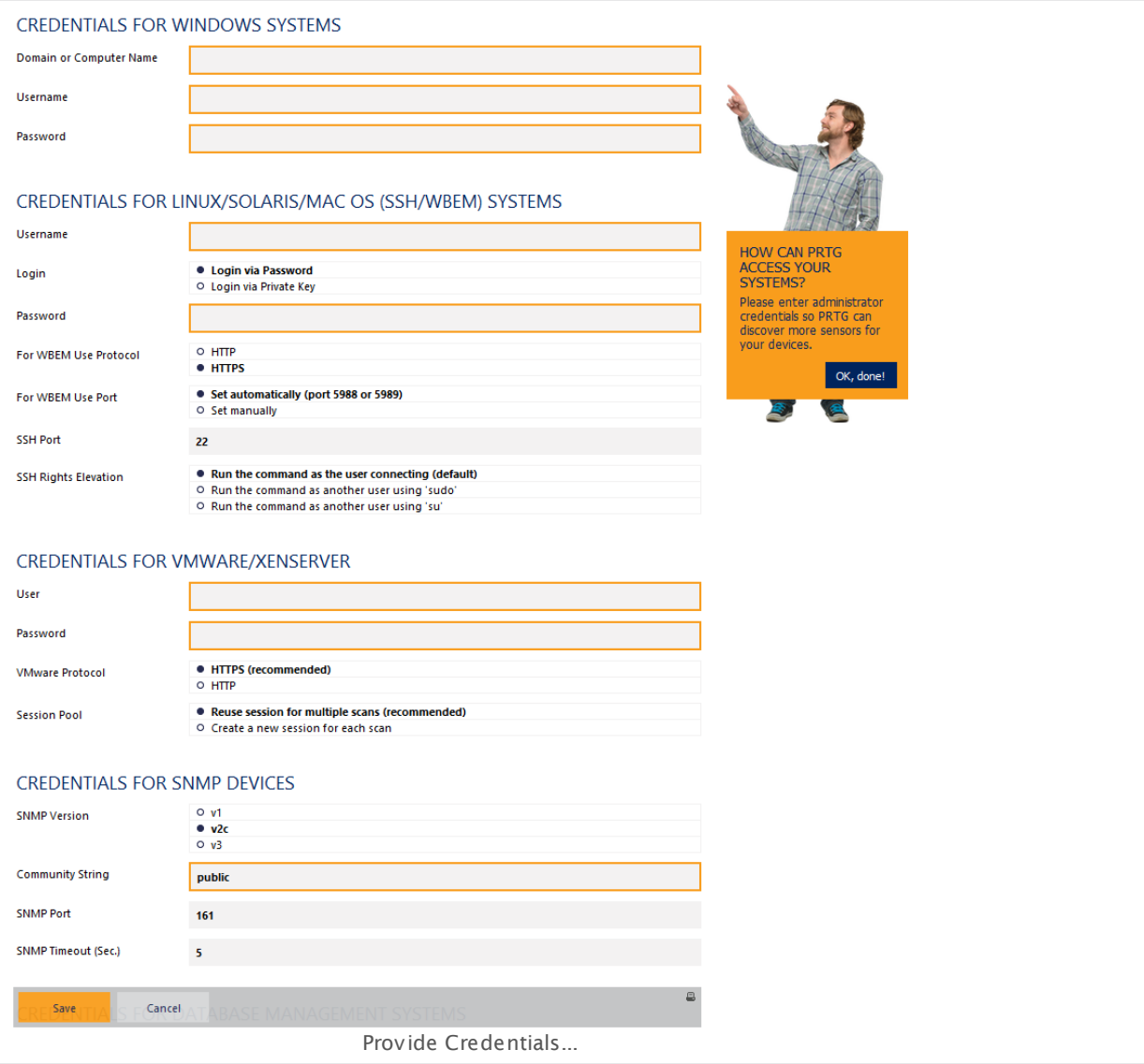
Step 1: Provide Credentials

Your personal setup assistant Greg asks you to provide credentials for devices in your network. Click **OK, show me!**, follow the animated yellow mouse pointer, and open the **Settings** tab of the **Root** group.



Have Your Credentials Ready

In the **Settings** tab, enter various administrator credentials for your network environment. With these credentials, PRTG can add a large number of additional devices and sensors automatically to your device tree. This way, PRTG helps you to set up your network monitoring so there is no need for you to manually add every single device one by one.

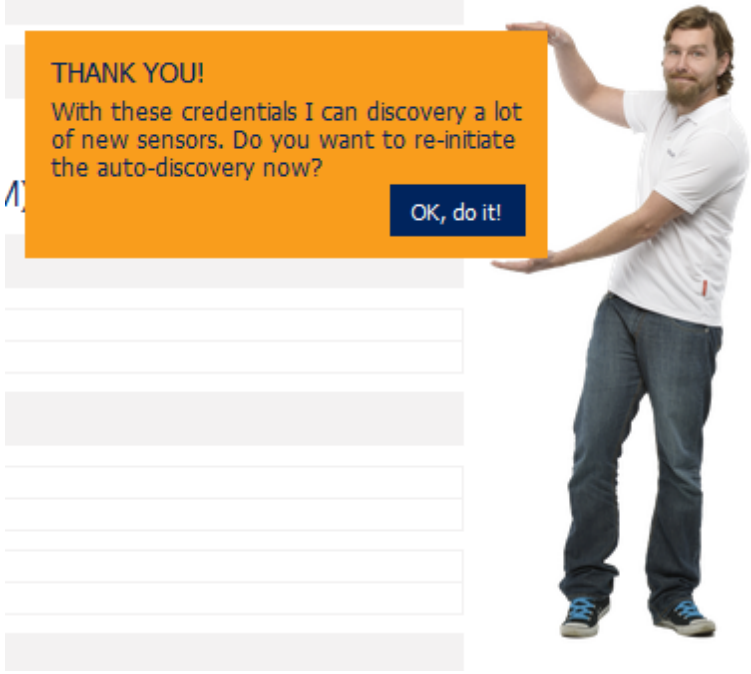


Provide Credentials...

- To monitor your Windows clients and servers via Windows Management Instrumentation (WMI), enter Windows administrator credentials for your network. We recommend that you use Domain Administrator credentials (if you use an Active Directory). For a general introduction to the technology behind WMI, see the manual section **Monitoring via WMI** 3092.
- If you have systems running on Linux, Solaris, or Mac OS X, enter root access credentials for these systems. For a general introduction to SSH monitoring, see the manual section **Monitoring via SSH** 3095.
- If you use the virtual environments VMware or Citrix XenServer, enter root access credentials for these systems. For a general introduction to the monitoring of virtual environments, see the manual section **Monitoring Virtual Environments** 3112.
- To monitor your hardware (router, switches, etc.), Simple Network Management Protocol (SNMP) is the most common protocol used. Usually, all SNMP-enabled devices use the same settings by default: SNMP v2c, community string public, SNMP port 161). For a general introduction to the technology behind SNMP, see the manual section **Monitoring via SNMP** 3087.

PRTG will store these credentials in the **Root** 294 group of your device tree. All dependent devices automatically inherit and use them for monitoring. You can discontinue **Inheritance of Settings** 122 at any level if you enter other credentials instead.

Click **OK, done!** to finish this setup step and confirm to start a detailed auto-discovery with the **OK, do it!** button.

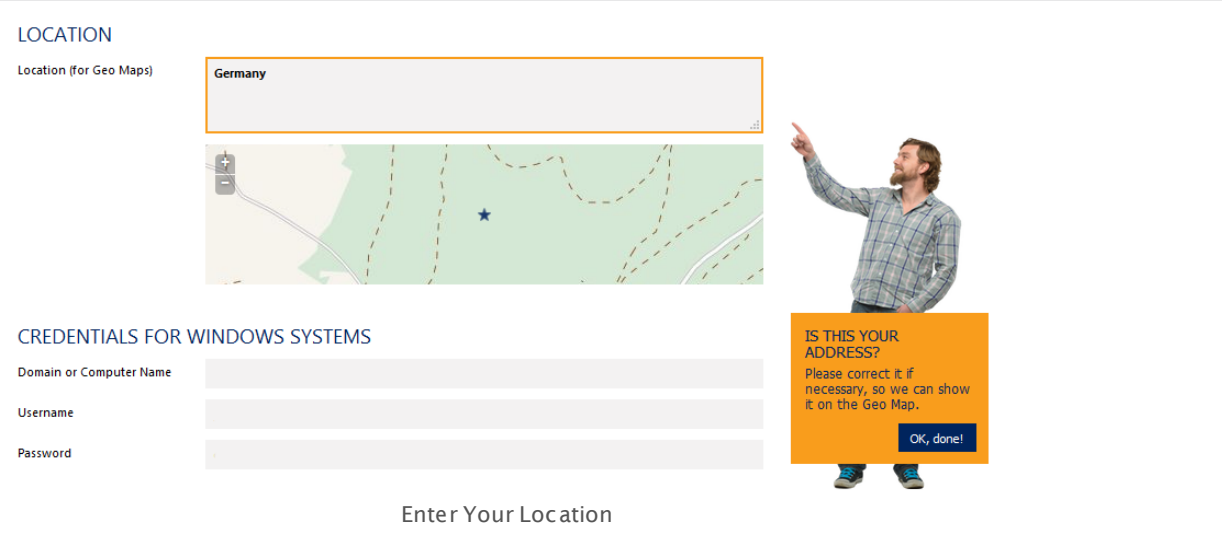


...and Start a Detailed Auto-Discovery

For details about the available options, please see the manual section **Root Group Settings** 295.

Step 2: Enter Location Information

While PRTG runs a new auto-discovery in your network with the provided credentials, the setup assistant asks you to provide the location of your PRTG server. This information will be displayed on PRTG **Geo Maps** 2824. Enter your location and confirm with **OK, done!**. Click **OK, show me!** to get back to the device tree.



Enter Your Location

For details about the available options, please see the manual section Root Group Settings 294.

Step 3: Change Your PRTG Login Password

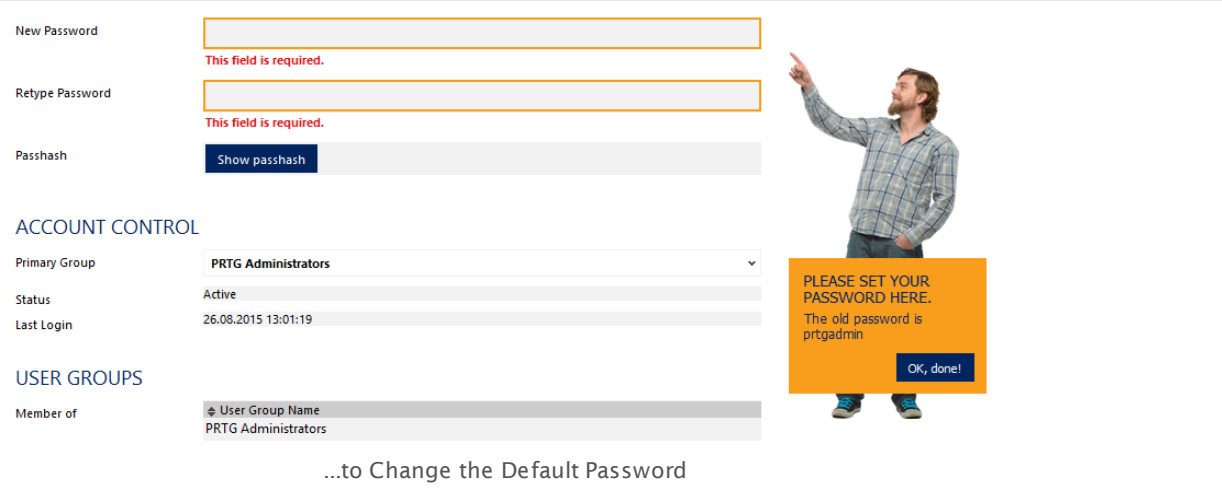
Back on the device tree, the PRTG on premises setup assistant asks you to change your password. Click **OK, show me!**, follow the assistant to your account settings. By default, PRTG uses the administrator account with login name **prtgadmin** and password **prtgadmin.** So we strongly recommend that you change the password to secure your PRTG installation against unauthorized access.

Follow the Assistant...

Enter your **New Password**, confirm it with **Retype Password**. The password must meet the following requirements:

- at least eight characters long
- at least one numeral
- at least one capitalized letter

Click **OK, done!** to save your new password.



...to Change the Default Password

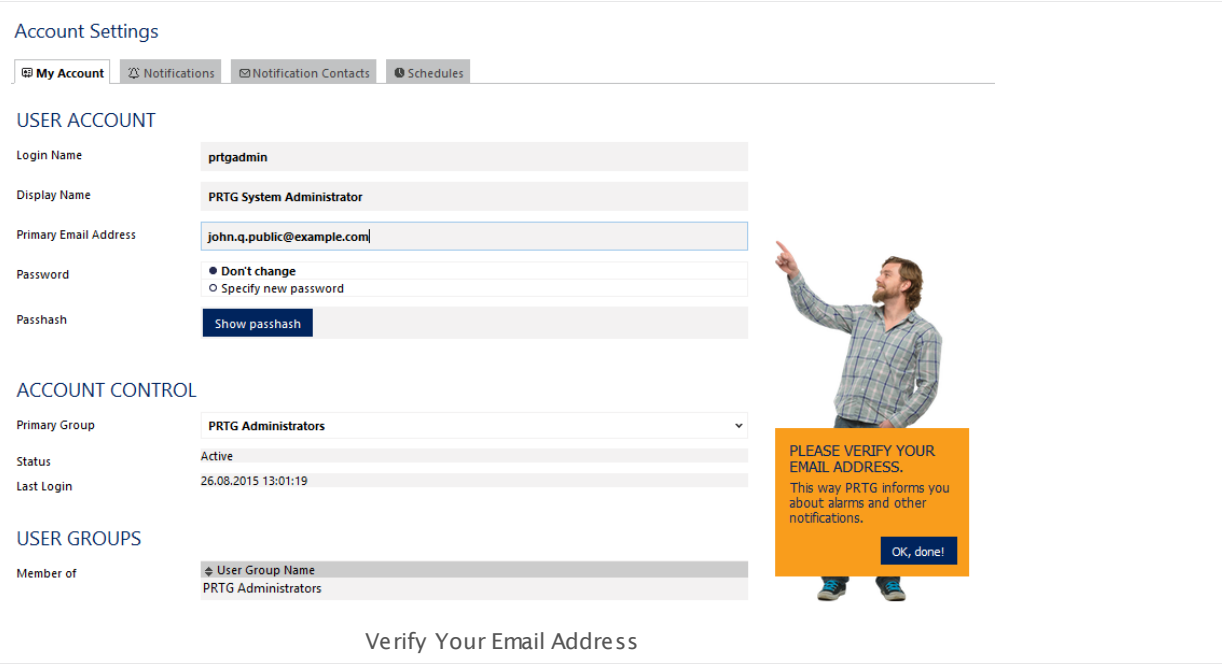
For details about the available options, please see the manual section [Account Settings—My Account](2909).

Step 4: Confirm Your Email Address

To complete the PRTG Smart Setup, check whether the email address that you have entered during the installation is correct.

A working email address is absolutely mandatory for PRTG to reach you via email notifications, alarms, and for other important messages.

If the address is correct, click **OK, done!** and follow the assistant back to the device tree.



Verify Your Email Address

For details about the available options, see the manual section **Account Settings—My Account** 2909.

Step 5: Switch to SSL

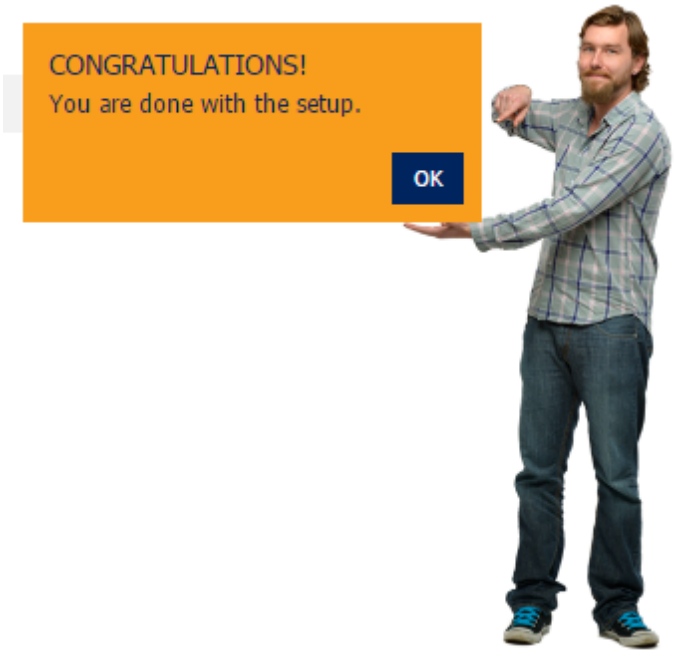
If you access the PRTG on premises web interface from a computer other than the computer where you installed PRTG, the assistant will appear and ask you to switch to a secure connection with Secure Sockets Layer (SSL)/Transport Layer Security (TLS) encryption. We strongly recommend that you run the PRTG web interface using SSL encryption (Hypertext Transfer Protocol Secure (HTTPS)), especially if you make your web interface available from the internet. Without encryption your passwords are sent unencrypted over your network.

- Click **OK, switch now!** to get more information about using SSL for the PRTG web server.
- In the new window, click the button **Yes, switch to SSL now** to switch to an SSL-encrypted connection.
- PRTG must restart its services to apply the changes and is reachable under an https URL afterwards.
- When the web interface reloads, most likely it will show a certificate warning 142. Confirm it to proceed to the login screen.

Switch to a Secure SSL Connection

For more details, see the manual sections **System Administration—User Interface** 2946 and **SSL Certificate Warning** 142.

You Are Done!



You are done with the Smart Setup!

While you were busy with the Smart Setup, PRTG created additional devices and sensors for you. There are first monitoring values available, too. Now you are all-in in your personal unified network monitoring! In the meantime, you can follow PRTG on Facebook, Twitter, and Google+. Just click the **Follow & Share** button on the page footer and connect to your new favorite monitoring tool!

To become familiar with the PRTG web interface, we recommend that you read on in the manual section **General Layout** 151 of the web interface.

More

Video Tutorial: PRTG Installation and Smart Setup

- https://www.paessler.com/support/videos/prtg-basics/installation_of_prtg_network_monitor

Part 3

Using PRTG on Demand

3 Using PRTG on Demand

BETA PRTG Network Monitor offers two options to monitor your network: PRTG on premises and PRTG on demand. With PRTG on premises, the core server and local probe run within your network. PRTG on demand is the PRTG cloud solution, where we at Paessler run the core server and local probe for you. The PRTG web interface 136 for monitoring configuration and reviewing monitoring data is the same for both, PRTG on demand and PRTG on premises.

The following sections show you how to **Create a PRTG on demand Instance** 63 and how to **Manage a PRTG on demand Subscription** 69.

See the Paessler website for **PRTG on Demand – Service Description** and **FAQ – PRTG on Demand**.

More

Paessler Website: PRTG on Demand – Service Description

- https://www.paessler.com/prtg/prtg-on-demand-service-description

Paessler Website: FAQ – PRTG on Demand

- https://www.paessler.com/support/faqs/faq-prtg-on-demand

PRTG Manual:

- **Differences between PRTG on Premises and PRTG on Demand** 3244

Using PRTG on Demand—Topics

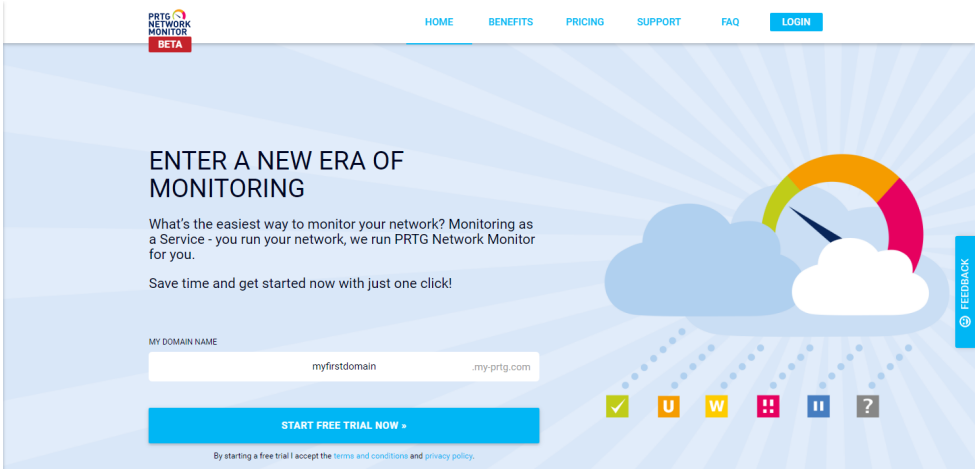
- **Create a PRTG on Demand Instance** 63
- **Manage a PRTG on Demand Subscription** 69

3.1 Create a PRTG on Demand Instance

BETA To create a PRTG on demand instance, open your web browser and go to https://my-prtg.com. This is the PRTG on demand web portal.

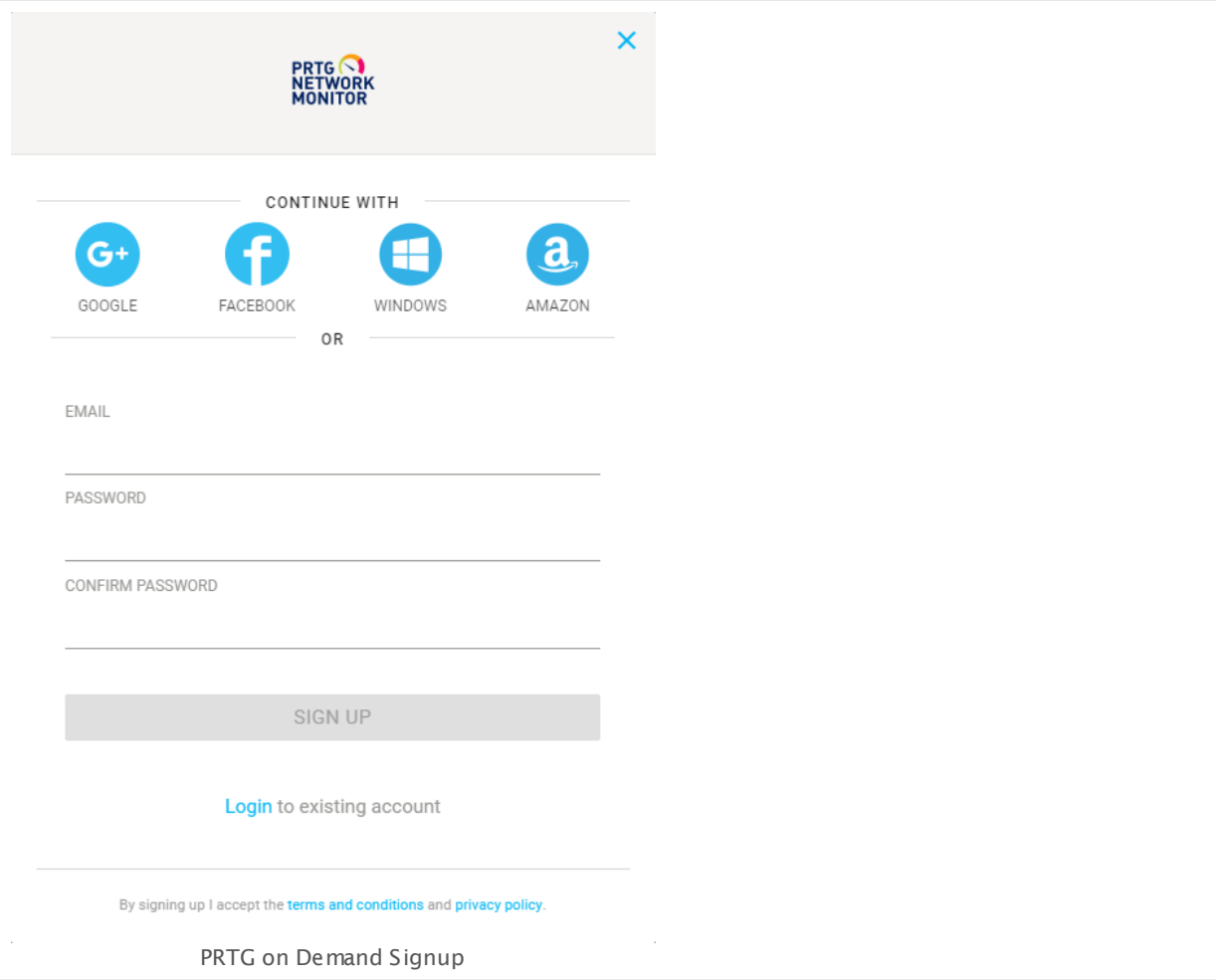
The following browsers are supported on my-prtg.com:

- Google Chrome 57 or later (recommended)
- Mozilla Firefox 52 or later
- Apple Safari 10



Start Free Trial Now

Enter a domain name of your choice, such as myfirstdomain. The domain name can be anywhere from 4 and 60 characters long and is where you can reach your PRTG on demand instance with your browser later. So if you enter myfirstdomain as the domain name here, your PRTG on demand instance will be reachable under myfirstdomain.my-prtg.com. Click **Start Free Trial Now** to continue.



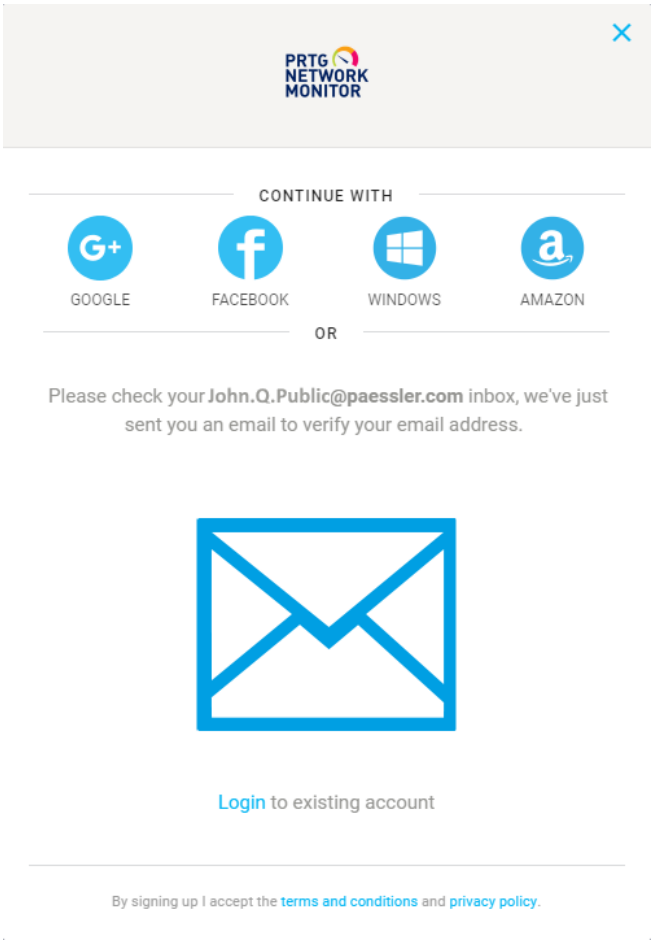
PRTG on Demand Signup

You can sign up with your Google+, Facebook, Windows, or Amazon account via single sign-on (Auth0). This account will then always be automatically used for login and will be connected to your PRTG on demand account. Just click the respective button and follow the instructions there.

Alternatively, you can sign up via email by entering a valid **Email** address, a **Password**, and confirming it with **Confirm Password**. The password must meet the following requirements:

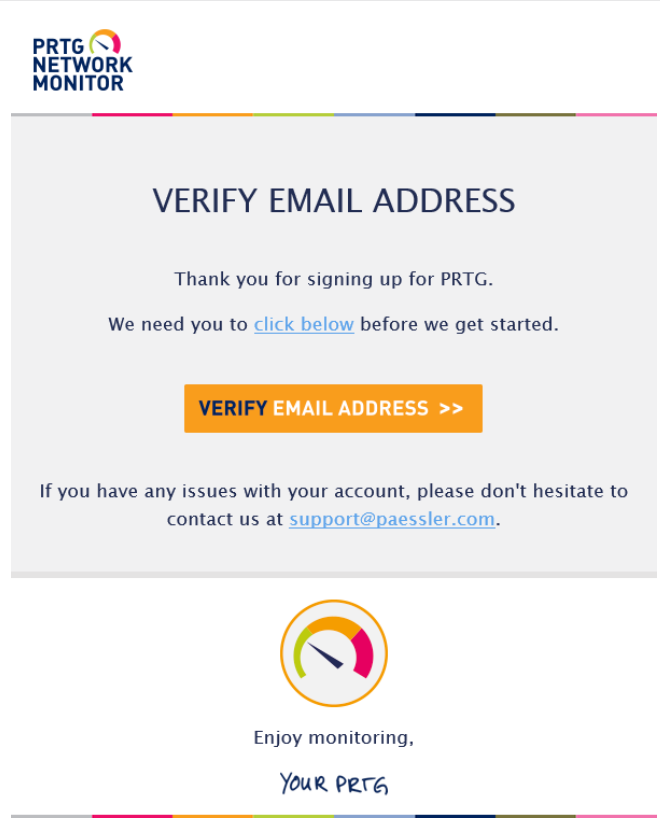
- at least 8 characters long
- at least one uppercase letter
- at least one lowercase letter
- at least one numeral

Click **Sign Up** to register for your PRTG on demand instance. PRTG then notifies you that a verification email has been sent to your inbox.



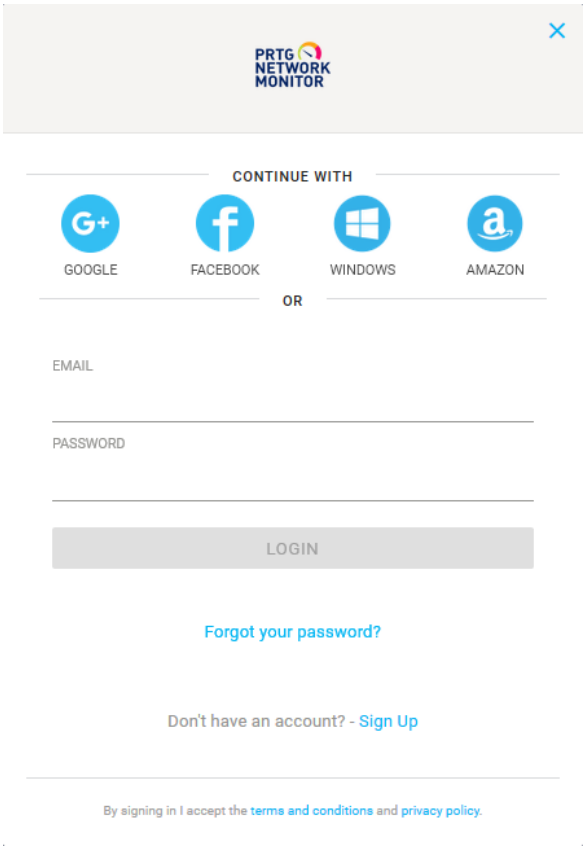
Verify Email Address Notification

Go to your inbox and open the email.



Verify Email Address

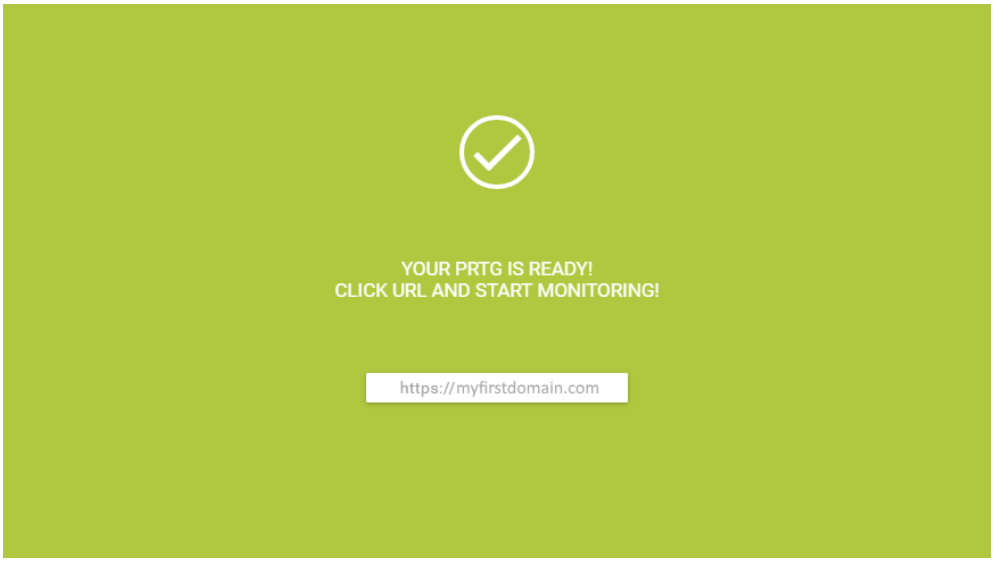
Click **Verify Email Address** to verify your email address and go to the login screen.



Login Screen

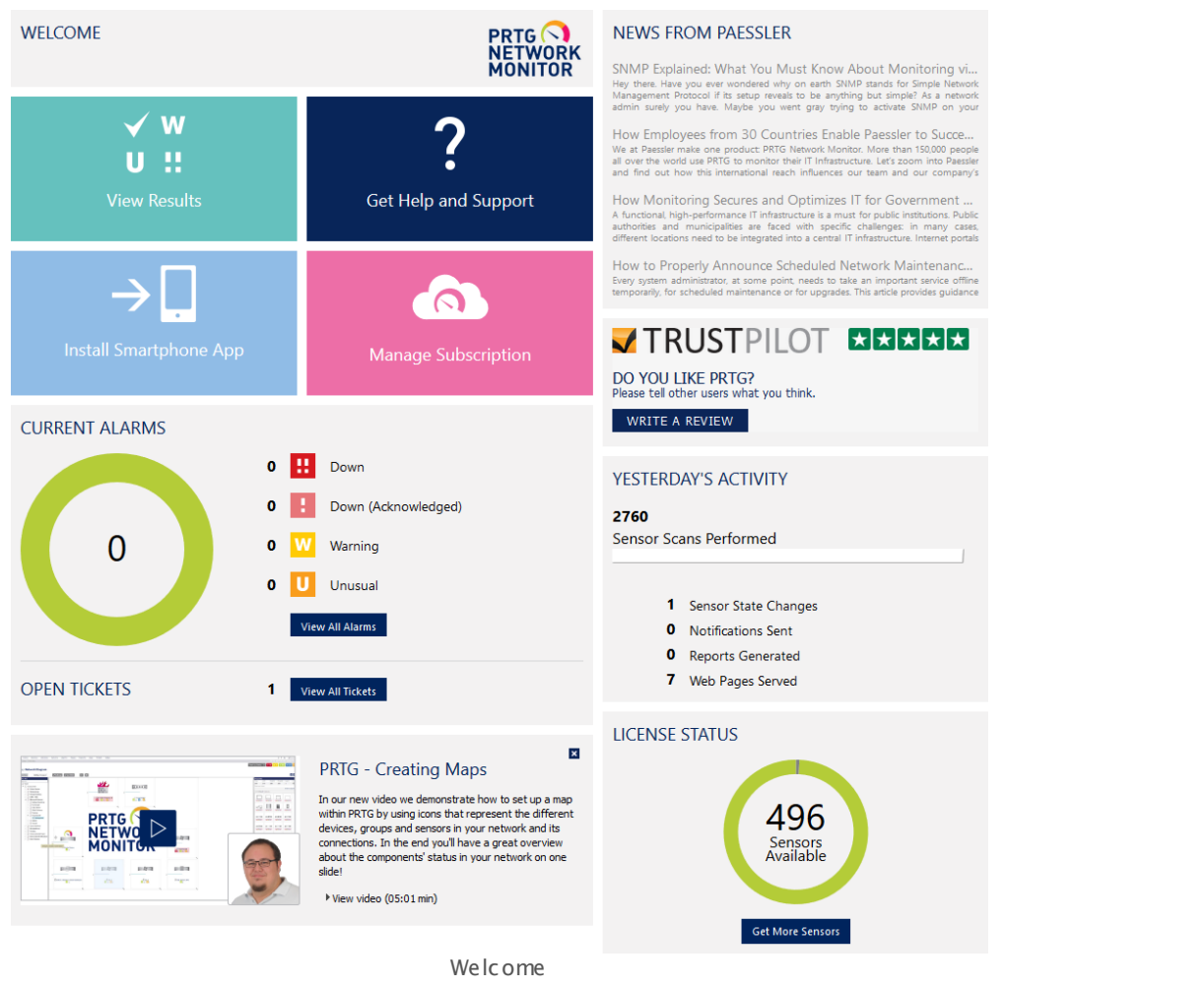
Enter your credentials and click **Login** to log in to PRTG on demand.

While we prepare your subscription, a welcome video plays that introduces the basics of network monitoring with PRTG on demand.



Your PRTG is Ready

When your subscription is ready, click the URL with your domain to open the Ajax web interface 136.



Welcome

Congratulations, your PRTG on demand instance is up and running! To open the device tree, click **View Results** or **Devices** in the main menu bar 231. You can instantly monitor all servers, services, and devices that are publicly available via the internet.

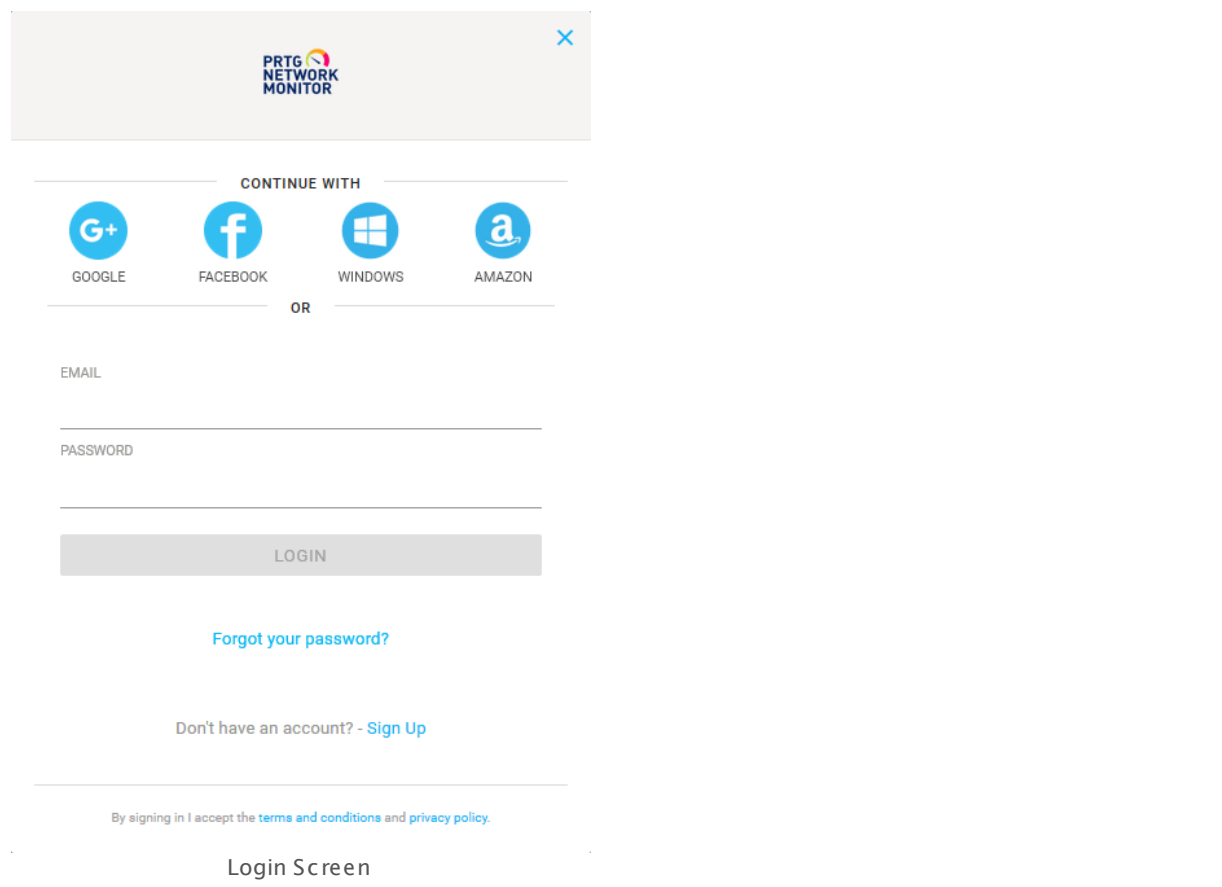
A Paessler employee will guide you through the **Smart Setup** 50. In particular, you will install a remote probe 3196, which is required for monitoring your LAN. We strongly recommend that you follow the instructions for best monitoring experience!

3.2 Manage a PRTG on Demand Subscription

BETA PRTG Network Monitor offers Monitoring as a Service with PRTG on demand. PRTG on demand runs in the cloud and does not require a PRTG core server installation inside your network, making monitoring even easier. We offer subscription plans that you can tailor to your needs and manage via the PRTG on demand web portal on my-prtg.com.

All you need to do is open a supported web browser (Google Chrome 57 or later (recommended), Mozilla Firefox 52 or later, Apple Safari 10), go to https://my-prtg.com, and log in to manage your subscription.

For details about setting up a PRTG on demand instance, see manual section **Create a PRTG on Demand Instance** 63.

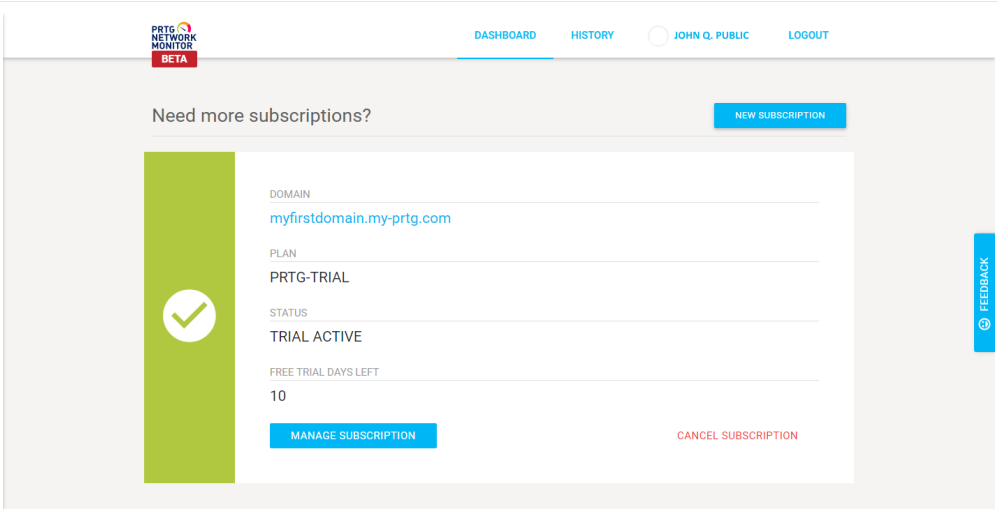


Login Screen

Provide the credentials you entered when signing up and click **Login** or use single sign-on and continue with your Google+, Facebook, Windows, or Amazon account via the respective button.

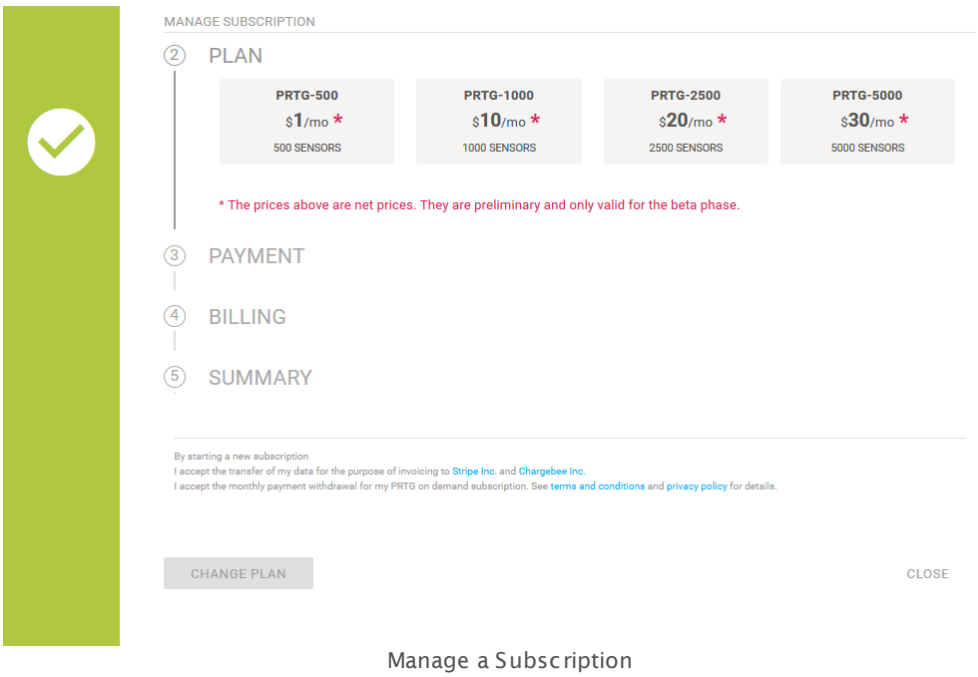
Dashboard

The **Dashboard** tab gives you an overview of your PRTG on demand subscription. Here you can manage or cancel your subscription, or add a new subscription. If you have purchased a subscription, you will also see when your next payment is due. You can also click the link under **Domain** to open the PRTG web interface [136].



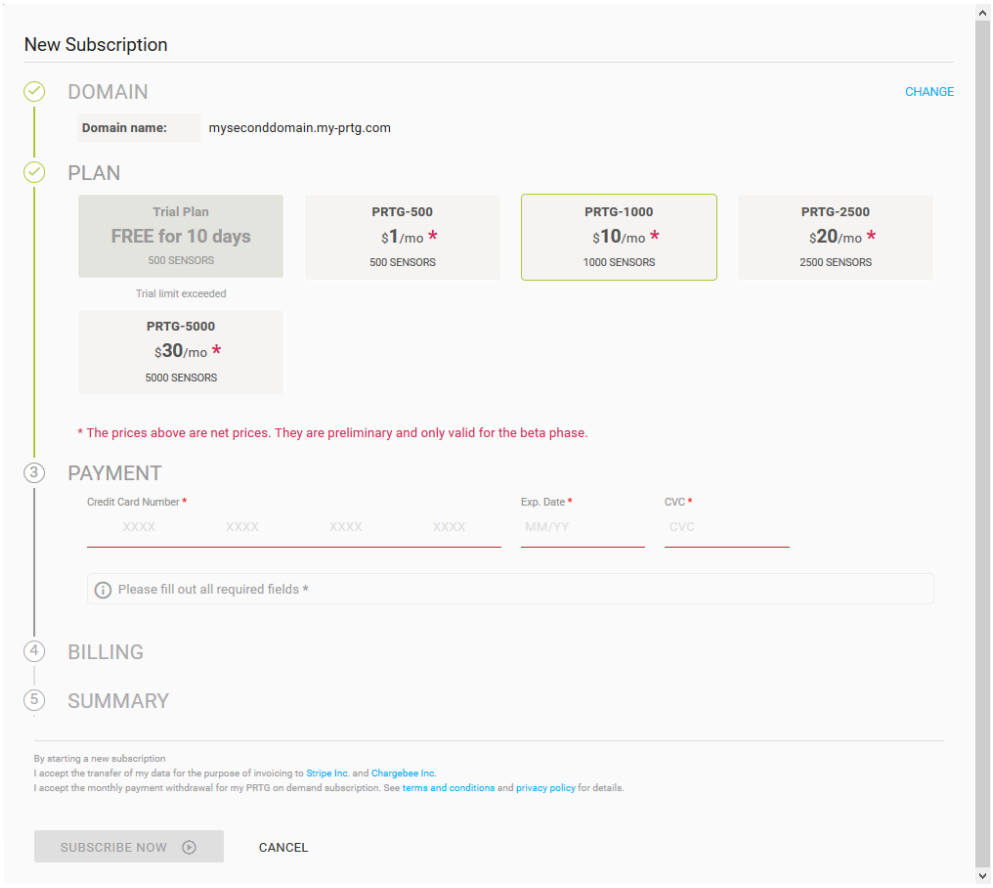
PRTG on Demand Dashboard

Click **Manage Subscription** to view your subscription details. The following information is displayed where you can edit your plan, payment, or billing address. Click **Change Plan** to save your changes.



Manage a Subscription

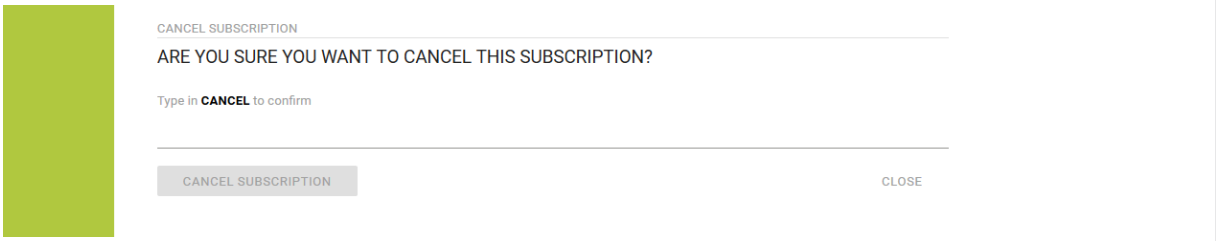
Click **New Subscription** to add a new subscription to your account.



Add a New Subscription

Enter a domain name, for example myseconddomain.my-prtg.com, choose a plan, and then enter your credit card information and billing address. Click **Subscribe Now** to add the subscription.

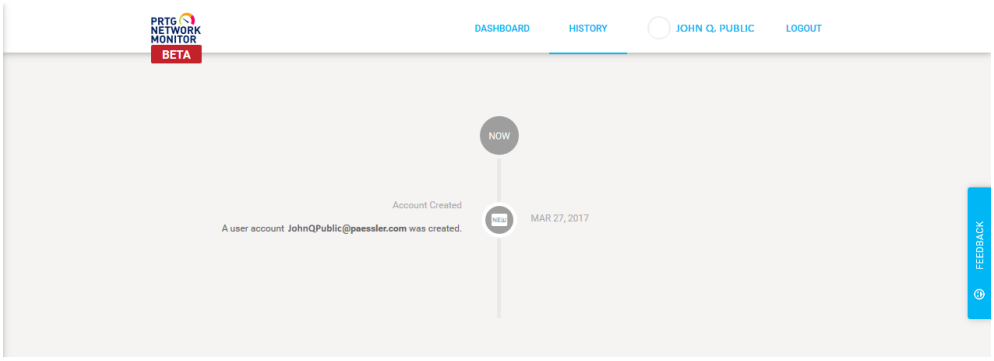
Click **Cancel Subscription** to cancel your PRTG on demand subscription. Enter CANCEL in the field and click **Cancel Subscription** again to finalize the cancellation.



Cancel a Susbcription

History

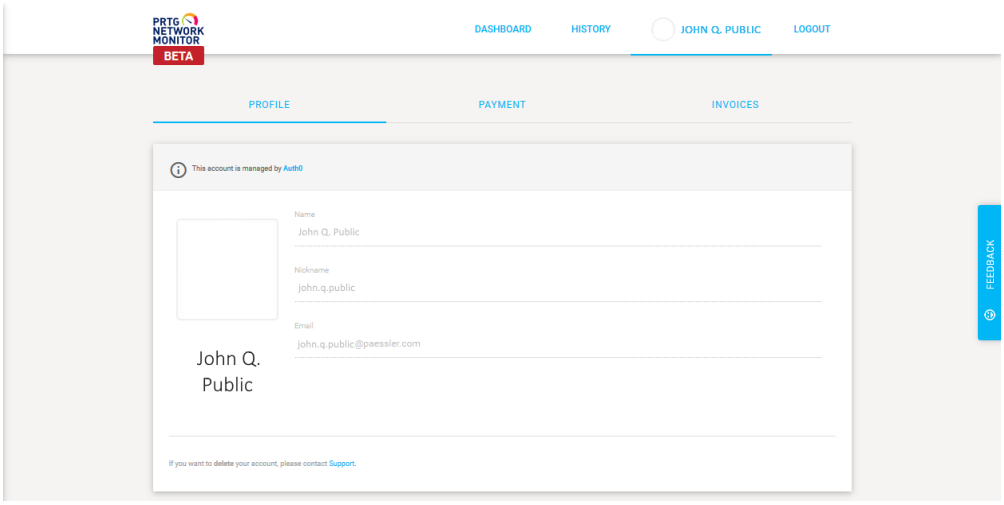
This tab gives you an overview of the history of your subscriptions.



Subscription History

Account Settings—Profile

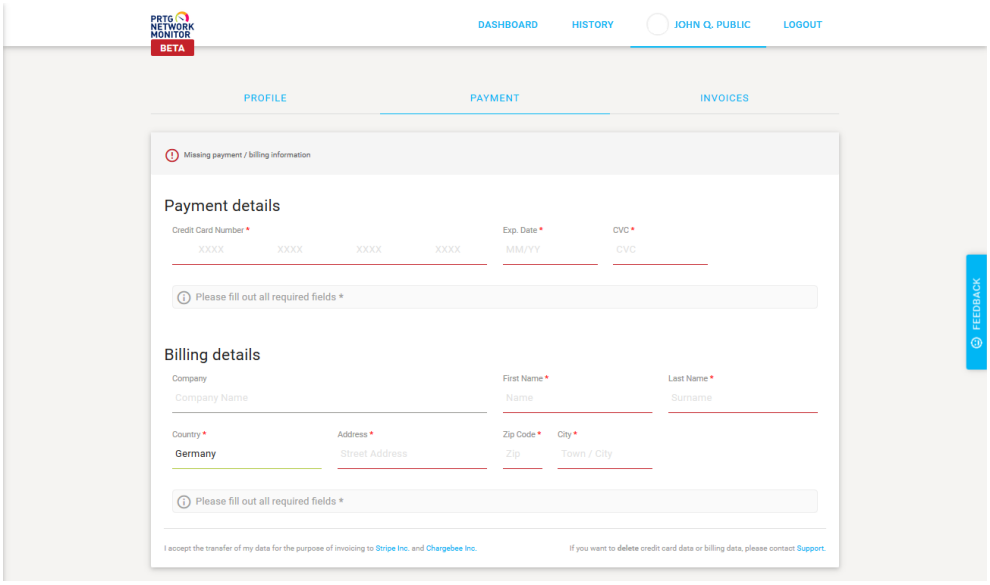
Here you can view your profile, view or update your payment information, and view your invoices.



User Account Settings

Account Settings—Payment

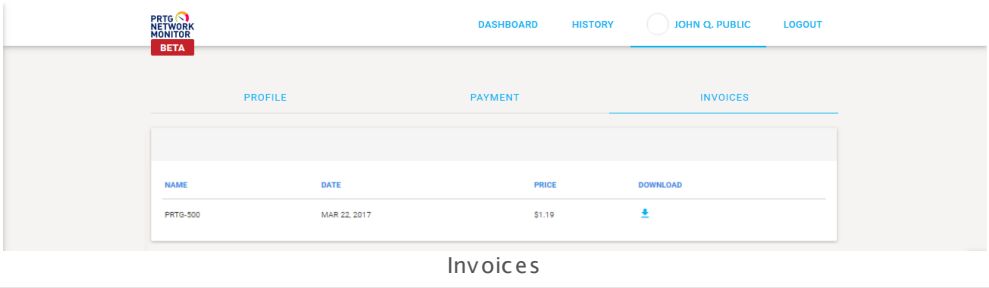
When purchasing a subscription, you will need your payment information. Enter your credit card information and billing address here to save it for later use.



Payment Informaton

Account Settings—Invoices

Here you can view and download all of your invoices.



Invoices

Logout

Click **Logout** in the upper-right corner to log out of your account.

Part 4

Installing the Software

4 Installing the Software

The following sections show you how to download and install your PRTG on premises instance. If you want to use PRTG on demand, just go straight to section Create a PRTG on Demand Instance 63 to get started.

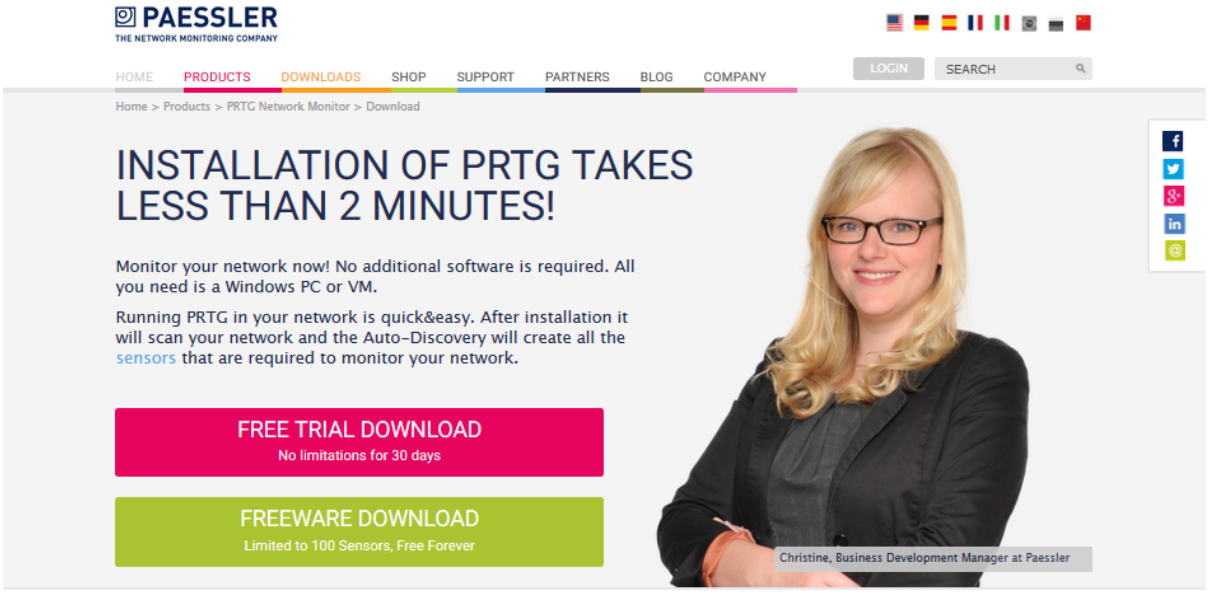
Installing the Software—Topics

- Download PRTG 77
- Update From Previous Versions 79
- Install a PRTG Core Server 84
- Create a PRTG on Demand Instance 63
- Install a PRTG Cluster 88
- Enter a License Key 89
- Activate the Product 91
- Install a PRTG Remote Probe 93
- Install the Enterprise Console 100
- Uninstall PRTG Products 106

4.1 Download PRTG

You can find the installer for PRTG on our website https://www.paessler.com. There you can also login to the Paessler shop to buy or upgrade your license, or to renew your maintenance.

This only applies to PRTG on premises instances, not to PRTG on demand.



Version Number, File Size	Version 17.1.28.1032 (January 10th, 2017), 146 MB
Available Translations	English, German, Spanish, French, Portuguese, Dutch, Czech, Japanese, Russian and Simplified Chinese
Operating Systems	All Windows versions (Windows 7 or later, see System Requirements)
What's new?	See Version History/Release Notes
Already PRTG customer?	Please log in to our website to download the full version

Download PRTG Network Monitor

Downloading PRTG Network Monitor

Please download the latest publicly available program version from the Paessler website. Simultaneously, you will receive a trial key. Enter this license key during the installation of PRTG. If you have already purchased a commercial license, use your commercial key. Please log in to the Paessler website to find your license key,

- **https://www.paessler.com/prtg/download**
- **https://shop.paessler.com/accounts/login/**

Every freeware installation starts as a trial version that allows you to use an unlimited number of sensors for 30 days. After the trial period has expired, your installation automatically reverts to the freeware edition with 100 sensors. Please understand that customers with a commercial license get prioritized support.

To upgrade your running trial or freeware version to a commercial edition, please purchase a commercial license key on https://shop.paessler.com and enter this key on the license page 3012 in the PRTG web interface.

Updates are free to customers with an active maintenance contract. If you do not have an active maintenance contract, please log in to the Paessler shop to renew it or contact sales@paessler.com.

Once installed, the PRTG **Software Auto-Update** 3005 will automatically download and install new software versions. This helps you keep PRTG up to date without manually installing new PRTG versions.

4.2 Update From Previous Versions

If you already have a previous software version installed, there are several things you have to consider before you update to the current PRTG version. Please see section **Detailed System Requirements** 25 to see all requirements for the current PRTG version.

We recommend that you always have a proper backup of your monitoring data and configuration. In most cases both will be maintained when upgrading. Anyway, we recommend a backup before upgrading. Please see **More** 83 section below.

On PRTG on demand instances, the update process is managed automatically, so you do not have to care about updating your PRTG.

Update from PRTG Network Monitor 16.1.22 or later

If you run PRTG Network Monitor with version 16.1.22 or later, simply install 84 the latest version on top of the previous version. Your configuration will be kept. PRTG updates remote probes 3196 automatically as well. If you have configured PRTG as a cluster 116, you only have to install an update on any node server (master or failover). PRTG deploys the new version to the cluster automatically.

We recommend that you use the **Auto-Update** 3005 of PRTG to install the latest version. Please always have a proper backup of your monitoring data.

With PRTG version 16.2.25, several sensor types have been removed from PRTG 80.

With PRTG 16.3.26, the Mobile Web GUI has been removed from PRTG.

Update from PRTG Network Monitor 13.1.1 through 16.1.21

As of version 16.1.22, PRTG is signed with renewed certificates. To be able to seamlessly update to version 16.1.22 or later an **intermediate update** is required for the PRTG core server and all probes if you currently run a PRTG version previous to 16.1.21.1691/1692. If you auto-update 3005 from previous versions (lower than 16.1.21.1691/1692), PRTG will automatically install this intermediate version first. You have to perform an additional auto-update to install the latest version. PRTG will notify you with a ticket 200 about this approach. Your configuration will be kept.

We recommend that you use the auto-update 3005 to install the latest PRTG version. If you update manually with an installer downloaded from the Paessler online shop, the intermediate update is only necessary if you currently run a PRTG version **previous to 16.1.21.1691/1692 with one or more remote probes or in a cluster setup.** If you do not perform this intermediate update, you will have to update your remote probes and cluster nodes manually. Please contact our technical support team 3022 to get the installer for this version if you do not use the auto-update.

- As of PRTG 14, **Internet Explorer 9 is no longer officially supported** for access to the PRTG web interface.
- Also as of PRTG 14, PRTG core and probes no longer officially support **Windows XP** and **Windows Server 2003** (including SP1 and SP2).

- As of PRTG 15, **Internet Explorer 10 is no longer officially supported** for access to the PRTG web interface.

Removed Sensor Types as of PRTG Network Monitor 16.2.25

We have removed several sensor types from PRTG with version 16.2.25. Sensors of these types that you still use in your PRTG installation will stop monitoring and show a down status as soon as you update to 16.2.25 or later. Most of the affected sensor types have been deprecated as of PRTG version 16.2.23 or before. You will receive tickets from PRTG that inform you if your PRTG setup is affected.

These sensor types were used by very few PRTG users and/or created substantial load for both our technical support and development team. We believe that the majority of PRTG users prefers that we focus on features that many customers use everyday rather than spending our precious energy on niche issues. We want to keep PRTG as easy to use as possible!

For a list of all discontinued sensors, possible alternatives, and more details about this approach, please see this article: https://kb.paessler.com/en/topic/68227

Web Interface Customizations as of PRTG Network Monitor 13.2.3

As of PRTG version 13.2.3, the website folder of the PRTG program directory is not used anymore. This means that if you update from a PRTG version older than 13.2.3 to the current version, all existing customizations of the web interface will be disabled and you have to revise them. You may find a way for a similar customization that you can add to the files in the current webroot folder that contains the web interface files now.

For details, please see the Knowledge Base: What about my web interface customizations as of PRTG 13.2.3?

Update from PRTG Network Monitor 9 and 12

We strongly recommend that you perform a clean install of the latest PRTG version instead of updating from an existing PRTG 9 or 12!

If you use PRTG 9 or 12 now, your configuration will be kept when installing the current PRTG version in **Standalone Mode** or when installing a **Master Node**. There are only a few things you should consider.

We recommend that you always have a proper backup of your monitoring data.

- **Intermediate versions:** You have to install two intermediate versions before you can update to the latest version.
  - If you currently run PRTG version 12.4.5.3164/3165 or lower, install the **intermediate version 12.4.7.3507** before you proceed.
  - If you have installed version 12.4.7.3507, install the **intermediate version 16.1.21.1691/1692** before you proceed. Afterwards you can seamlessly update to the latest PRTG version. For details about this intermediate update, please see section **Update from PRTG Network Monitor 13.1.1 through 16.1.21** 79 above.

  - We recommend that you use the **Auto-Update** 3005 feature. In this case PRTG will automatically install the intermediate versions. Run the auto-update three times if you come from a version previous to 12.4.7.3507, run it twice if you come from a version previous to 16.1.21.1691/1692. If you do not use the auto-update, please contact our technical support team 3022 to get the installers for these intermediate versions.

- **Discontinued Sensors:** Existing instances of the following sensor types will stop working as of PRTG V12 and must be replaced with their successor sensor types!

  - **VMware Host Server (SOAP)**
  - **VMware Virtual Machine (SOAP)**
  - **Xen Virtual Machine**

  If your configuration contains these sensor types, they will stop monitoring after upgrading to the current version. We recommend that you to pause them to keep their data. To continue monitoring, please add the sensors anew (for example, using the auto-discovery).

- **Please install .NET 4.0:** We strongly recommend that you install .NET 4.0 on systems that run the core server (and the remote probes, if you use those). Otherwise the following features will not work: VMware 391 auto-discovery and monitoring, Citrix XenServer 550 auto-discovery and monitoring, SIP Options Ping Sensor 1490, Windows Last Update Sensor (deprecated as of PRTG 16.x.23).

- **Changed Geo Maps Provider:** When you update to the current PRTG version, the provider for geographical maps will automatically be switched from Google Maps to MapQuest (using Open Street Map data).

- **Windows 2000 Not Supported:** Since PRTG 7 we do not officially support Windows 2000 systems anymore. This means that PRTG cannot be installed on systems running Windows 2000, and you cannot officially monitor Windows 2000 systems (for example, via WMI). However, if you could successfully monitor your Windows 2000 systems with PRTG 9, this might actually not be possible anymore with the current PRTG version.

We recommend that you to have a look at the **Detailed System Requirements** 25 before updating to the current version! Officially supported operating systems, browsers, and other requirements may have changed since version 9.

Update from PRTG Network Monitor 7 or 8

We strongly recommend that you perform a clean install of the latest PRTG version instead of updating from an existing PRTG 7 or 8!

If you use PRTG 7 or 8 now, you have to update PRTG to intermediate versions first to ensure all data is carried over correctly. You **cannot update to PRTG 15 or later directly** from PRTG 7 or 8!

- We recommend that you first update to the latest PRTG 8 version.
- From the latest PRTG 8 version update to PRTG version 9.
- From PRTG 9, update to both intermediate versions 80 12.4.7.3507 and 16.1.21.1691/1692 and then to the current PRTG version.

Please contact our technical support 3243 to obtain download links for these PRTG versions. Always keep a proper backup of your configuration and monitoring data!

Updating from PRTG 7 or 8 to Current PRTG Version

- Packet Sniffer (Content) sensors are not supported anymore. Existing sensors of this type will automatically be switched to Packet Sniffer (Header) sensors after the update. As a benefit, you can now also sniff IPv6 traffic.
- Internet Explorer 8 is no longer supported for access to the PRTG Ajax web interface.
- You may experience a slow Enterprise Console 3028 (former 'Windows GUI') due to different reasons.
- When installing a failover node on top of an existing stand-alone PRTG 7, 8, 9, 12, or 13+ installation, the configuration cannot be kept and is written to a backup folder. Then, the new cluster configuration is received from the master node of the cluster. As all nodes work with the same configuration, a failover node's old configuration and monitoring data can no longer be used. If you want to keep a configuration of PRTG 7, please install the master node on top of the old installation and use other servers for the failover node installations.
- Since PRTG 9 the SNMP sensors use the **IPv4 Outgoing IP** set for the probe service (this setting was formerly ignored by those sensors, using the **auto** setting instead). If you experience failing sensors, please check the setting in the probe settings 330.
- If you have (manually) configured the PRTG probe or PRTG core service to run under a different Windows user account (for example, for successful internet access through an ISA server firewall), please apply the respective Windows user account for the "PRTGProbeService" and/or "PRTGCoreService" anew after installing the current PRTG version.
- System Requirements for the PRTG core server and probes: please have a look at our latest **Detailed System Requirements** 25.
- If you use the default data path in your PRTG setup, it will be changed automatically. Up to version 8 all data was stored in a sub folder reflecting a PRTG version number (v7 or v8). As of version 9 this sub folder is omitted, and data is stored directly at %ALLUSERSPROFILE%\Application data\Paessler\PRTG Network Monitor. During setup, all data will be moved to the new directory. If you use a custom data path it will not be changed.
- Up to version 8 all data in the registry was stored in a sub key reflecting a PRTG version number (v7 or v8). As of version 9 this sub key is omitted, and registry data is stored directly under the key HKEY_LOCAL_MACHINE\SOFTWARE\Paessler\PRTG Network Monitor (on 32-bit systems) respectively HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Paessler\PRTG Network Monitor (on 64-bit systems). During setup, all existing registry values will be moved to the new key.

We strongly recommend that you have a look at the **Detailed System Requirements** 25 before updating to the current version! Officially supported operating systems, browsers, and other requirements may have changed since version 8.

Updating from PRTG 7 to Current PRTG Version

- Regarding custom sensors, the interpretation of returned values is handled more strictly as of PRTG 8. If you use custom sensors with PRTG 7, these may not work with the current PRTG version if they do not fully apply to the API definition 3174.

Update from Older PRTG Products

For all other predecessor products, a direct data import into the current version is not possible.

If you have been using IPCheck 5 or PRTG Traffic Grapher 6, please perform a clean installation of PRTG Network Monitor and set up your configuration anew. Using the **Auto-Discovery** 249 in PRTG is the easiest way to quickly configure a monitoring of your entire network. Please see **Quick Start Guide** 44 section for more information.

More

Knowledge Base: How do I backup all data and configuration of my PRTG installation?

- https://kb.paessler.com/en/topic/523

Knowledge Base: What about my web interface customizations as of PRTG 13.2.3?

- https://kb.paessler.com/en/topic/44703

Knowledge Base: How and where does PRTG store its data?

- https://kb.paessler.com/en/topic/463

Knowledge Base: Updating from Version 7, 8, 9 or 12? Read this important message!

- https://kb.paessler.com/en/topic/35563

Knowledge Base: Can I update from PRTG Traffic Grapher or IP Check 5 to the current PRTG version?

- https://kb.paessler.com/en/topic/26553

Knowledge Base: What does error code PE251 mean?

- https://kb.paessler.com/en/topic/65764

Knowledge Base: The signature of my PRTG server is not valid. What can I do?

- https://kb.paessler.com/en/topic/66308

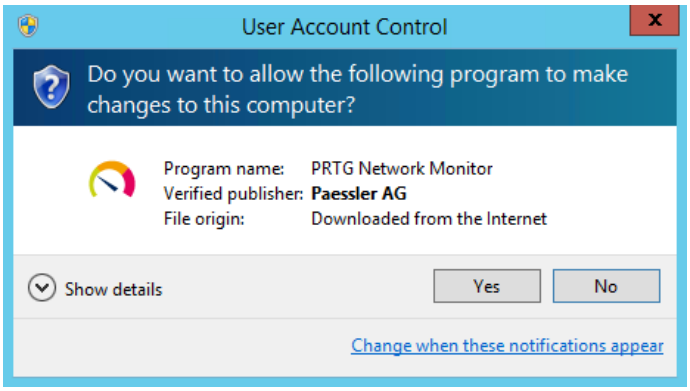
Knowledge Base: Which sensor types do you remove from PRTG and what are the alternatives?

- https://kb.paessler.com/en/topic/68227

4.3 Install a PRTG Core Server

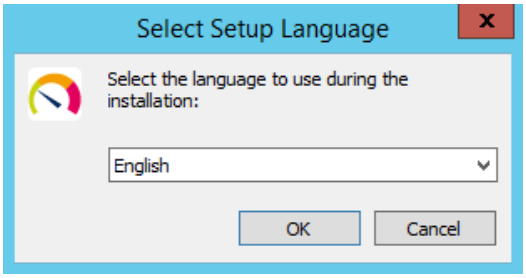
Installing PRTG Network Monitor is easy and works like other Windows-based applications. To install PRTG, run the installation setup program from the ZIP file that you have downloaded.

This only applies to PRTG on premises instances, not to PRTG on demand.



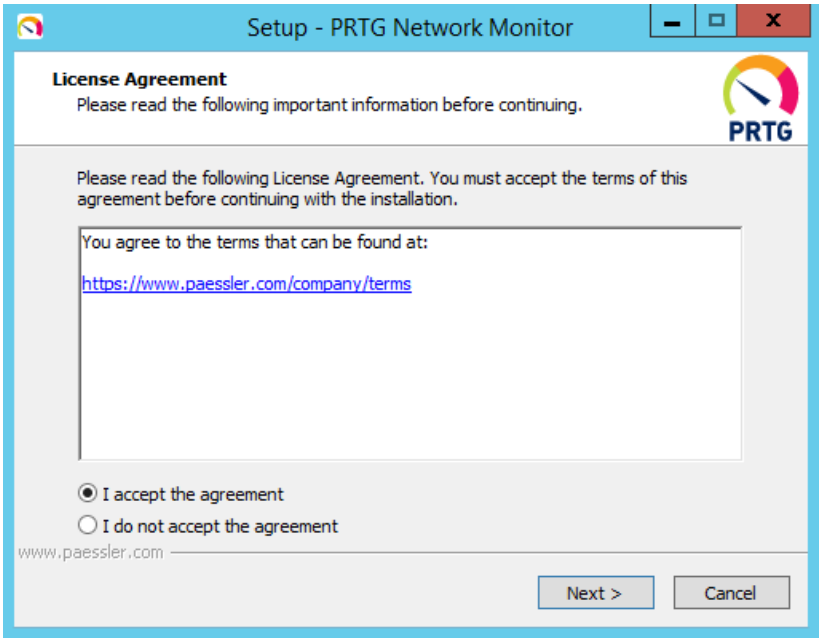
Windows User Account Control Confirmation Request

Confirm the question of the Windows User Account Control with **Yes** to allow the program to install. The PRTG installation dialog will guide you through the installation process.



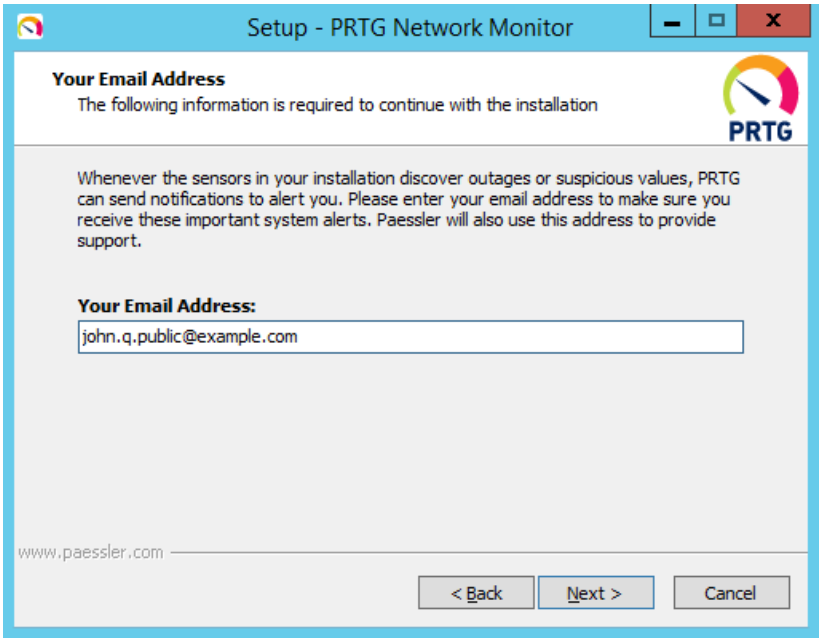
Setup Language Selection

Select a language for the program and click the **OK** button. The available language options depend on both your Windows version and the setup file.



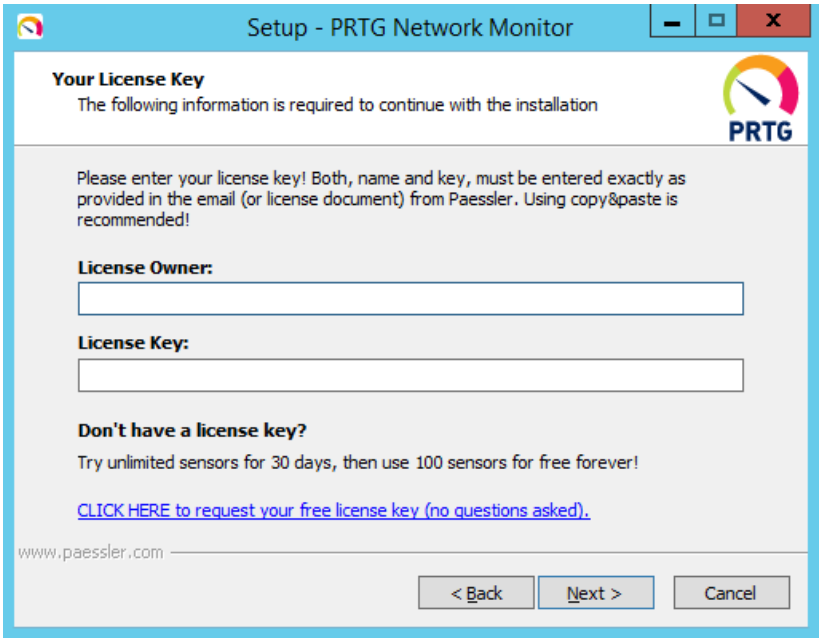
Setup Dialog: License Agreement

Accept the license agreement and click **Next**.



Administrator Email Address

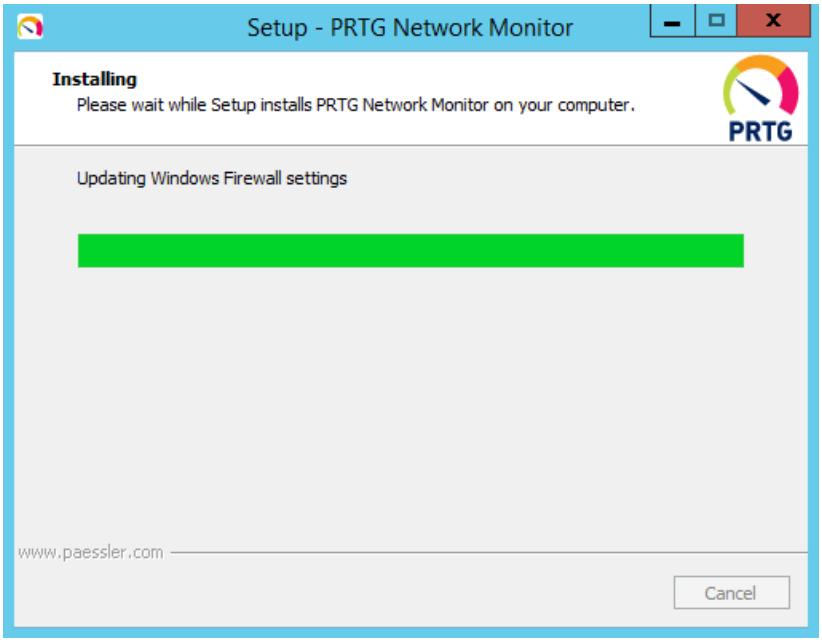
Enter a valid email address. Your PRTG server will send important and urgent system alerts to this address. Click the **Next** button to continue.



License Key Information

Enter your license information. You have to provide the **License Name** and the **License Key** exactly as you received it in the email or license document from us, the Paessler AG. We recommend that you use copy&paste to avoid typos. Click **Next** to confirm.

You will find the label License Owner in some documents from the Paessler shop. License Owner is the same as License Name for which you will be asked while installing PRTG or when you change your license key 89.



Setup: Installing PRTG

After installation, PRTG opens the **Ajax Web Interface** 136 in your system's default browser. Make sure there is Google Chrome 57 or later (recommended), Mozilla Firefox 52 or later, or Microsoft Internet Explorer 11 available on the system, and set as default browser (see **System Requirements** 23).

Enter License Information

PRTG will validate your license information during the install process by connecting to the activation server. If you have entered incorrect license information before, PRTG will ask you to re-enter a correct License Name and key. Please enter both **License Name** and **License Key** exactly as received from Paessler. We recommend that you use copy&paste to avoid typing mistakes. For details, please see **Enter a License Key** 89.

If you think that you have correctly entered your license information but get a **License Invalid** message, please contact sales@paessler.com.

You will find the label License Owner in some documents from the Paessler shop. License Owner is the same as License Name for which you will be asked while installing PRTG or when you change your license key 89.

More

Knowledge Base: How can I establish a secure web interface connection to PRTG?

- https://kb.paessler.com/en/topic/273

Knowledge Base: PRTG blocks port 80 although I'm using SSL on port 443. How to free port 80?

- https://kb.paessler.com/en/topic/5373

License Agreement

- https://www.paessler.com/company/terms

4.4 Install a PRTG Cluster

PRTG offers single failover clustering in all licenses—even using the freeware edition. A single failover cluster consists of two servers ("Current Master" Node and "Failover Node"), each of them running one installation of PRTG. They are connected to each other and exchange configuration and monitoring data. You can run a cluster with up to 5 nodes.

This feature is not available in PRTG on demand.

Illustration of a Single Failover Cluster

Click here to enlarge: http://media.paessler.com/prtg-screenshots/clustering-1_en.png

For detailed information, please see **Failover Cluster Configuration** 3212.

More

Knowledge Base: What's the Clustering Feature in PRTG?

- https://kb.paessler.com/en/topic/6403

4.5 Enter a License Key

A license key for PRTG Network Monitor consists of the **License Name** and a **License Key**. The key is a string that consists of 8 blocks with 5 characters each.

This only applies to PRTG on premises instances, not to PRTG on demand.

Your Personal License Information

You have received the **License Name** and the **License Key** from Paessler via email or in a license document on Paessler shop. Please copy this information and insert it when PRTG asks you to about your license information in the setup dialog.

You will find the label License Owner in some documents from the Paessler shop. License Owner is the same as License Name for which you will be asked while installing PRTG or when you change your license key 89.

For the Trial and Freeware editions, you will receive the required license information on the Paessler webpage when you download the trial or freeware version of PRTG. For a commercial edition, use your commercial license information.

EXAMPLE OF LICENSE INFORMATION

License Name: **John Q. Public**
License Key: **P1000-FFSEJ-ZHGRD-UR1CS-U73FG-G645F-YVF1D-H8323**

During the setup process, PRTG will ask you to enter your license information. Please use copy and paste to fill out the form in the installer dialog.

- **Trial/Freeware license key:** When entering a Trial license key, you can experience unlimited functionality of PRTG during the 30-day trial period. Your installation automatically switches to a Freeware Edition afterwards. For details about how to get your free Trial edition, please see **Download PRTG** 77 section.
- **Commercial license key:** You can only enter this key if you have purchased a commercial license. Your installation allows the number of sensors according to your license 21.

Change License Key

Usually you do not need to enter a key manually after the installation to activate it, because PRTG asks for it during the install process. However, there are still scenarios where you need to change your key and activate this license. You have to provide your commercial license key, for example, if you have purchased a PRTG Commercial Edition and want to upgrade your running PRTG Freeware or Trial installation, or if you upgrade an existing commercial license to a higher edition.

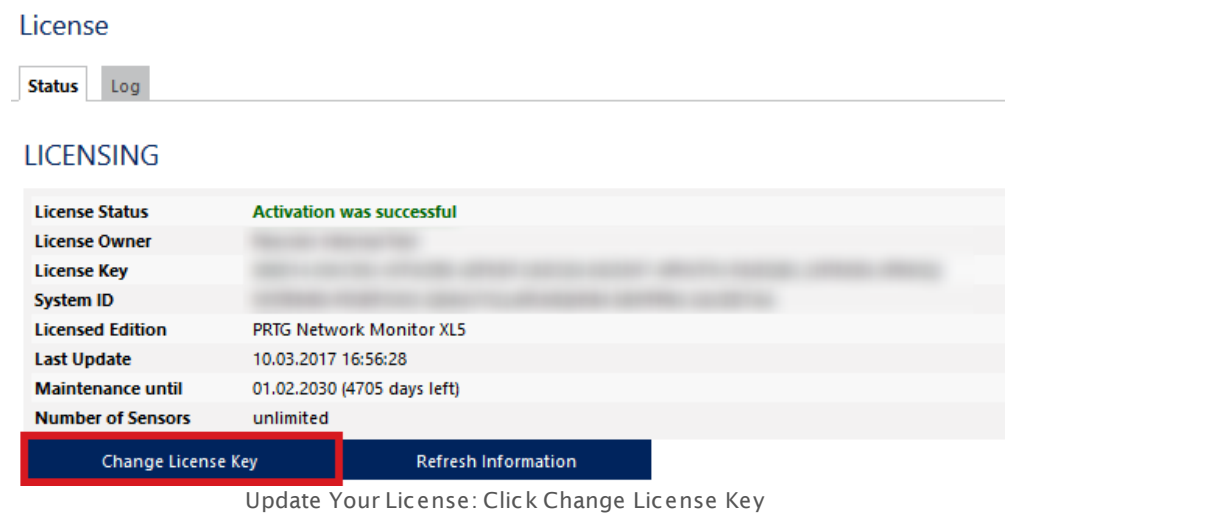
- To enter a new license key, log in to the PRTG web interface 136.
- Choose **Setup | License** from the main menu bar 231.

- Click **Change License Key**.
- The **Update Your License** page appears where you can activate your new license.
- Choose the activation type **Automatic (online activation with optional HTTP proxy)** if your PRTG server can connect to the internet.
  Without internet access, you have to choose **Manual (offline activation)**. The activation process works a bit different in this case and requires manual interactions.
- Provide your license information and click **Update License**.
- PRTG will connect to the Paessler activation server via SSL on port 443 and validate your license.
- If everything works fine, you will see the message **Activation was successful** as **License Status** on top of the page.

For details, please see manual section **PRTG Status—Licensing Status and Settings: Update Your License** 3014.

The PRTG core server needs an internet connection on port 443 to activate. If a proxy connection is needed, please configure it in Step 3: Activate 3015 on the **Update Your License** page. If activation fails, you can also try an offline activation.

This option is not available in PRTG on demand.



Update Your License: Click Change License Key

More

Video Tutorial: PRTG License and Maintenance

- https://www.paessler.com/support/videos/prtg-basics/license-maintenance

Video Tutorial: PRTG Sensor Count and License Upgrade

- https://www.paessler.com/support/videos/prtg-basics/sensor-count

Knowledge Base: How do I upgrade to a higher edition of PRTG?

- https://kb.paessler.com/en/topic/4193

4.6 Activate the Product

PRTG will activate your license automatically via the internet during the install process. Only if PRTG cannot connect to the internet directly and so cannot access the activation server, will you have to activate your license manually.

You have to complete the product activation process once to use PRTG, otherwise it will not run. Do not forget to activate your commercial license when you want to upgrade your trial or freeware installation!

This only applies to PRTG on premises instances, not to PRTG on demand.

Online Activation

Usually you do not need to enter a key manually after the installation to activate it, because PRTG asks for it during the install process. However, there are still scenarios where you need to change your key and activate this license. You have to provide your commercial license key, for example, if you have purchased a PRTG Commercial Edition and want to upgrade your running PRTG Freeware or Trial installation, or if you upgrade an existing commercial license to a higher edition.

- To enter a new license key, log in to the PRTG web interface 136.
- Choose **Setup | License** from the main menu bar 231.
- Click **Change License Key**.
- The **Update Your License** page appears where you can activate your new license.
- Choose the activation type **Automatic (online activation with optional HTTP proxy)** if your PRTG server can connect to the internet.
  Without internet access, you have to choose **Manual (offline activation)**. The activation process works a bit different in this case and requires manual interactions.
- Provide your license information and click **Update License**.
- PRTG will connect to the Paessler activation server via SSL on port 443 and validate your license.
- If everything works fine, you will see the message **Activation was successful** as **License Status** on top of the page.

For details, please see manual section **PRTG Status—Licensing Status and Settings: Update Your License** 3014.

The PRTG core server needs an internet connection on port 443 to activate. If a proxy connection is needed, please configure it in Step 3: Activate 3015 on the **Update Your License** page. If activation fails, you can also try an offline activation.

This option is not available in PRTG on demand.

Offline Activation

If there is no internet connection available, you have to activate PRTG manually.

This option is not available in PRTG on demand.

- In the PRTG web interface 136, choose **Setup | License** from the main menu bar 231.
- Click **Change License Key**.
- The **Update Your License** page appears where you can activate your license.
- Choose the activation type **Manual (offline activation)** if your PRTG server cannot connect to the internet.
- Provide your license information and follow the instructions in step 3 3016 and step 4 3016.
- Click **Update License**.
- If everything works fine, you will see the message **Activation was successful** as **License Status** on top of the page.

For details, please see manual section **PRTG Status—Licensing Status and Settings: Update Your License** 3014.

If your PRTG server is offline, you need to manually activate your license after you have renewed your maintenance. This ensures you can enjoy the benefits of an active maintenance like the possibility to install updates. Your maintenance information has to fit the PRTG installer, so accomplish your offline activation before you install an update.

More

Knowledge Base: Which servers does PRTG connect to for Software Auto-Update and for Activation?

- https://kb.paessler.com/en/topic/32513

4.7 Install a PRTG Remote Probe

A PRTG remote probe helps you extend your monitoring to distributed networks or take load from the system running the core installation. All you need is a computer on which you can install your remote probe.

Your PRTG core server installation 84 already includes a local probe. This is why you cannot additionally install a remote probe on your core system.

Because your remote probe needs to connect to your PRTG core server, your PRTG core server must accept incoming connections. Please **prepare the core server** 3206 first.

PRTG updates remote probes automatically, but in rare cases a manual probe update is required. You will receive a ToDo ticket 201 in this case. Please follow the steps below to manually update a remote probe.

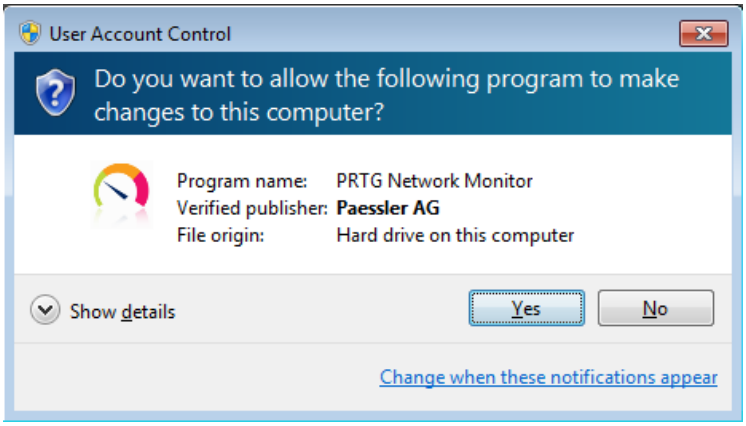
Download the Remote Probe Installer from the PRTG Web Interface

On the computer on which you want to install remote probe, log in to the PRTG web interface 138. From the main menu bar 231, select **Setup** | **Downloads** | **Remote Probe Installer**. Click **Download: Remote Probe Installer** and save the setup program to your local disk.

The version numbers of core and probe services must match. PRTG updates probes automatically when a new version is installed on the PRTG core server. If PRTG advises you to update your remote probe manually, open a web browser on your remote computer and download the remote probe installer as described in this manual section.

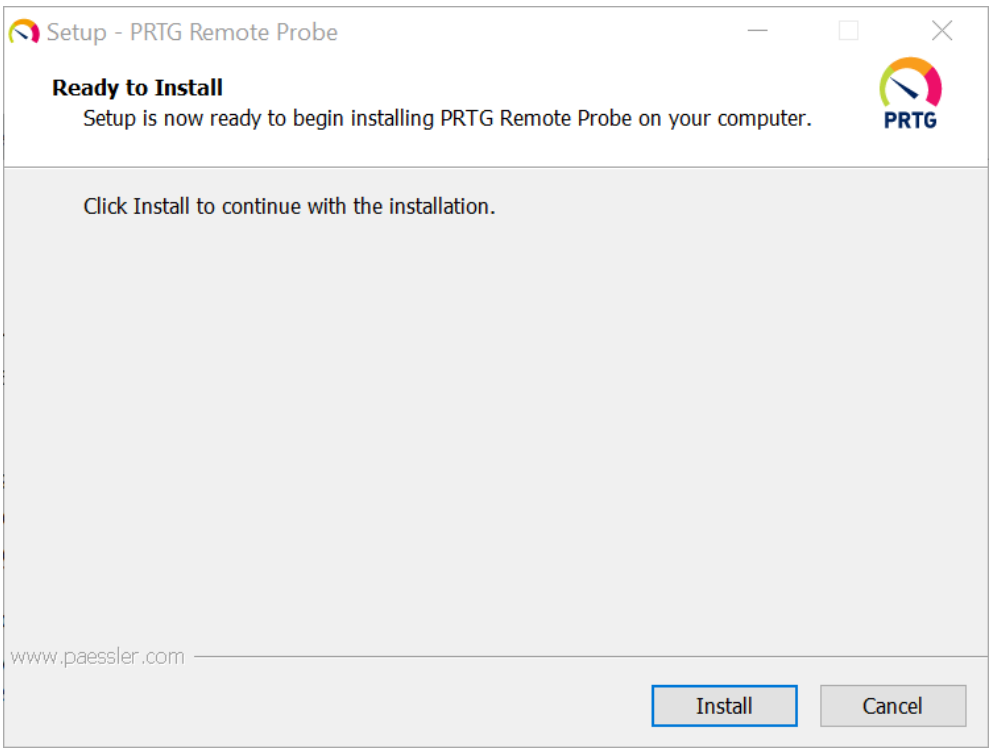
Install the Remote Probe

Execute the setup program that you have just downloaded.



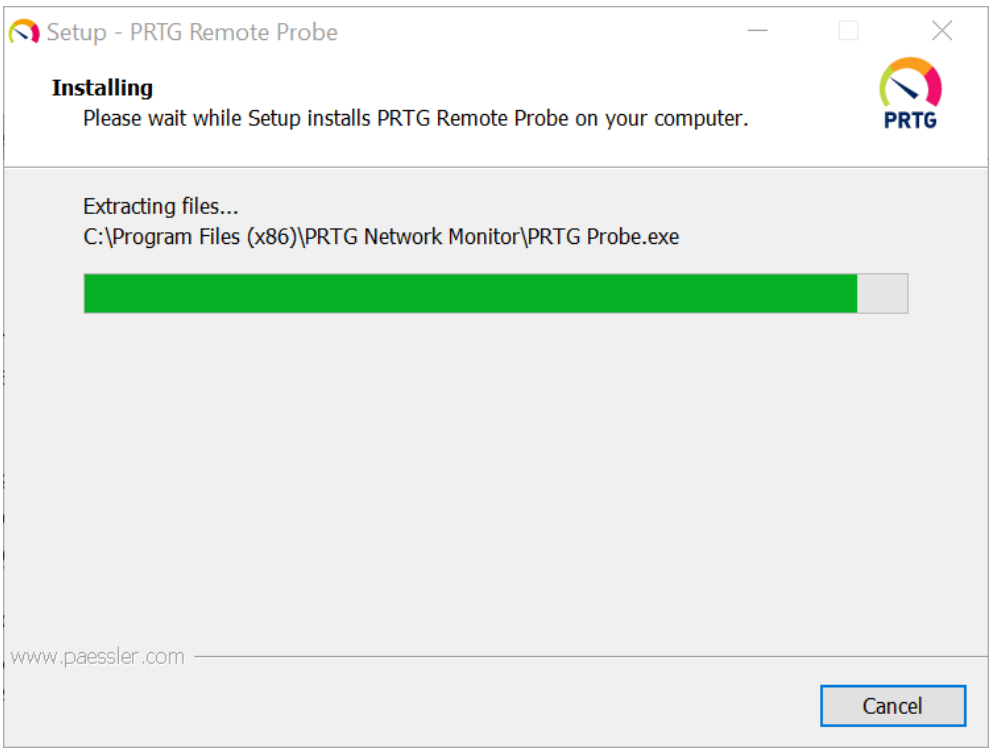
Windows User Account Control Confirmation Request

Confirm the Windows User Account Control dialog with **Yes** to allow the installation. The usual software installation wizard will guide you through the installation process.



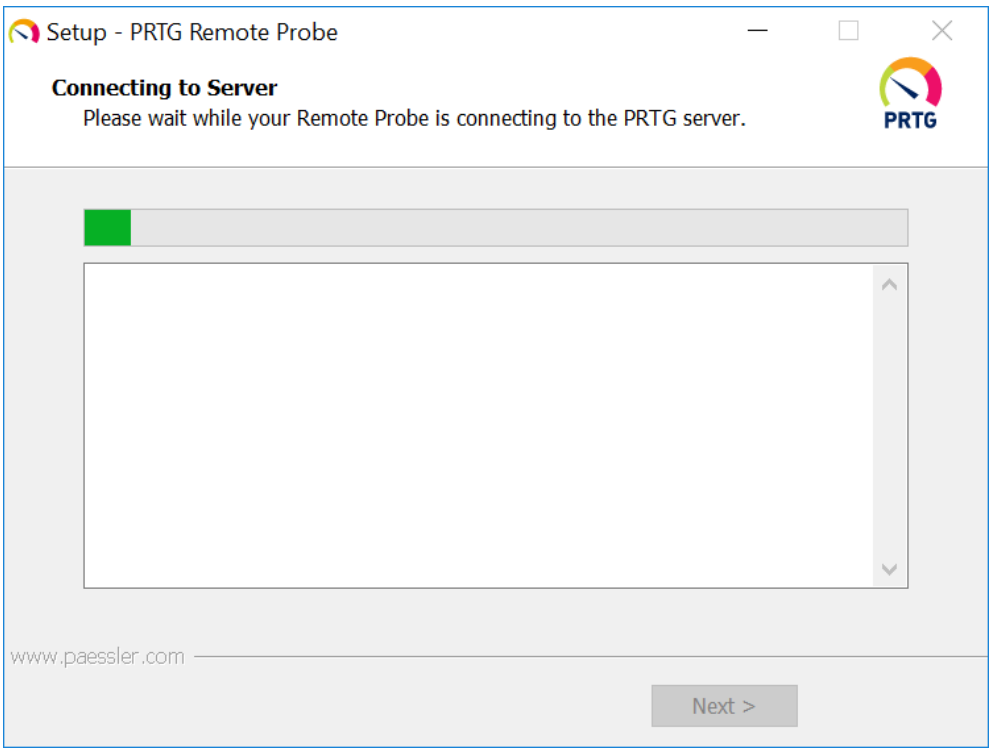
PRTG Remote Probe Setup Ready to Install

Click **Install** to start the installation process of your remote probe.



PRTG Remote Probe Setup Installing

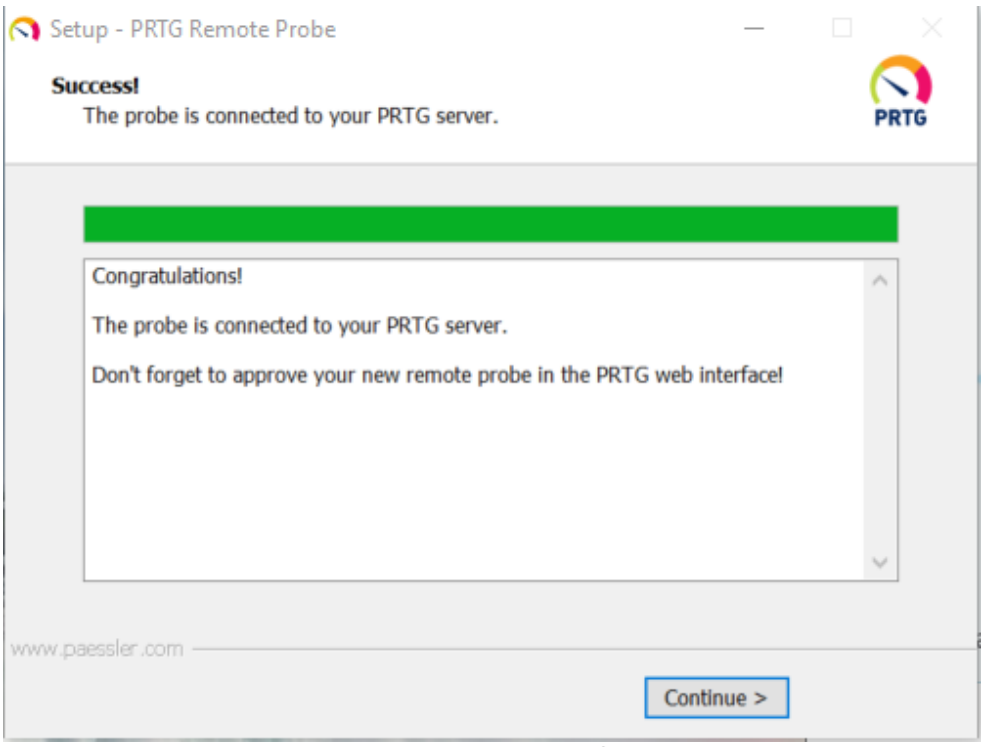
Please wait until the installation is completed. The remote probe will automatically connect to your PRTG core server then.



PRTG Remote Probe Setup Connecting to Server

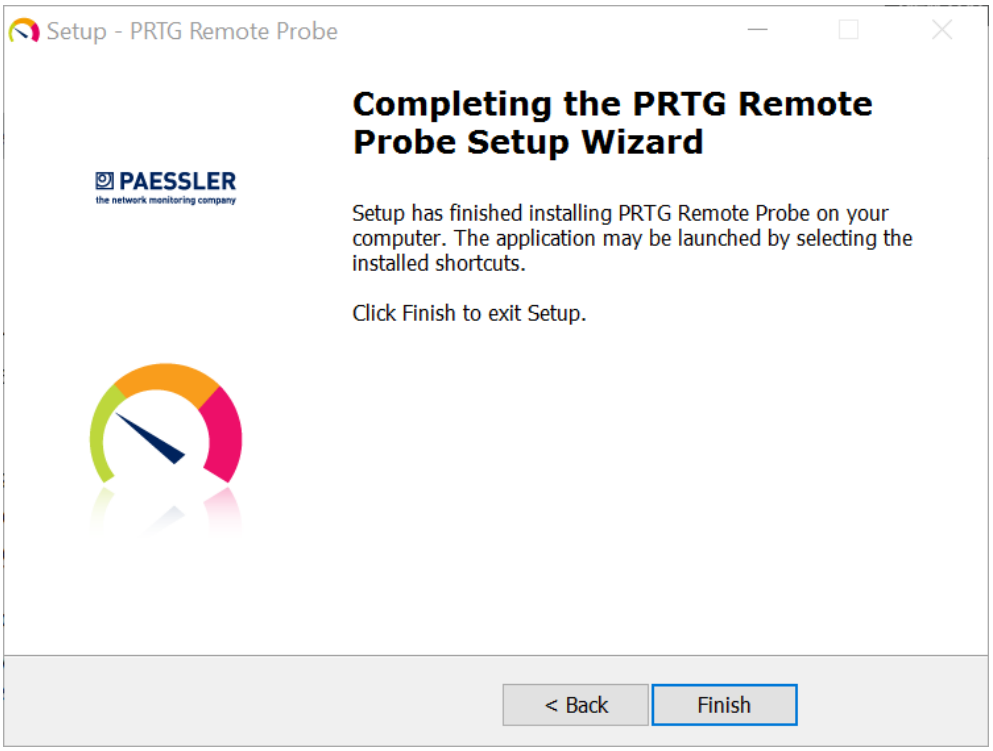
If the remote probe successfully connects to your PRTG core server, you can complete the setup of your new remote probe.

To allow your new remote probe to connect to the PRTG core server, PRTG automatically sets the **Allow IPs** field in System Administration—Core & Probes 2968 to **any**. We recommend that you use this setting in intranets only. If **any** is not an option for you, cancel it in the **Allow IPs** field and enter the IP address of your remote probe instead.



PRTG Remote Probe Successful Setup

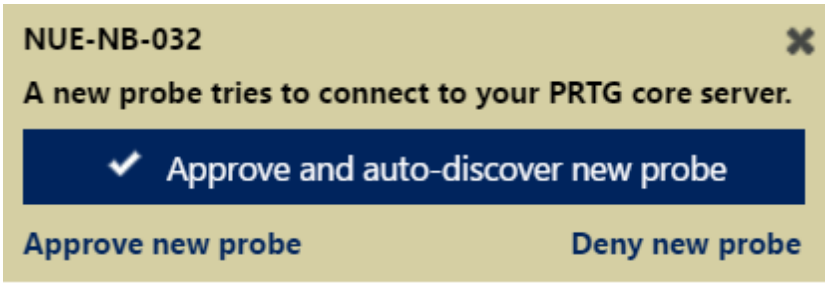
Click **Continue** to finish the remote probe installation.



PRTG Remote Probe Finish Setup

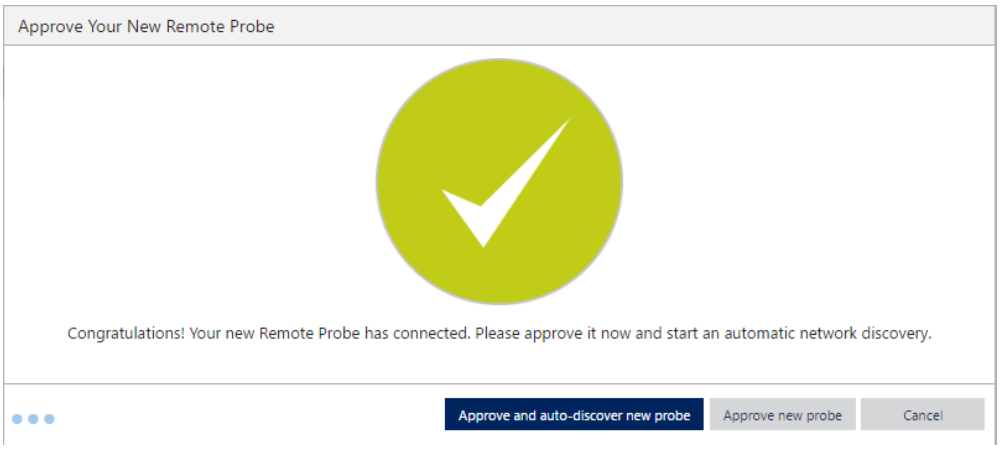
Finally, click **Finish** to exit the installation wizard. The remote probe is now installed on your computer as a Windows service.

Remember to log in to the PRTG web interface to acknowledge your new remote probe!



PRTG Remote Probe Approval

If you successfully installed the remote probe from a PRTG on demand installation, you will see the following dialog box.

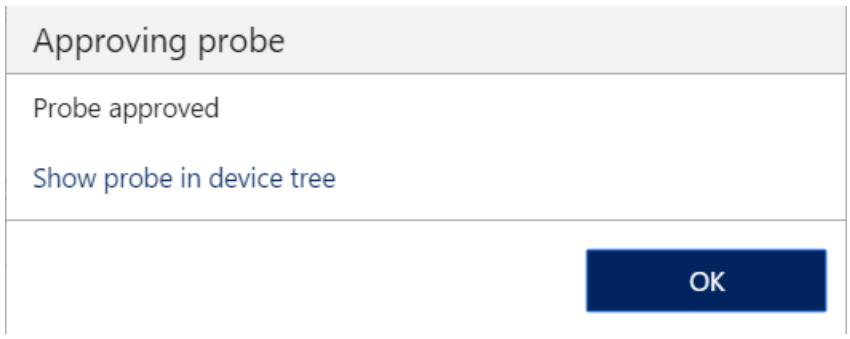


Approve PRTG Remote Probe for PRTG on demand

Click **Approve and auto-discover new probe** to include your new remote probe device and network in your device tree and to start the PRTG auto-discovery 249. It helps you discover devices and automatically create suitable sensors. Optionally, you can also choose to only approve your remote probe without starting an auto-discovery by clicking **Approve new probe**. The probe now appears as a new object in your device tree.

For unwanted probe connections, you can click **Deny new probe**. Note that this does not uninstall the remote probe, but only prohibits the probe from connecting to the PRTG core server.

If you deny or remove a remote probe, PRTG will include this device's global ID (GID) into **Deny GIDs** in System Administration—Core & Probes 2967. Future probe connections from this device will be denied automatically.



PRTG Remote Probe Approved

In the **Approving probe** dialog, click **OK** to exit the dialog, or click **Show probe in device tree** to open the new probe in the device tree directly.

You do not have to approve remote probes after updates.

More

For more details about the remote probe installation and core probe connection process, see the **Remote Probe Using Installer** 3206 section.

You can also use the **PRTG Administration Tool** 3134 to edit administrative settings regarding your PRTG core and probe installations. See the **Remote Probe Setup** 3206 section for more detailed information about the remote probe setup.

4.8 Install the Enterprise Console

The Enterprise Console is already included in a PRTG core server installation 84 (PRTG on premises only) You can install additional Enterprise Consoles on other computers.

PRTG on demand does not support connections from the Enterprise Console. If you want to use it, please connect the Enterprise Console to a PRTG on premises instance.

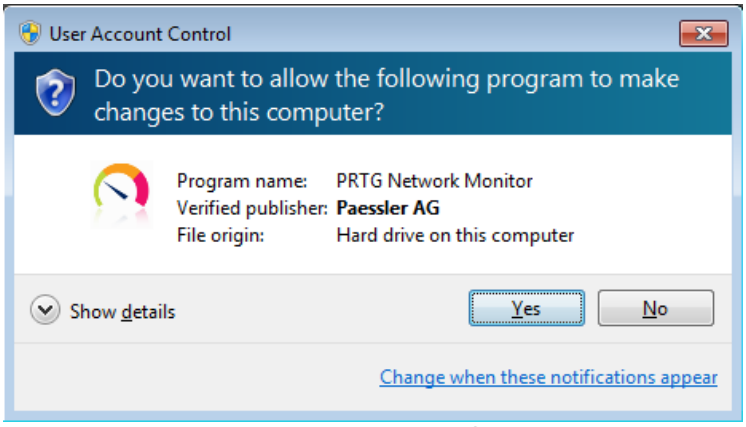
Download Enterprise Console from the Web Interface

The version of the Enterprise Console (EC) has to match the PRTG core server version you want to connect to. It can connect to a PRTG server where the third entry in the version number is equal to the third entry of the EC version number. For example, EC version 15.1.16.2023 can connect to any PRTG server with version 15.1.16.xxxx.

1. From the computer you want to install the Enterprise Console on, connect to the Ajax 136 web interface of PRTG.
2. On the login screen 138 of the web interface, enter login name and password and click **Download Client Software (optional, for Windows, iOS, Android)**.
3. You will see the downloads page 3018 where you can download the EC.
4. Click **Download: PRTG Enterprise Console** and save the setup program to the local hard disk drive.

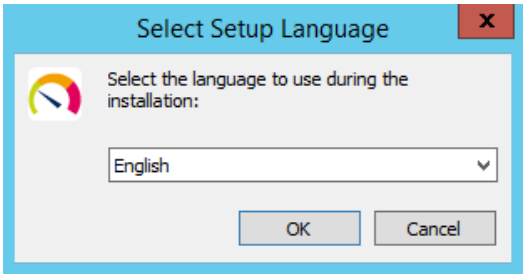
Install Enterprise Console

Execute the setup program **PRTG_Enterprise_Console_Installer.exe** that you have downloaded.



Windows User Account Control Confirmation Request

Confirm the question of the Windows User Account Control with **Yes** to allow the program to install. The usual software installation assistant will guide you through the installation process.

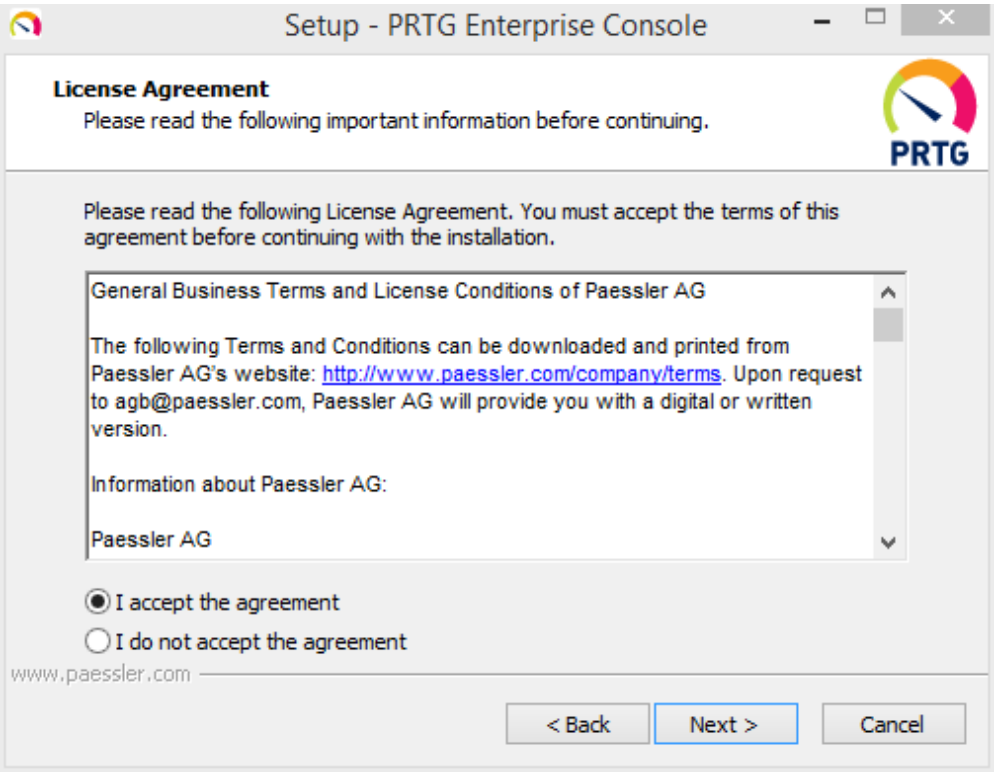


Setup Language Selection

Select a language for the program and click the **OK** button. The available language options depend on both your Windows version and the setup file.

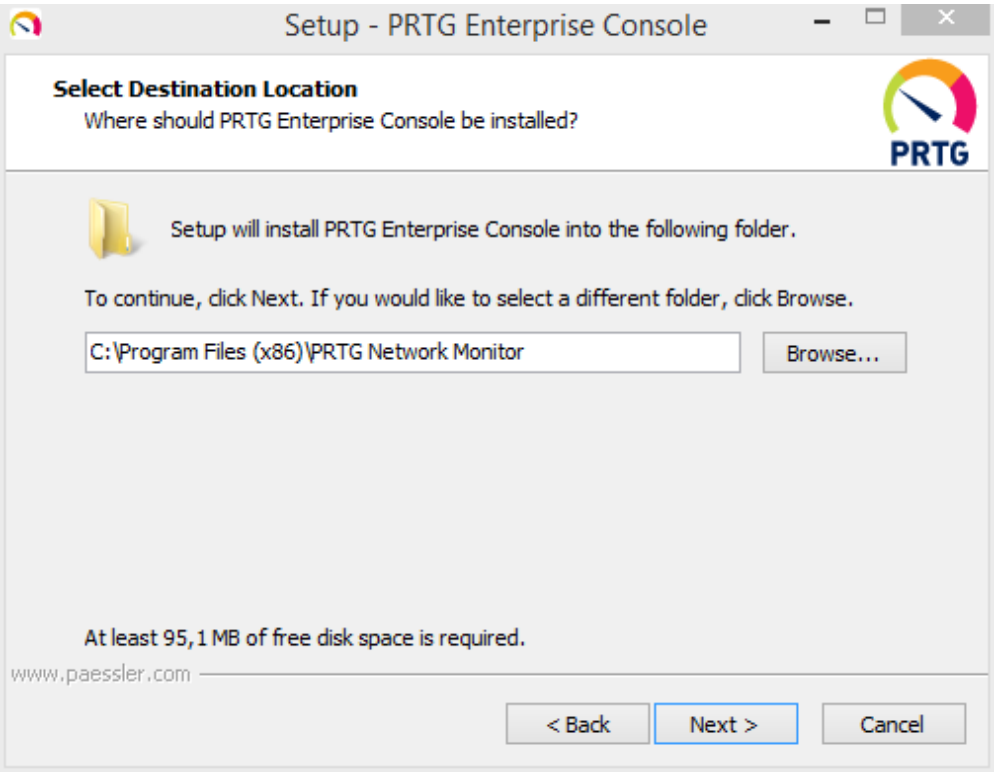
Enterprise Console Setup: Welcome Screen

Click **Next** to walk through the wizard.



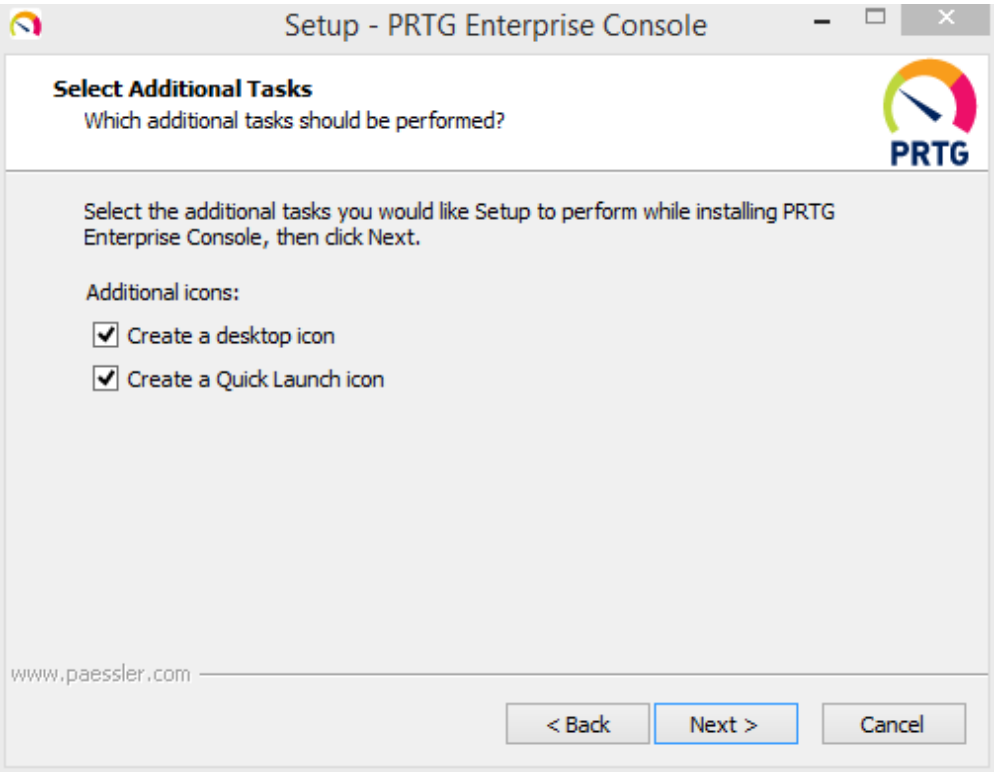
Enterprise Console Setup: License Agreement

After accepting the license agreement, you can choose the folder you wish to install the software in. We recommend that you use the default value.



Enterprise Console Setup: Installation Folder

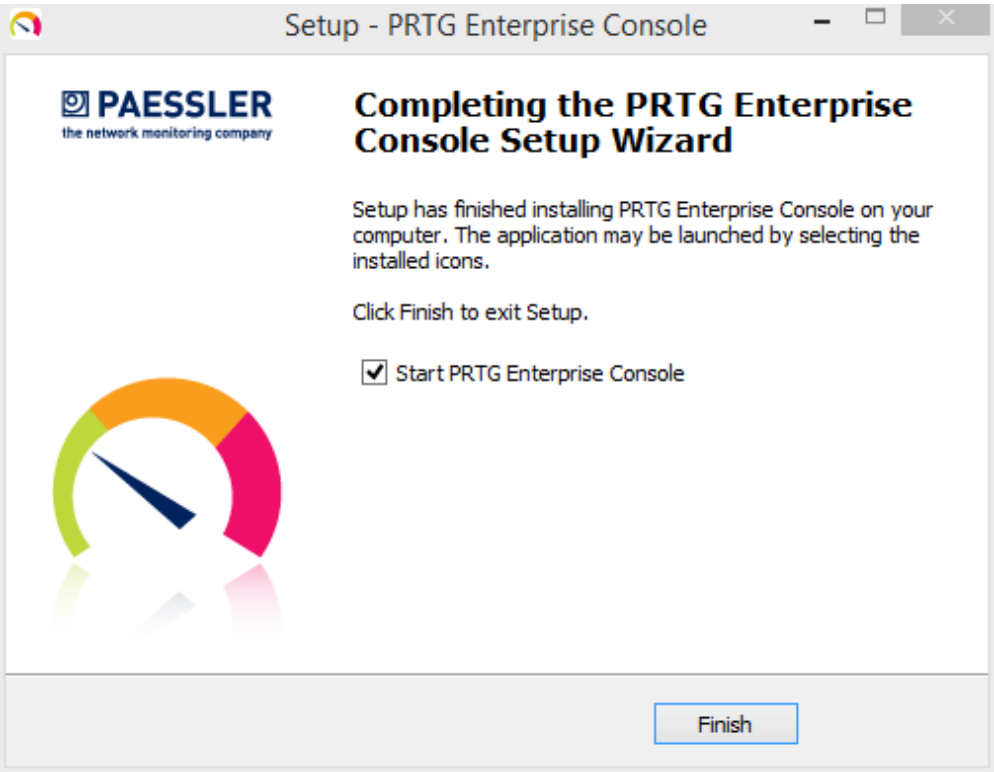
Select the start icons you want to create for the Enterprise Console. We recommend that you use the default value.



Enterprise Console Setup: Additional Tasks

Click **Next** to copy the necessary files to the disk of your computer.

After installation, click **Finish** to start the Enterprise Console. Enter the settings for the connection to your PRTG server 3029 in the appearing dialog.



Enterprise Console Setup: Finish

More

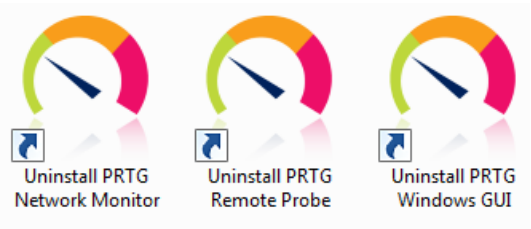
Please see the section **Enterprise Console** 3028 for more information on how to use this Graphical User Interface (GUI).

4.9 Uninstall PRTG Products

The uninstall process has six steps—regardless of if you are uninstalling an entire PRTG Network Monitor installation, a single Enterprise Console installation, or a PRTG Remote Probe installation. Use the Windows uninstall routines to remove the PRTG software from your system.

Step 1

From the Windows Start Menu, select the **Uninstall PRTG Network Monitor** icon, the **Uninstall PRTG Enterprise Console** icon, or the **Uninstall PRTG Remote Probe** icon, or open your Windows Control Panel and choose the respective entry in the **Programs** section. Depending on the installed products, not all uninstall programs are available.



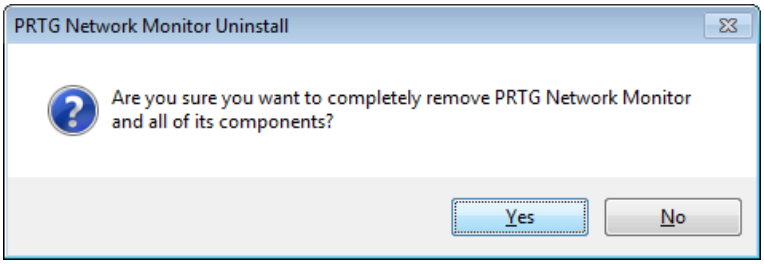
Start Menu Icons

Step 2

If asked, confirm the question of the Windows User Account Control with **Yes** to allow the program to uninstall. The usual software uninstall wizard will guide you through the uninstall process.

Step 3

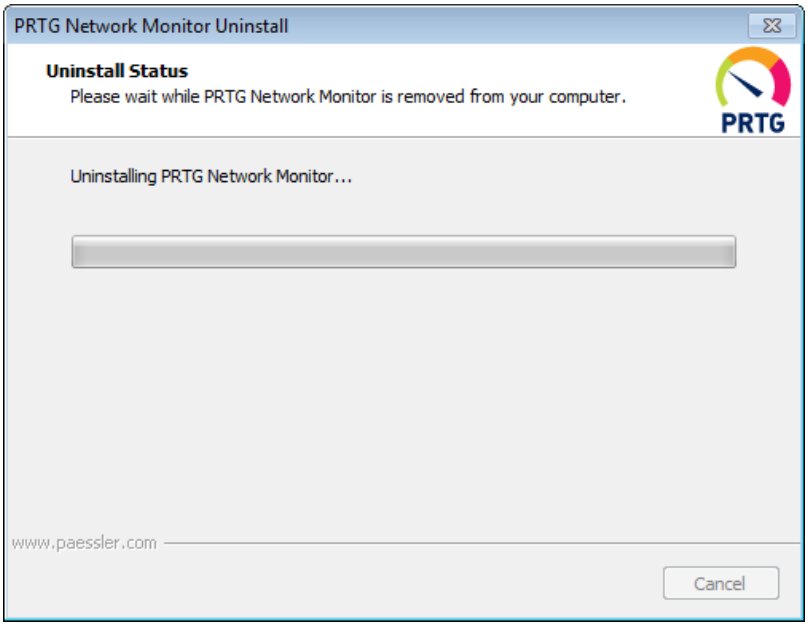
Confirm the removal of the software by clicking the **Yes** button.



Uninstall PRTG Network Monitor Step 1

Step 4

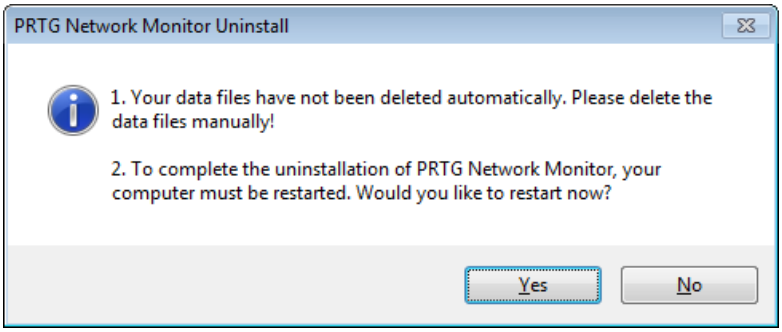
Wait while the software is being removed.



Uninstall PRTG Network Monitor Step 2

Step 5

Confirm a system restart by clicking the **Yes** button.



Uninstall PRTG Network Monitor Step 3

Step 6

After system restart, the software is removed. However, there are still custom data left in the PRTG program folder. If you have uninstalled an entire PRTG Network Monitor installation or a remote probe installation, your monitoring data is still stored on the system. To completely remove all PRTG data, delete the **PRTG Network Monitor** program folder as well as the **Paessler\PRTG Network Monitor** folder in your data path. For more information on where the data is stored see the **Data Storage** 3226 section.

More

Knowledge Base: Can we remotely and silently uninstall a Remote Probe?

- https://kb.paessler.com/en/topic/27383

Part 5

Understanding Basic Concepts

5 Understanding Basic Concepts

There is a number of basic concepts that are essential for understanding the functionality and ease of use of PRTG Network Monitor. We have made using our software as easy as possible. Setting it up for the first start and getting first monitoring results happens almost automatically 50.

Nevertheless, there are some basic principles we would like to explain to you. Please read these sections carefully to understand the underlying workflow like architecture of the monitoring system, hierarchy of objects, settings inheritance, and notifying. You will be able to enhance your monitoring experience permanently as soon as you know the basic principles of PRTG!

Understanding Basic Concepts—Topics

- Architecture and User Interfaces 111
- Clustering 116
- Object Hierarchy 118
- Inheritance of Settings 122
- Tags 124
- Dependencies 126
- Scheduling 127
- Notifying 128
- Data Reporting 132
- User Access Rights 129
- IPv6 133

5.1 Architecture and User Interfaces

PRTG Network Monitor consists of three main categories: System parts, control interfaces, and a basic administration interface.

TYPE	PART OF PRTG
System Parts	Core Server 112 This is the central part of a PRTG installation and includes data storage, web server, report engine, a notification system, and more. The core server is configured as a Windows service that runs permanently. Probe(s) 112 The part of PRTG that performs the actual monitoring. There are local probes, remote probes, and cluster probes available. All monitoring data is forwarded to the central core server. Probes are configured as Windows services that run permanently. We assume that all computers on which the PRTG core server with its local probe or any remote probes run are secure. It is every administrator's responsibility to make sure that only authorized persons can access these machines. For this reason we highly recommend that you use dedicated machines for your PRTG system parts.
User Interfaces	Ajax Web Interface 136 The Ajax-based web interface is used for configuration of devices and sensors, as well as for the review of monitoring results. Also system administration and user management are configured here. Enterprise Console 3028 A native Windows application as alternative to the web interface to manage your monitoring. With the Enterprise Console, you can connect to different independent PRTG core server installations and review their data at a glance! PRTG Apps for Mobile Network Monitoring 3082 Monitor your network on the go with PRTG and apps for iOS, Android (including BlackBerry devices), and Windows Phone.
System Administration Program	PRTG Administration Tool on Core Server System 3135 Used to configure basic core server settings, such as administrator login, web server IPs and port, probe connection settings, cluster mode, system language, and more. PRTG Administration Tool on Remote Probe System 3157 Used to configure basic probe settings such as name of the probe, IP and server connection settings, and more.

Core Server

The core server is the heart of your PRTG system and performs the following processes:

- Configuration management for monitoring objects (for example, servers, workstations, printers, switches, routers, virtual machines, and many more)
- Management and configuration of the connected probes
- Cluster management
- Database for monitoring results
- Notification management including a mail server for email delivery
- Report generator and scheduler
- User account management
- Data purging (culling data that is older than 365 days, for example)
- Web server and API server

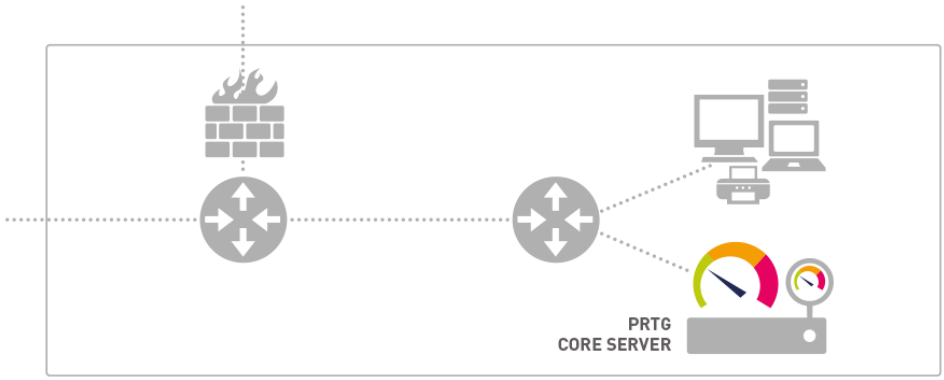
In a cluster 116, the current master node is responsible for all of these tasks.

The built-in, fast, and secure web server (no additional IIS or Apache is required) supports HTTP as well as secure HTTPS (via SSL). It serves the web interface when you access it via a browser and also answers PRTG Application Programming Interface (API) calls (for example, for user scripts or the Enterprise Console).

Core server and probe(s) are configured as Windows services that are permanently run by the Windows system without the requirement for a logged-in user.

Probe(s)

On a probe, PRTG performs the actual monitoring via the sensors created on a device (for example, computer, router, server, firewall). The probe receives its configuration from the core server, runs the monitoring processes, and delivers monitoring results back to the core server. On every system running a PRTG core server, there is always a local probe running on the same machine.



PRTG Core Server and Local Probe Monitoring a Local Area Network

Click here to enlarge: http://media.paessler.com/prtg-screenshots/probes.png

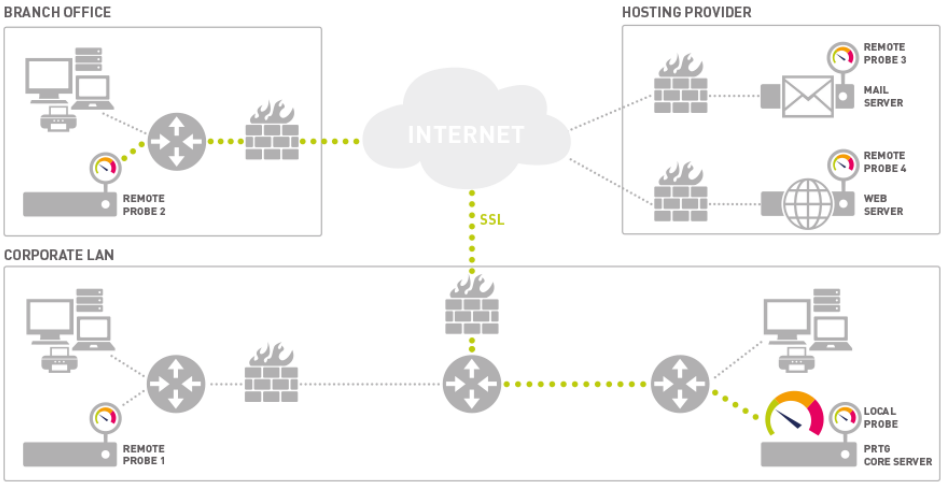
The actual monitoring is performed by PRTG probe processes that run on one or more computers. During installation, the system automatically creates the **Local Probe**. In a single-probe installation—which is the default setup—the local probe performs all monitoring.

The PRTG on premises core server with the local probe inside the corporate LAN (bottom-right in the figure above) is able to monitor services and servers in the entire Local Area Network (LAN). For PRTG on demand you need at least one remote probe installation in your network for this purpose.

Core server and probe(s) are configured as Windows services that are permanently run by the Windows system without the requirement for a logged-in user.

You can create additional **Remote Probes** to achieve monitoring of multiple locations, for LAN monitoring with PRTG on demand, or for several other scenarios. They use Transport Layer Security (TLS)-secured connections to the core and allow you to securely monitor services and systems inside remote networks that are not openly accessible or are secured by firewalls. For more information, please see **Remote Probes and Multiple Probes** 3195.

For more information, see this video tutorial on our website: Distributed Monitoring with PRTG using Remote Probes



Remote Probes: Monitoring of Several Scenarios

Click here to enlarge: http://media.paessler.com/prtg-screenshots/remote_probes_en.png

In a cluster setup 116, a cluster probe runs on all nodes. This is the additional **Cluster Probe**. All devices that you create on it are monitored by all nodes in the cluster, so data from different perspectives is available and monitoring for these devices always continues, also if one of the nodes fails.

PRTG Mini Probes allow you to create small probes on any device (not just on Windows systems). You can implement mini probes to gather monitoring data exactly like you need it and you can create them on any platform. For more information, see the **Mini Probe API** definition in the PRTG web interface (see section **Application Programming Interface (API) Definition** 3174).

PRTG automatically monitors system health of its own core server and of each probe to discover overloading situations that may distort monitoring results. To monitor the system status of the probe computer, PRTG automatically creates a few sensors. These include **Core Health** 602 and **Probe Health** 1378, **System Health** 2321, **Cluster Health** 589, disk free 2573, and bandwidth 2441 sensors for all installed network cards, as well as a **Common SaaS sensor** 594 that checks the availability of widely used SaaS providers.

We recommend that you keep these sensors, but you can optionally remove all except the **Health** sensors. They measure various internal system parameters of the probe system hardware and the probe's internal processes and computes a resulting value. Frequent or repeated values below 100% should be investigated. Please check the channels 166 of a particular sensor for details.

More

Looking for a comprehensive PRTG training? PRTG e-learning in 9 modules:

- https://www.paessler.com/support/training/e-learning

Video Tutorials: Learn about the PRTG Network Monitor basics on the Paessler video tutorials page.

- https://www.paessler.com/support/videos/prtg-basics

Video Tutorial: Distributed Monitoring with PRTG using Remote Probes

- https://www.paessler.com/support/videos/prtg-basics/distributed_monitoring

Video Tutorial: What is a sensor?

- https://www.paessler.com/support/videos/prtg-basics/what-is-a-sensor

Video Tutorial: PRTG User Interfaces

- https://www.paessler.com/support/videos/prtg-basics/user-interfaces

5.2 Clustering

A PRTG Cluster consists of two or more installations of PRTG 84 that work together to form a high availability monitoring system. The objective is to reach true 100% uptime for the monitoring tool. By clustering 3212, the uptime will no longer be degraded by failing connections because of an internet outage at a PRTG server's location, failing hardware, or because of downtime due to a software update for the operating system or PRTG itself.

This feature is not available in PRTG on demand.

How a PRTG Cluster Works

A PRTG cluster consists of one **Primary Master Node** and one or more **Failover Nodes**. Each node is simply a full installation of PRTG which could perform the whole monitoring and alerting on its own. Nodes are connected to each other using two TCP/IP connections. They communicate in both directions and a single node only needs to connect to one other node to integrate into the cluster.

During normal operation the **Primary Master** is used to configure devices and sensors (using the web interface 136 or Enterprise Console 3028). The master automatically distributes the configuration to all other nodes in real time. All nodes are permanently monitoring the network according to this common configuration and each node stores its results into its own database. This way, the storage of monitoring results is also distributed among the cluster (the downside of this concept is that monitoring traffic and load on the network is multiplied by the number of cluster nodes, but this will not be a problem for most usage scenarios). The user can review the monitoring results by logging into the web interface of any of the cluster nodes in read-only mode. Because the monitoring configuration is managed centrally, it can only be changed on the master node, though.

By default, all devices created on the **Cluster Probe** are monitored by all nodes in the cluster, so data from different perspectives is available and monitoring for these devices always continues, even if one of the nodes fails. In case the **Primary Master** fails, one of the **Failover Nodes** takes over the master role and controls the cluster until the master node is back. This ensures a fail-safe monitoring with gapless data.

If you use remote probes in a cluster, each probe connects to each node of your cluster and sends the data to all cluster nodes, the current primary master as well as the failover nodes. You can define **Cluster Connectivity** of each probe in the **Probe Administrative Settings** 330 .

During the outage of a node, it will not be able to collect monitoring data. The data of this single node will show gaps. However, monitoring data for this time span is still available on the other node(s). There is no functionality to actually fill in other nodes' data into those gaps.

If downtimes or threshold breaches are discovered by one or more nodes, only one installation, either the Primary Master or the Failover Master, will send out notifications (via email, SMS text message, etc.). Thus, the administrator will not be flooded with notifications from all cluster nodes in case failures occur.

More than 5,000 sensors per cluster are not supported.

Set Up a PRTG Cluster

For detailed information, see **Failover Cluster Configuration** 3212.

More

Knowledge Base: What's the Clustering Feature in PRTG?

- https://kb.paessler.com/en/topic/6403

Video Tutorial: Cluster in PRTG — This is how it works

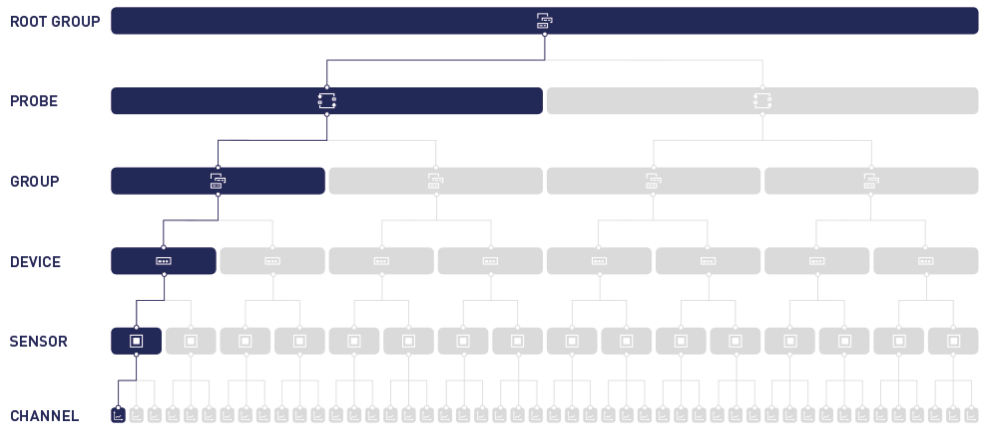
- https://www.paessler.com/support/videos/prtg-advanced/cluster-animation

Video Tutorial: How to set up a PRTG cluster

- https://www.paessler.com/support/videos/prtg-advanced/how-to-set-up-a-cluster

5.3 Object Hierarchy

All objects in a PRTG monitoring configuration are arranged in a treelike hierarchy to create an easy to navigate list and to give the user the possibility to arrange them in groups that monitor similar devices, services, or particular locations. This hierarchical order is also used to define common settings for larger groups of objects, for example, settings of the **Root** group apply by default to all other objects underneath (see section **Inheritance of Settings** 122).



Object Hierarchy in PRTG

Click here to enlarge: http://media.paessler.com/prtg-screenshots/object-hierarchy_en.png

The figure shows the object hierarchy in PRTG:

- **Root** group contains all objects in your setup; all probes are directly under the root node.
- A **Probe** contains one or several groups.
- A **Group** contains one or several devices.
- A **Device** represents a physical or virtual component in your network that is reachable via an IP address. Several sensors are attached to one device.
- A **Sensor** monitors one single aspect of a device and has at least one channel.
- A **Channel** tracks one specific data stream and displays it as part of a sensor.

Root Group

The **Root** group is the topmost instance in PRTG. It contains all other objects in your setup. Using the inheritance 122 mechanism, we recommend that you adjust the default settings for the Root group 294. This will make configuration easier later on, because all other objects then inherit these standard settings by default. Thus, you will not have to set up the same configuration for each object anew.

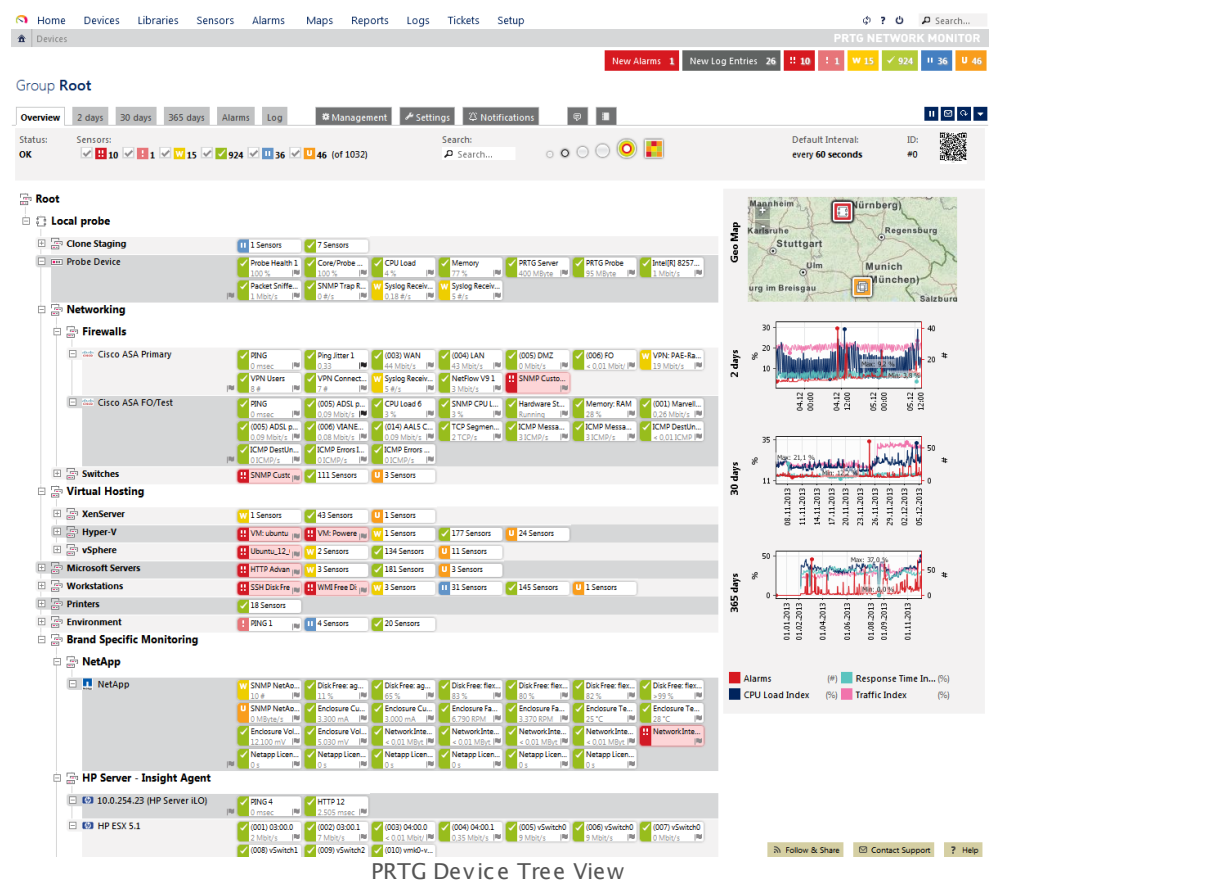
Probe

Each group (except the **Root** group) is part of a **Probe**. This is the platform where the monitoring takes place. All objects configured below a probe will be monitored via that probe. Every PRTG core installation automatically installs a **Local Probe** service. You can add additional probes and remote probes to your configuration to include remote devices from outside your network into the monitoring (see section Multiple Probes and Remote Probes 3195). In a cluster, there is an additional **Cluster Probe** running on all nodes. Devices on the cluster probe are monitored by all nodes of the cluster, so data from a different perspective is available and monitoring for these devices will always continue, even if one of the nodes fails.

Group

On each probe, there are one or more **Groups**, which serve merely structural purposes. Use groups to arrange similar objects so that they inherit the same settings. To a group, you add devices. You can arrange your devices in different nested groups to reflect the structure of your network.

Find below a sample configuration: A device tree with local probe, several groups, devices and their sensors.



PRTG Device Tree View

Device

You can add **Devices** that you want to monitor to each probe or group. Each device in your PRTG configuration represents a real hardware or virtual device in your network. These can be, for example:

- Web or file server
- Client computer (Windows, Linux, or Mac OS)
- Router or network switch
- Almost every device in your network that has its own IP address

Sometimes you may want to add the same device in PRTG several times to receive a better overview when using a large number of sensors for very detailed monitoring, or to use different device settings for different groups of sensors. In PRTG you can simply add multiple devices with the same IP address or DNS name. The sensors on all of these PRTG devices will then query the same real hardware device in your network.

PRTG additionally adds a so called **Probe Device** to the local probe. This is an internal system device. It has access to the computer where the probe is running and monitors its health parameters with several sensors running on it.

To get a better and more detailed picture about your devices, PRTG automatically analyzes the devices that you add and recommends appropriate sensor types 385 on the device overview tab 166. In the **Recommended Sensors** table, click the **Add Sensors** button in the corresponding table row to create recommended sensor types with one click.

You can turn off the sensor recommendation in **System Administration—Monitoring** 2959.

Sensor

On each device you can create a number of **Sensors.** Every sensor monitors one single aspect of a device. This can be, for example:

- One network service like SMTP, FTP, HTTP, etc.
- One network switch port's traffic
- CPU load of a device
- Memory load of a device
- Traffic on one network card
- One NetFlow device
- System health of a device
- Other content (for example, of databases, mails, HTTP, XML, files, etc.)
- etc.

For more information, see this video tutorial: What is a sensor?

Channel

Every sensor has a number of **Channels** through which it receives the different data streams. The available channels depend on the type of sensor. One sensor channel can contain, for example:

- **Downtime** and **uptime** of a device
- **Traffic in** of a bandwidth device (for example, a router)
- **Traffic out** of a bandwidth device (for example, a router)
- **Traffic sum** of a bandwidth device (for example, a router)
- **WWW traffic** of a NetFlow device
- **Mail traffic** of a NetFlow device
- **Other traffic** of a NetFlow device
- **CPU load** of a device
- **Loading time** of a web page
- **Download bandwidth** of a web page
- **Time to first byte** of a web page
- **Response time** of a Ping request to a device
- **Response time** of a Remote Desktop service
- etc.

More

Video Tutorial: What is a sensor?

- https://www.paessler.com/support/videos/prtg-basics/what-is-a-sensor

5.4 Inheritance of Settings

The hierarchical tree [118] does not only help organize the devices and keep everything neat and tidy. There is also an important aspect involved that we call inheritance. To ensure administration is quick and easy—especially for large monitoring setups—certain settings are inherited from the higher level. For example, you can change the monitoring interval for all sensors by editing the interval setting of the topmost **Root** group (unless no other setting is defined below).

Settings are Inherited to Child Objects

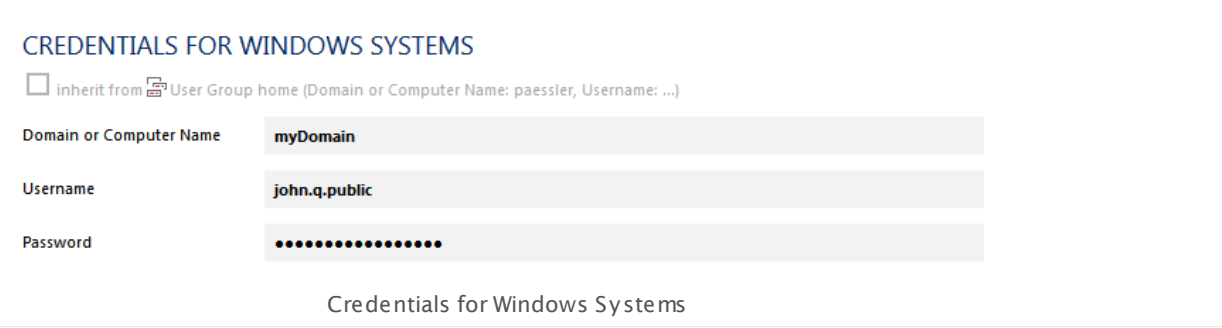
You can override this inheritance on any level of the hierarchy by setting a different value for a specific probe, group, device, or sensor. All objects below will inherit these new settings; object settings from levels above will not be affected.

Settings that are inherited among all objects include:

- Monitoring interval
- Notification triggers
- Authentication settings for several systems
- Compatibility settings (for certain types of sensors)
- Channel and unit configuration
- User access rights [129]
- Tags [124]
- Paused status: If an object is paused by the user, or a schedule, all sensors on it are paused as well
- etc.

There is one exception for devices and sensors: The **IP address** or **DNS name** of a device and compatibility settings are always inherited by sensors and cannot be changed on sensor level.

The actual overriding of the parent's settings takes place in an object's settings: Remove the check mark symbol at the beginning of the respective line **inherit from [parent object]**. For example, the screenshot below shows Windows systems credentials settings after removing the check mark symbol.



Credentials for Windows Systems

Default Values Set in Root Group

For all settings (except passwords), PRTG already includes a set of default values so you can get started with the software immediately. For example, the following settings will be inherited by all sensors from the **Root** group:

- Default monitoring interval of one minute
- SNMP version 1 with community string set to **public** (default values for most devices)
- Dependency type **Use parent**
- etc.

You may need to change some of the default entries as you become used to the interface. However, these settings will initially suffice for most situations.

Before sensor setup, please review the **Root** group settings and set the default values to suit your setup. This should include the credentials for the types of systems in your network that you want to monitor (Windows, Linux, virtual servers, etc.).

See section Root Group Settings 294 for more details.

Inheritance of Notification Triggers

If you add notification triggers at probe, group, or device level, these will also be inherited to all sensors underneath, unless you break the inheritance manually.

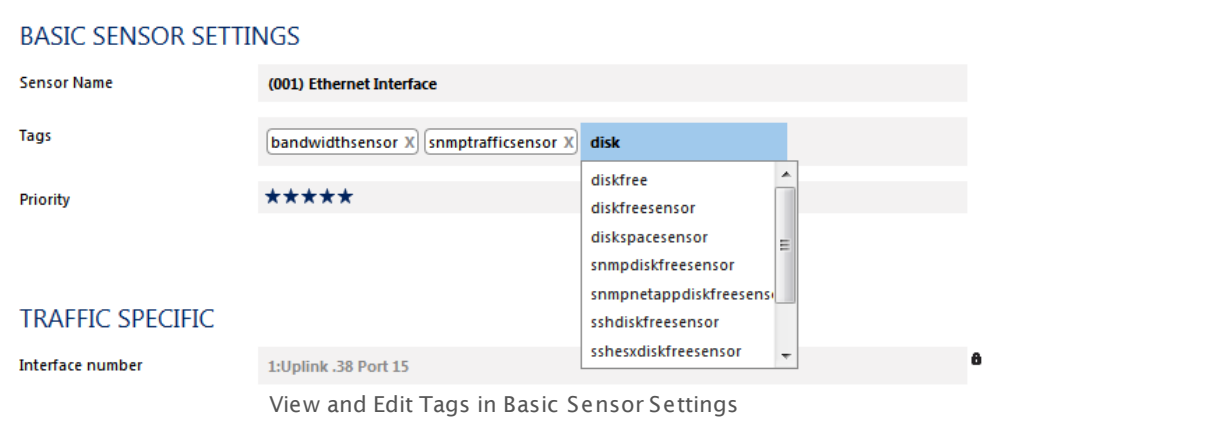
See section Sensor Notifications Settings 2791 for details.

5.5 Tags

For every object in your PRTG setup, you cannot only name objects, you can also define tags in the object settings 188 to additionally mark an object as a member of certain categories. Although some tags are automatically predefined when adding objects 267, you are completely free in which tags you want to add. For example, you can mark all of the bandwidth sensors that are especially important for you with the tag bandwidth_important.

Later on, you can view lists of objects with certain tags (helpful for multi-edit 2814 of settings), or select sensors via tags when creating reports 2862. A smart arrangement of tags can be a huge time saver. The keys enter, space, or comma confirm a tag.

You can also change tags for several objects simultaneously using the multi-edit 2814 function.



View and Edit Tags in Basic Sensor Settings

Tags are Inherited

The tags in the settings of an object are automatically inherited 122 by all other objects underneath in the **Object Hierarchy** 118. You can view inherited tags in section **Parent Tags** in the settings of a sensor 120, device 120, or group 119. So, for example, a device with the tag myExampleTag automatically passes on this tag to all sensors that you add to it. These sensors appear in lists whenever you search for myExampleTag. This is useful, for example, when you add sensors by tag in reports 2862 settings, because you do not have to tag every single sensor manually.

Inheritance for tags cannot be disabled.

Filtering with Tags

You can use tags to filter table lists 207 for specific objects, or to add sensors to **Libraries** 2845 and **Reports** 2862. For example, you can restrict the sensors overview page 236 to the sensors that have the tag bandwidth_important. You can also use more than one tag to filter for monitoring objects like sensors.

When filtering with tags, you can also use plus (+) and minus (-) signs in front of the tags to include or exclude them:

- Tags with + must exist for an object to be shown
- Tags with – must **not** exist for an object to be shown
- At least one tag of the tags without either a + or – must exist on an object

The filter shows an object only if all three conditions are true. The order of the tags in a tag field does not matter.

For example, if you enter –windows into a tag field, all sensors/devices that do not have "windows" as tag are shown. With +windows or windows you filter for objects that are tagged with "windows".

You can use more than one logical operator in a tag field: For example, if you enter +netflow –bandwidth_important into a tag field, the corresponding list, library, or report includes all sensors that are tagged with "netflow" but not with the tag "bandwidth_important". If you enter netflow bandwidth_important, a sensor has to be tagged with "netflow" or "bandwidth_sensor" or both to be affected.

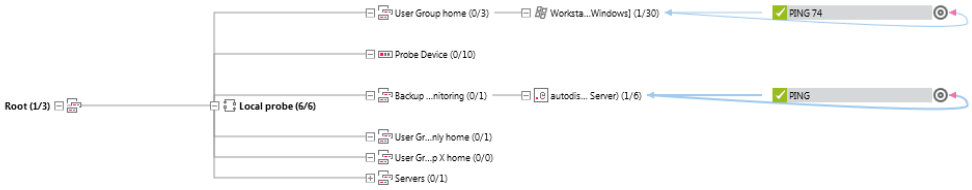
5.6 Dependencies

Using dependencies, you can pause sensor monitoring based on the status [163] of another sensor to avoid false alarms and incorrect downtime recording. A dependency stops the monitoring of one sensor or a set of sensors as soon as a specific sensor is in **Down** status or in **Paused** status caused by another dependency. This means, for example, that you can stop monitoring remote network services when the corresponding firewall is down due to connection problems.

When using the auto-discovery [249] function, the **Ping Sensor** [1319] on a device is by default set as the master object for this device. This means that monitoring for the entire device is paused if the Ping sensor is in **Down** status or in **Paused** status caused by another dependency. Usually, it makes little sense to monitor any other parameters while the **Ping** sensor indicates that the device can't even be reached.

You do not trigger a status change by dependency if you manually pause a master object or if you pause it by schedule [127].

To view the list of dependencies, choose **Devices** | **Dependencies** and the corresponding dependencies path from the main menu [233]. From there you can also access the **Dependencies Graph** [2822] that visualizes all dependencies within your network.



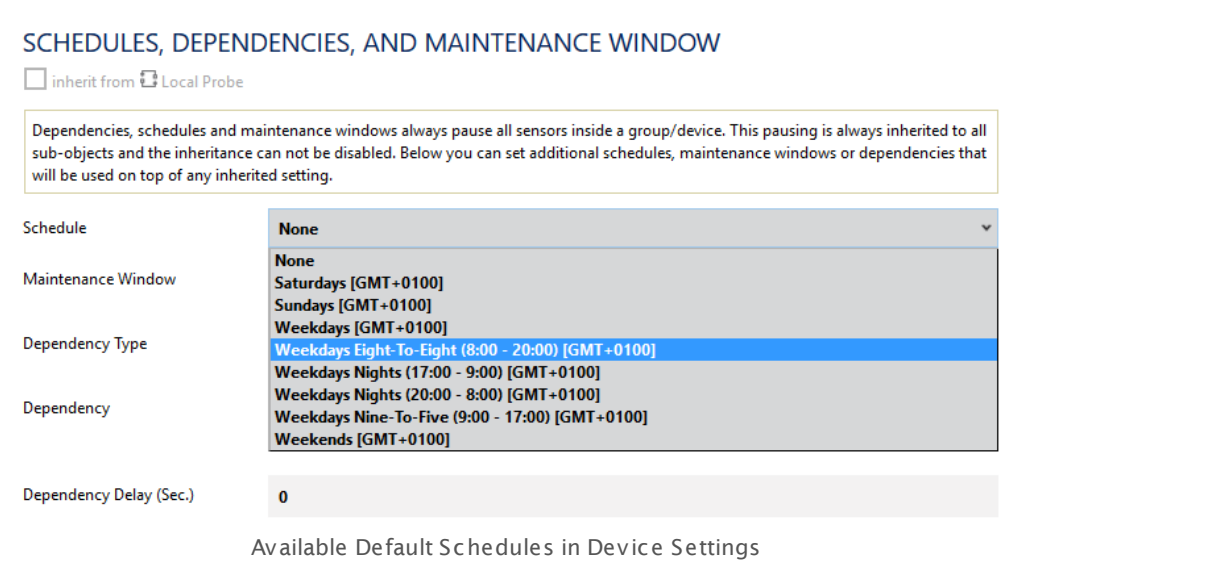
Dependencies Graph

For more information about the dependency settings, please see the settings of the object [188] you want to set a dependency for, section **Schedules, Dependencies, and Maintenance Window** [378] respectively.

5.7 Scheduling

With the help of schedules you can pause [214] the monitoring of certain objects automatically for a certain time, for example, on Sundays between 4 and 8 a.m. A paused sensor will not collect monitoring data, will not change its status, and will not trigger any notifications [128]. You can also pause monitoring for planned system maintenance time spans to avoid false alarms. You can apply different schedules to every object. Schedules are also used for reports and notifications.

If you pause a master object by schedule (or manually), you do not trigger a status change by dependency [126].



Available Default Schedules in Device Settings

Schedules are user account specific. To change the default pre-defined schedules or to add your own schedule, please see **Account Settings—Schedules** [2938] section.

If you use failover clustering with nodes in different timezones, scheduling applies at the local time of each node. For more information, please see section **Failover Cluster Configuration—Before Getting Started** [3213].

5.8 Notifying

PRTG Network Monitor keeps the administrator or other responsible persons informed about the current status of the network. There are several methods how the administrator can stay up to date.

Notifications

This is the most powerful information tool. Whenever PRTG discovers downtime, an overloaded system, threshold breaches (for example, a disk runs full), or similar situations, it can send a notification. Notifications use various methods with which you can be notified (for example, email 2922, SMS 2916, push messages 2923, and others). After creating notifications in the system settings, you can select them on the notifications tab of probes, groups, devices, and sensors, as well as on the root group.

See **Notifications** 2829 section for more details and **Setting Up Notifications Based on Sensor Limits: Example** 2832 for a step-by-step guide.

Limits

In a sensor channel's settings 2782, you can set limits to change the status of the sensor when certain limits are breached. This way, you can set, for example, a traffic sensor (typically never in an error status) to **Down** status whenever bandwidth values are measured that you consider critical. This sensor will then show up in the alarms list.

Alarms

The alarms list shows all sensors that are currently in a **Down**, **Down (Acknowledged)**, **Warning**, or **Unusual** status. This is useful for keeping track of all irregularities in your network. In the table list, you can re-sort the items by clicking on the column's header items. See **Alarms** 190 section for more details.

Logs

In the logs list, the log file with all monitoring events is shown. In a typical setup, a huge amount of log data is produced. As the activity of every single object is minuted, you can use this data to check exactly if your setup works as expected. See **Logs** 198 section for more information.

Tickets

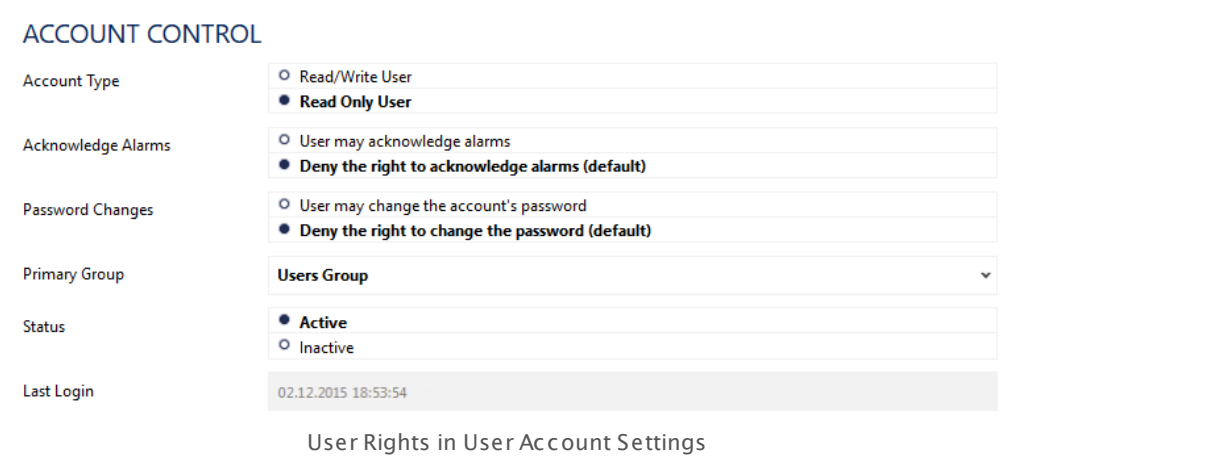
The tickets list shows items with important system information or action steps for the administrator to take. You should view every ticket and take appropriate actions. By default, an email is sent to the administrator for every new ticket that is created by the system or another user. If a ticket is assigned to a specific user, this user will get an email by default. See **Tickets** 200 section for more information.

5.9 User Access Rights

Define which user can access what in your PRTG Network Monitor installation and manage all user rights with the access rights system of PRTG.

The default administrator can be the only user of a PRTG installation, but can also create a nearly unlimited number of other users. Individual users are organized in a nearly unlimited number of user groups. Each user group can separately have access rights for each individual object 118 in your PRTG device tree (except for sensor channels). Objects can also inherit 122 access rights according to the hierarchic structure of the device tree.

In addition, every user has specific rights: There are administrator users, read/write users, and read-only users. You can define these settings in System Administration—User Accounts 2975. Via these tools, you can create an access rights management that allows you to specify exactly what users will be able to see and edit and what they will not be able to access.



User Rights in User Account Settings

Individual user rights, in combination with the access rights of the group(s) they belong to, determine the access rights to certain objects in the device tree. This means that group membership specifically determines what a user is allowed to do and which objects the user will see when logged in.

The actual access rights for each object in the device tree can be defined in the object's settings. You can define different access rights for all sensors, devices, groups, or probes via the corresponding Context Menus 215 or in the Object Settings 188.

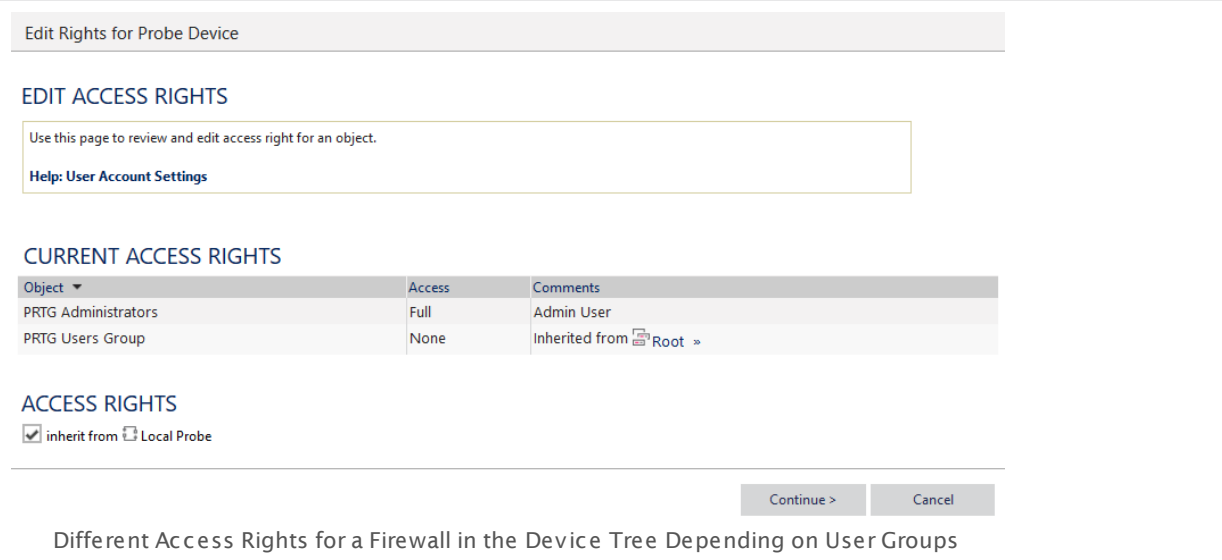
Access Rights Overview

The following classes of access rights for objects are available in hierarchical order as they can be given to user groups (lowest rights to highest rights):

- **None**: The object will not be displayed to the users of the group; no logs, no tickets, no alarms regarding this object will appear.
- **Read**: You can only see monitoring results and change your own password if allowed by your administrator.

- **Write**: You are allowed to review monitoring results and edit settings. In addition, you can add objects to and delete them from the device tree.
- **Full**: Review monitoring results, edit settings, and edit access rights. In addition, you can add objects to and delete them from the device tree.
- **Admin rights**: If a user group has administrator rights, all options are available, including creating users, creating user groups, and deleting objects from the device tree. Users in the administrator user group always have maximum access rights to all objects and will never have access restrictions.

Access rights that are defined locally on an object, for example, on a device, override inherited rights. For a certain object, the highest directly defined access right applies for a user group. If there is no access right set directly on an object, the next higher object level will be checked for access rights. This process is repeated until defined access rights are found to be inherited 122 or there is no higher object level.



Different Access Rights for a Firewall in the Device Tree Depending on User Groups

Please see the table below for which user rights apply when. Column headings show access rights of user groups for objects in the device tree; line headings show the type of user.

Users are either members in PRTG user groups or in Active Directory Domain user groups. They cannot be members in both. We recommend that you use only one type of user group (either PRTG or Active Directory) to minimize your administration effort.

	▪ **PRTG User Group** ▪ **Domain User Group**	▪ **PRTG User Group** ▪ **Domain User Group**	▪ **PRTG User Group** ▪ **Domain User Group**	▪ **PRTG System Administrator** ▪ **Domain Administrator**
	READ ACCESS	READ/WRITE ACCESS	FULL ACCESS	
▪ **PRTG User Read Only**	Read-only rights	Read-only rights	Read-only rights	Admin rights

- **Domain User Read Only**
- **PRTG User Read/Write** Read-only rights Read/write rights Full access Admin rights
- **Domain User Read/Write**

- **Users in an administrator group** always have administrator access rights, no matter what access rights have been defined for an object.
- **Read-only users** just have reading permission, no matter what access rights their group has. Users who are members of an administrator group are an exception. Read-only users can change their own passwords in their user account settings 2975, if the administrator has enabled them to do so.
- **Read/write users** in a group with full access to a given object have full access rights to this object only.
- If a user is in **more than one group**, access rights of the user group with the highest rights apply .
- Administrator rights can only be granted by membership in the **administrator group**.

For more information about defining access rights, please see the following sections:

- System Administration—User Accounts 2975
- System Administration—User Groups 2982

For information about connecting PRTG to an existing Active Directory, see Active Directory Integration 3171.

5.10 Data Reporting

With **Reports** 2862 you can analyze and review monitoring data for specific time spans. There are several ways to create data reports in PRTG for your individual needs.

View Historic Data

To get a report for a single sensor, there is a function included to review historic data in PRTG. It allows you to generate reports and charts for a single sensor's data. See the **Historic Data Reports** 175 section for more information.

Generate Reports

You can use the sophisticated reports machine included in PRTG to create comprehensive and detailed reports for all monitoring data. See the **Reports** 2862 section for more information.

Export Data Using the API

You can also export all monitoring raw data to XML or CSV files and generate your own reports using any third-party software. See the **Using the PRTG API (Application Programming Interface)** 3174 section for more information.

Make Data Available

You can make monitoring data available to other persons using a special user with read-only rights (see the **User Access Rights** 129 section), or you can create public or semi-public HTML pages with monitoring data using the Maps feature. See the **Maps** 2885 section for more information.

Bill Customers

You can also create custom billing reports based on PRTG's monitoring data, using the open source **Billing Tool** for PRTG.

For details and download, please see the Paessler website: Billing Tool

More

- **Data Storage** 3226

Paessler Website: Billing Tool

- https://www.paessler.com/tools/billingtool

5.11 IPv6

PRTG supports the IPv6 protocol for most sensor types. You can choose whether you want PRTG to query data from your network devices via an IPv4 or IPv6 connection. Indicate your preference in the **Device Settings** 360 of each device. The sensors you add to the device will use the protocol you have indicated.

In the **Outgoing IP Settings** of the **PRTG Administration Tool** 316, you can additionally choose which IPv6 address will be used for outgoing monitoring requests. The the same option is also available for IPv4.

Not all sensor types are IPv6 compatible. You can see which sensors support IPv6 in the **Add Sensor** 288 dialog. Incompatible sensors are not selectable on IPv6 devices.

The **Cloud HTTP Sensor** 571 and the **Cloud Ping Sensor** 580 do not support IPv6 although you can add them to IPv6 devices. You will receive an error message if you do so.

Part 6

Ajax Web Interface—Basic Procedures

6 Ajax Web Interface—Basic Procedures

The Ajax-based web interface is your access to PRTG. Use it to configure devices and sensors, to set up notifications, as well as to review monitoring results, and to create reports. This web interface is highly interactive and uses Asynchronous Java Script and XML (AJAX) to deliver a powerful and easy-to-use user experience. While you are logged in 138, the PRTG web interface continuously refreshes the data on the screen (via Ajax calls) so it always shows the current monitoring results (you can set 2975 refresh interval and method individually).

Because the web interface works as a Single Page Application (SPA), you rarely see a full page refresh to avoid a performance impact due to redundant processing. Only single page elements are refreshed when necessary. The AJAX web interface shows all object setting dialogs as pop-up layers, so you never lose the current context. This speeds up the user experience appreciably and makes the configuration of objects in PRTG comprehensible. The responsive design of the web interface ensures that it always adjusts to the size of your screen so that you see more information at a glance.

The following sections introduce the features and concepts of the Ajax Graphical User Interface (GUI).

If you are interested in a video overview of the PRTG web interface, see this video tutorial: The PRTG Web User Interface—Overview

Ajax Web Interface—Basic Procedures—Topics

- Login 138
- SSL Certificate Warning 142
- Welcome Page 145
  - Customer Service 149
- General Layout 151
- Sensor States 163
- Review Monitoring Data 166
- Compare Sensors 172
- Historic Data Reports 175
- Similar Sensors 180
- Recommended Sensors 184
- Object Settings 188
- Alarms 190
- System Information 193
- Logs 198
- Tickets 200
- Working with Table Lists 207

- Object Selector 210
- Priority and Favorites 211
- Pause 214
- Context Menus 215
- Hover Popup 230
- Main Menu Structure 231

Other Ajax Web Interface Sections

- Ajax Web Interface—Device and Sensor Setup 248
- Ajax Web Interface—Advanced Procedures 2804

Related Topics

- Enterprise Console 3028
- PRTG Apps for Mobile Network Monitoring 3082

6.1 Login

For PRTG on premises instances, you can log in to the web interface once the PRTG core server is installed [84]. In your browser, load the IP address or DNS name of the computer PRTG is installed on and log in using the **Login** button. For PRTG on demand instances, open your registered PRTG on demand domain and log in to the web interface.

You can look up and change the web server settings of PRTG on premises instances at any time using the **PRTG Administration Tool** [3136] Windows application on the system where the PRTG core server is installed. Especially when accessing PRTG from the internet, you should use an SSL-encrypted connection. You can easily switch to SSL using the **Yes, switch to SSL** button shown on the welcome screen.

Loading the Web Interface

In a web browser window, please enter the IP address or URL of the system PRTG is installed on. When using a cluster, please connect to the primary master node. You can also double-click on the **PRTG Network Monitor** icon on the desktop of the system PRTG is installed on. If you are using PRTG on demand, enter the URL of your instance, for example myfirstdomain.my-prtg.com to access the web interface with a supported browser [30].

If you run PRTG on localhost, please do not use the DNS name http://localhost to log in to the web server, as this may considerably slow down the PRTG web interface. Please use your local IP address or http://127.0.0.1 instead.

If you see a certificate warning in your browser, you can usually just confirm it. For more information please see **SSL Certificate Warning** [142].

Login Screen PRTG on Premises

This only applies to PRTG on premises instances, not to PRTG on demand.

After loading the web interface, the login screen is visible. You can either login as default administrator or as any other PRTG user. As PRTG Administrator user you can use all functionalities of the web interface. Administrators can create additional users [2975] with administrator rights or with more restricted privileges (for example, read-only users).

PRTG Login Screen

Login as Default Administrator (First Time Login)

This only applies to PRTG on premises instances, not to PRTG on demand.

When logging in for the first time, login name and password for the default administrator login are both **prtgadmin**. PRTG automatically fills in the default credentials and shows the password in plain text.

After login you should change the default password. To do so, go to **Setup | Account Settings | My Account** and specify a new password in section **User Account**.

If you are not logged in into the web interface, you can change the credentials for this default user account any time in the **PRTG Administration Tool** 3146 Windows application.

If you enter another login name or change your password, the password is no longer shown in plain text.

Login as PRTG User

This only applies to PRTG on premises instances, not to PRTG on demand.

If you have received user credentials from your administrator, please enter them here to log in. Also, when using other administrator credentials, please enter them here.

Login Options

This only applies to PRTG on premises instances, not to PRTG on demand.

- **Login**: Log in to the fully featured Ajax web interface which is the standard interface. We recommend that you use this option for PRTG whenever possible. It offers the full functionality of PRTG. Use Google Chrome 57 or later (recommended) or Mozilla Firefox 52 or later for best performance. In some browsers, the Ajax option is not shown, for example, in old browser versions.

Although you can log in using Microsoft Internet Explorer 11, the Ajax web interface might not be fully compatible with Internet Explorer! When using Microsoft Internet Explorer 11, please set the security level to **Medium-high** (or lower) and make sure no **Compatibility View** is enabled!

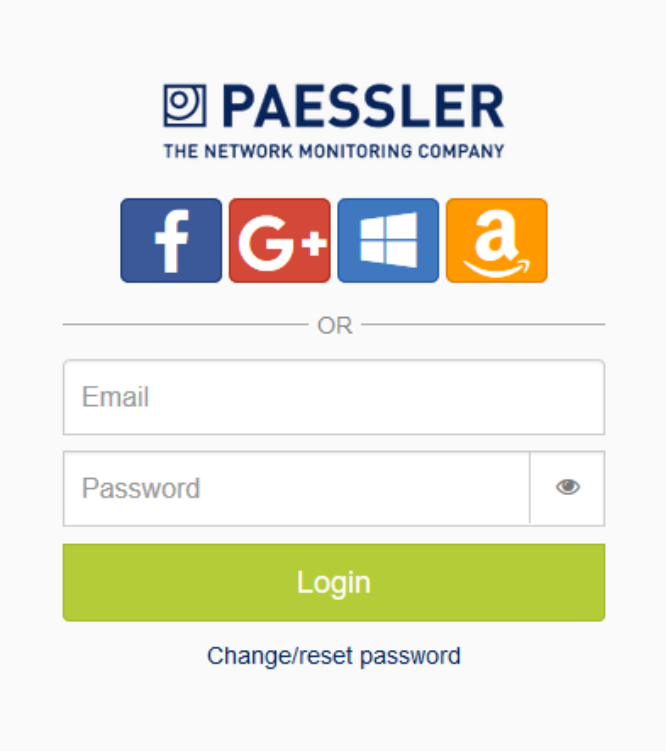
- **Download Client Software (optional, for Windows, iOS, Android)**: This option opens the PRTG download page 3018 in the web interface. You can optionally download the native Windows application **Enterprise Console** to the desktop. You have to install 3026 it on the client computer before use. The Enterprise Console 3028 provides full functionality. However, for some functions the Ajax Web GUI opens. As an additional feature, the Enterprise Console can view data of several independent PRTG core installations in one single application.
  You can also access pages on the Paessler website from here, for information about the PRTG apps 3082 PRTG for iOS, PRTG for Android and PRTG for Windows Phone. These pages also contain the download links to the corresponding app stores.
  Also, when using this download option, your name and password (or the default credentials) are required for login!

Only Google Chrome 57 or later (recommended) and Mozilla Firefox 52 or later are fully compatible with the Ajax web interface.

Enter specific credentials or use the default credentials, which are automatically filled in, and click the **Login** button to proceed to the PRTG web interface.

Login Screen PRTG on Demand

BETA For PRTG on demand instances, load the PRTG web interface with the domain you have registered at https://my-prtg.com and use the login method that you chose when signing up.



PRTG on Demand Login Screen

To log in with your Facebook, Google+, Windows, or Amazon, click the respective button. A popup window appears where you can enter your credentials for the respective account. Alternatively, you can log in with the email and password that you chose when signing up. If you have received an invitation to PRTG on demand, click the link in the invitation and proceed to log in.

Recover Password

If you cannot remember your PRTG on premises password, click the **Forgot password?** link. The **Password Recovery** page opens. Enter your **Login Name**, click **Request a New Password**, and PRTG will send a new password to the primary email address of this PRTG user account. The **Need Help?** link will open the current manual page.

If you cannot remember your PRTG on demand password, click the **Change/reset password** link. You are then asked to enter your email address. Click **Change/reset password** again and PRTG will send you an email to reset your password.

6.2 SSL Certificate Warning

If you use PRTG on premises outside your internal LAN, especially when you use it on the internet, you should switch the internal web server to use SSL 2946. After doing so, your browser shows a certificate warning because the certificate that comes with PRTG cannot be signed by a valid authority. Anyway, the connection to your PRTG web server is secured via SSL, and you can confirm the claimed security risk.

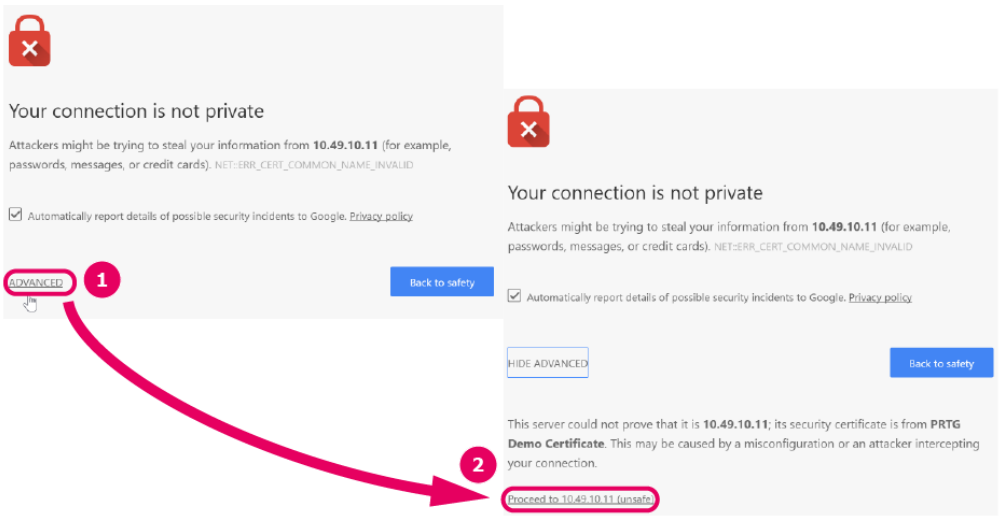
Every browser shows a slightly different certificate warning. The necessary steps are similar for every browser, with a few small differences:

- Google Chrome 142
- Mozilla Firefox 143
- Internet Explorer 143
- Other 144

You can avoid these browser warnings by using your own trusted SSL certificate 3228 with PRTG. For this purpose we provide the freeware tool PRTG Certificate Importer 3228.

Google Chrome

In **Google Chrome**, click **Advanced** and then **Proceed to [yourPRTGserver] (unsafe)** every time you call the PRTG web interface.

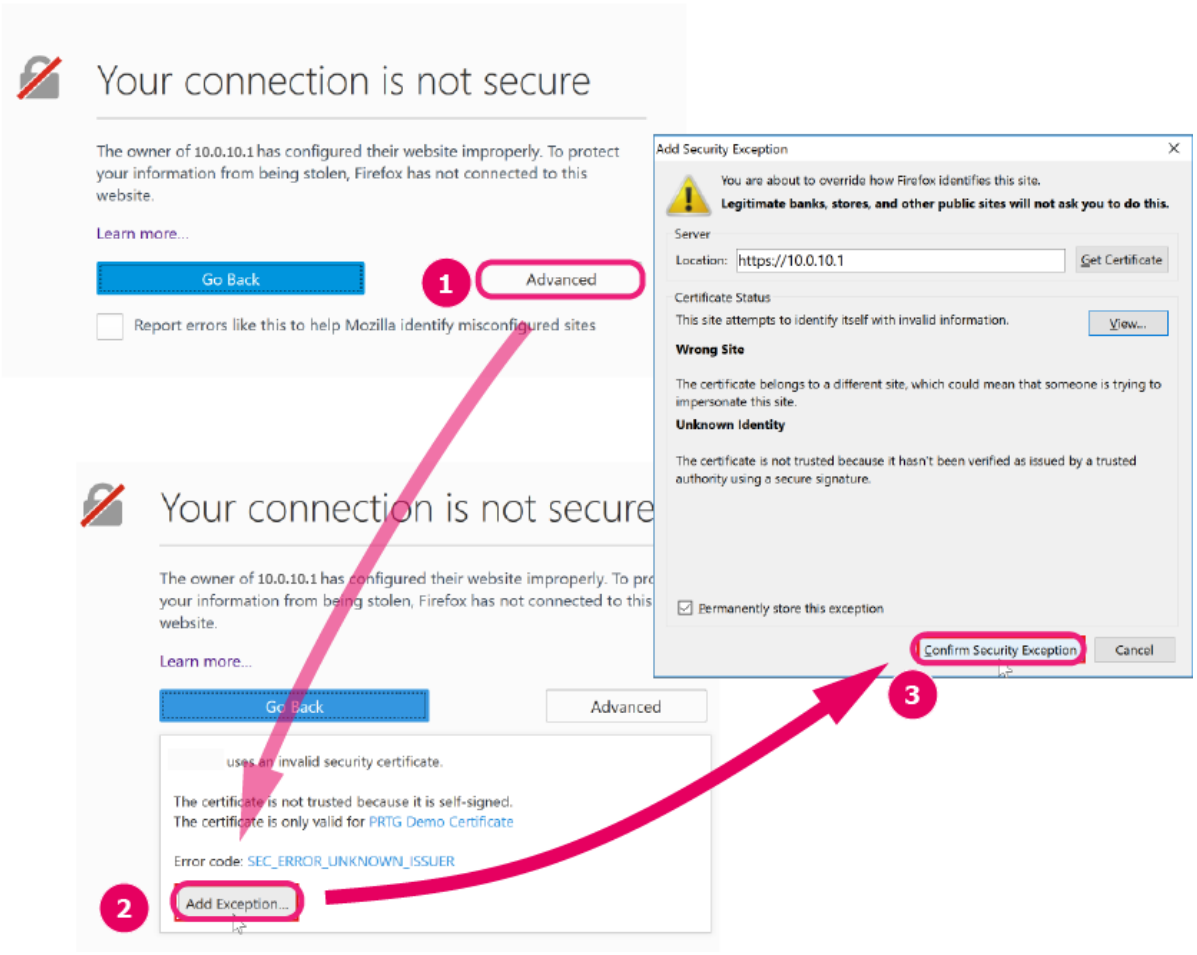


SSL Warning in Chrome

Click here to enlarge: http://media.paessler.com/prtg-screenshots/chrome_SSL-Exception.png

Mozilla Firefox

In **Mozilla Firefox**, click **Advanced** and then click the **Add Exception...** button. A window opens, leave the check mark for **Permanently store this exception** and finally click the **Confirm Security Exception** button.



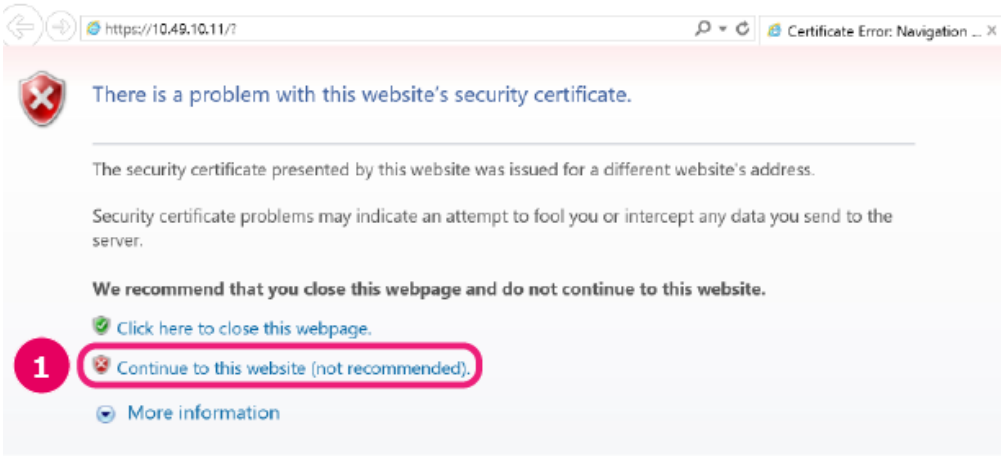
SSL Warning in Firefox

%P_ENLARGE%> http://media.paessler.com/prtg-screenshots/FF_SSL-warning.png

You only have to go through this procedure once for every Firefox browser and PRTG core server.

Internet Explorer

In **Internet Explorer**, click **Continue to this website (not recommended)** every time you call the web interface.



SSL Warning in IE

%P_ENLARGE%> http://media.paessler.com/prtg-screenshots/IE_SSL-Exception.png

Other

For other, not officially supported browsers, the procedure is similar.

More

- **Using Your Own SSL Certificate**

Freeware Network Tools: PRTG Certificate Importer—Installing Trusted SSL Certificates for PRTG Network Monitor

- https://www.paessler.com/tools/certificateimporter

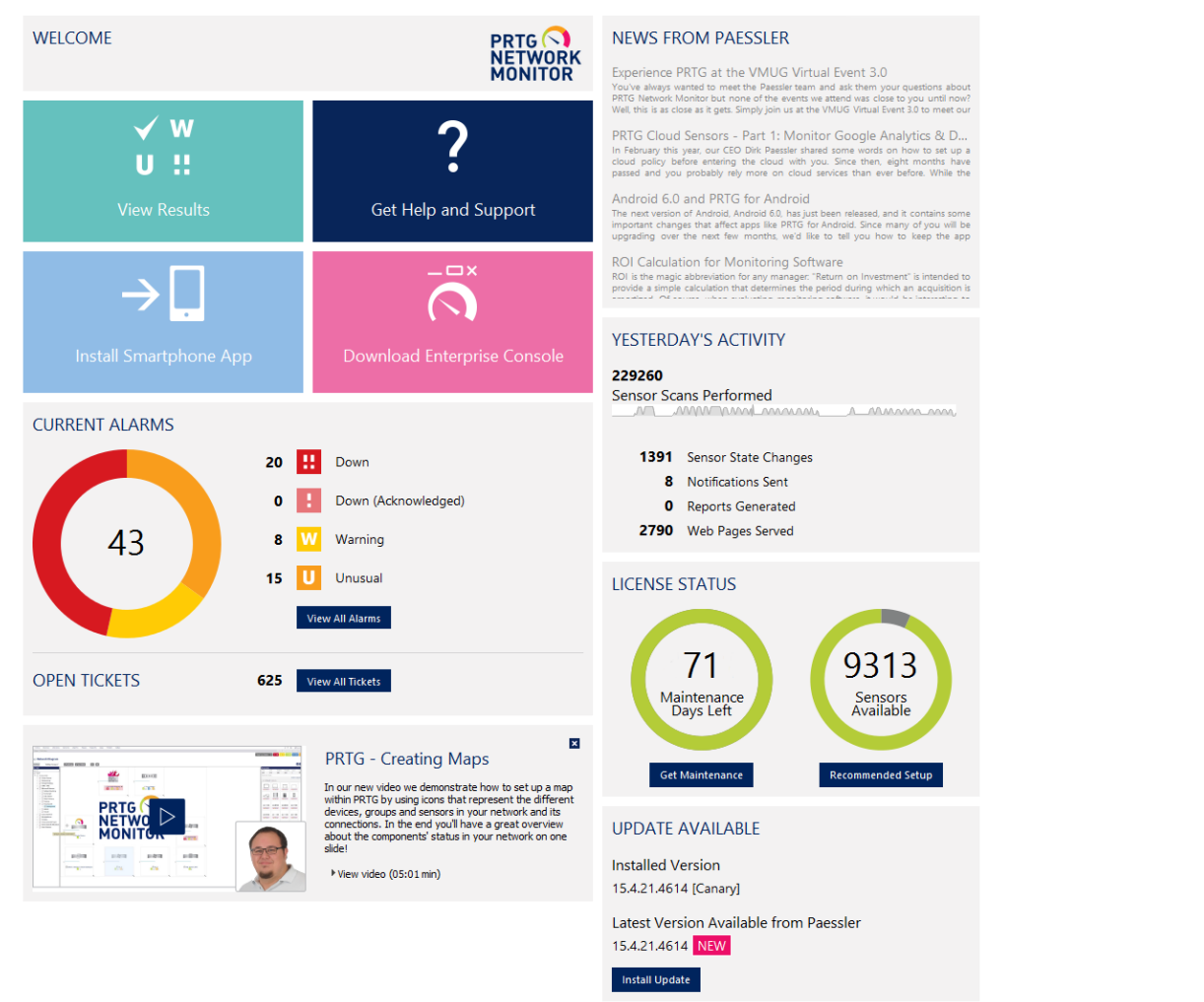
Knowledge Base: Why can't I save my PRTG password in Google Chrome?

- https://kb.paessler.com/en/topic/61982

6.3 Welcome Page

After completing the **Smart Setup** 50, you will see PRTG's welcome page by default when you log in to the web interface. You can set another homepage in your account settings 2909, section **Web Interface**.

This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.



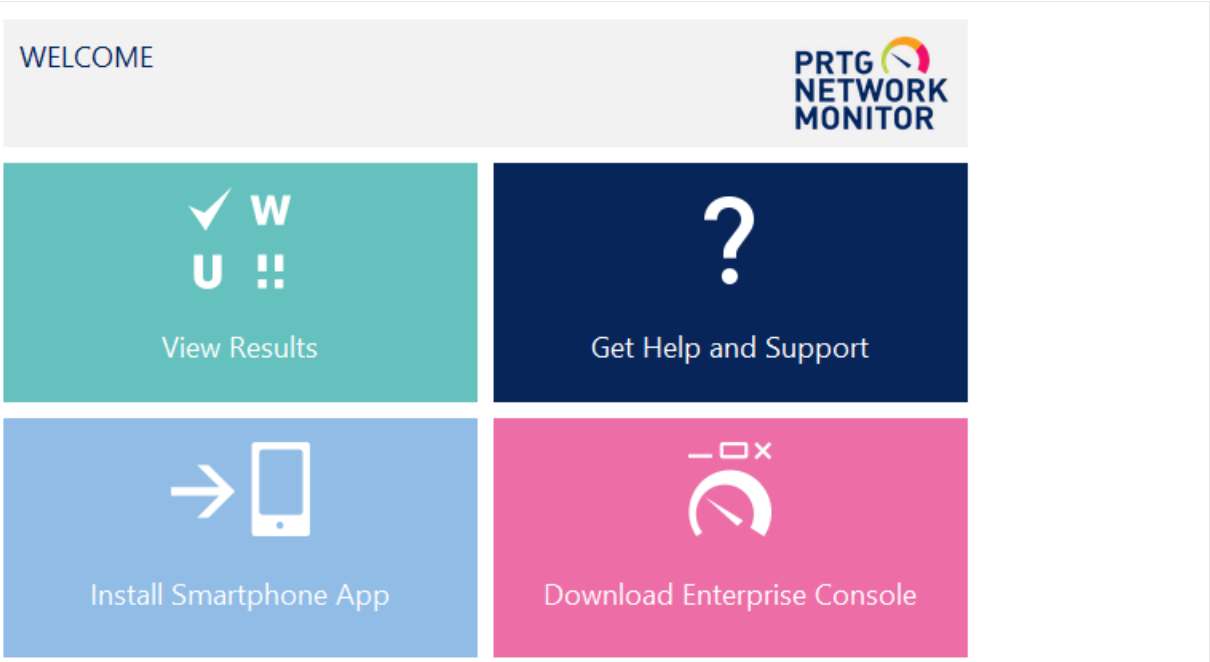
Welcome to PRTG Network Monitor

The PRTG welcome page shows you various information about your PRTG installation at a glance, similar to a dashboard. You can also directly access several pages in the PRTG web interface from the welcome page.

You have the following options on the welcome page:

- **View Results**: Open the device tree 151 that shows your monitoring results.

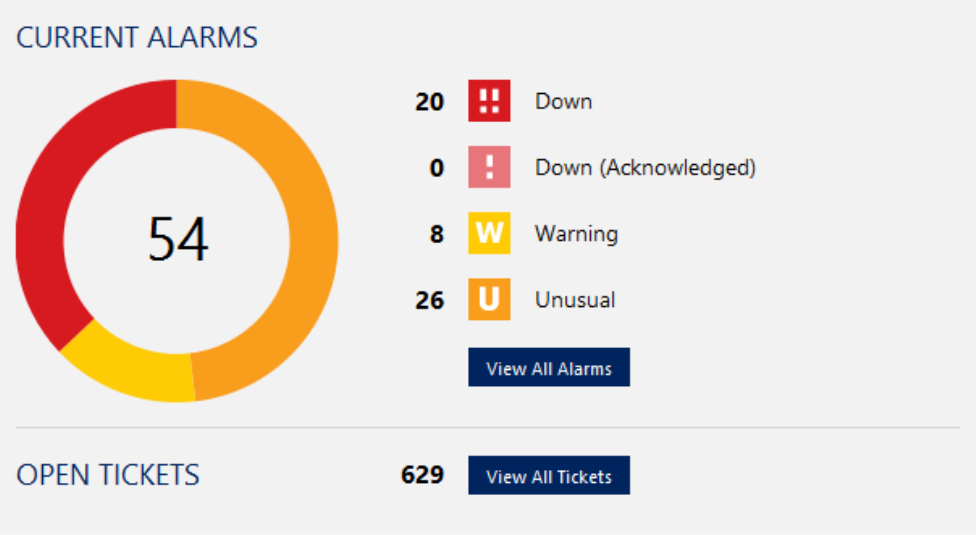
- **Get Help and Support**: Open the PRTG help and support page from where you can access the PRTG user manual, the Knowledge Base, and video tutorials. You can also open support tickets 3022 and contact our customer service 149 from this page.
- **Install Smartphone App**: Open the download page for PRTG's mobile apps 3018.
- **Download Enterprise Console**: Open the download page for the Enterprise Console 3018 in PRTG (PRTG on premises only).
- **Manage Subscription**: Open your PRTG on demand dashboard and manage your subscriptions.



Welcome Page: A Good Starting Point for Your Daily Monitoring Activities

The welcome page keeps you informed about current **Alarms** 190 and open **Tickets** 200:

- **View All Alarms**: Open a list of alarms 190 in your PRTG installation.
- **View All Tickets**: Open a list of all open tickets 200 that are assigned to the currently logged in user.



Welcome Page: Alarms Overview and Open Tickets

Other sections are:

- **News from Paessler**: Shows recent information about PRTG and Paessler. Click the heading of an article to open it on paessler.com with your browser.
- **Yesterday's Activity**: Shows what your PRTG server did for you on the day before. Point with your mouse to the mini graph to show the number of sensor scans on a specific day. See also manual section PRTG Status—System Status 2998, section **Activity History**.
- **License Status**: Shows the number of your remaining maintenance days for PRTG on premises and the number of sensors you can still add with your current license. Click **Get Maintenance** to open the Paessler shop and extend your maintenance for PRTG on premises installations. Click **Get More Sensors** to open the Paessler shop and upgrade your license. See also manual section PRTG Status—License Status and Settings 3012.
  The number of available sensors that is displayed here does not consider paused sensors 214 for technical reasons. However, paused sensors do not count against the maximum number of sensors that your license allows. Add the number of your paused sensors to the displayed number to know exactly how many sensors are still available on your installation.
  If you use a PRTG on premises license with an unlimited number of sensors, PRTG takes 10,000 sensors as starting point to calculate the number of available sensors which is displayed here. Please consider the system requirements 25 for a properly working PRTG setup and click **Recommended Setup** for more information.
- **Update Available**: Shows the version number of your PRTG on premises core server and the version number of the latest available PRTG version. You will see the label **NEW** if there is a newer version available. Click **Install Update** to open the PRTG Auto-Update 3005 page.
- If your PRTG on premises installation is currently not SSL-secured, the welcome page will ask you to enable SSL encryption for the PRTG website. Click **Yes, Switch to SSL** to enable SSL encryption or **Don't Tell Me Again** to remove this note from the welcome page. See also manual section System Administration—User Interface 2946.

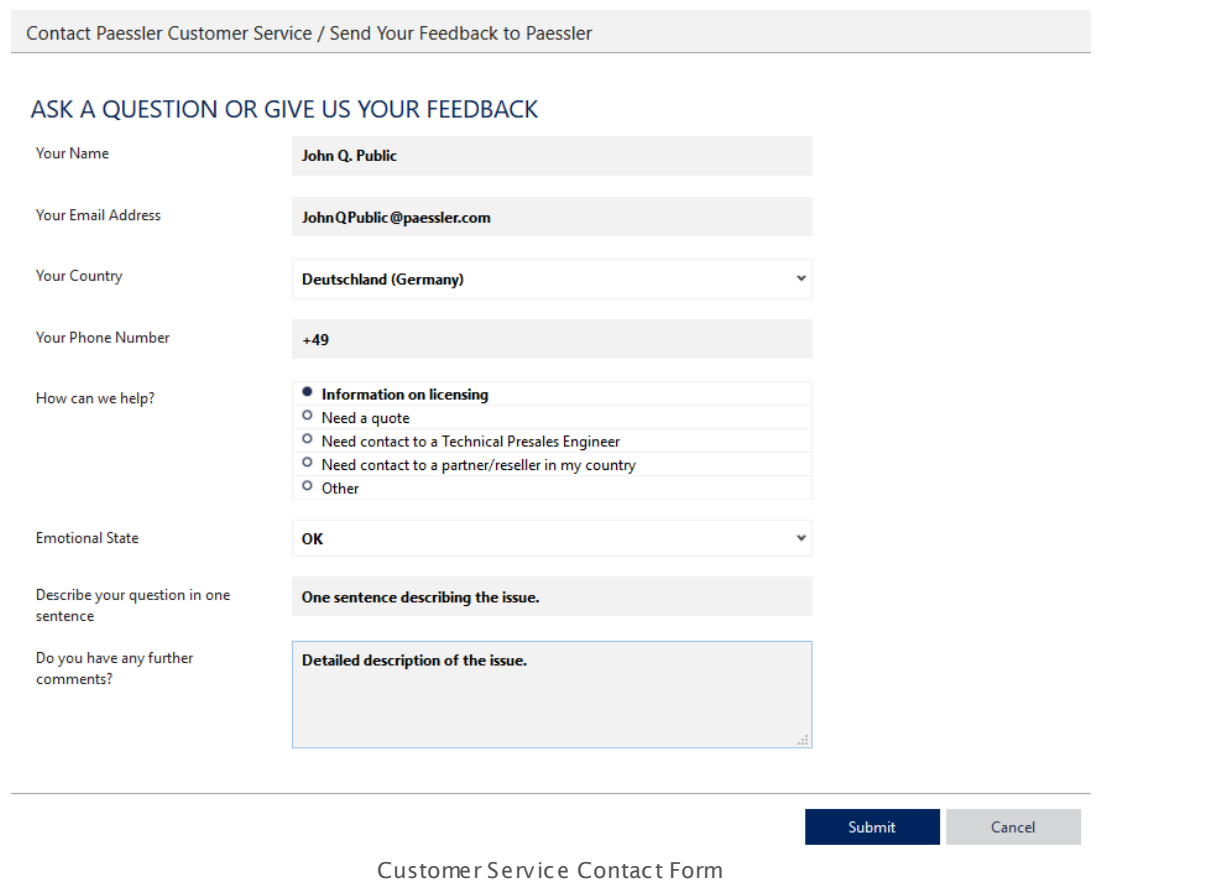
- If you still use the default password of the PRTG System Administrator user (prtgadmin) on a PRTG on premises installation, the welcome page will ask you to set a secret password if your PRTG website is publicly accessible. Click **Change Default Password Now** to define a new password. See also manual section **System Administration—User Accounts** 2976.
- In the **video section** you find informative and helpful videos about monitoring with PRTG. Click a video to open and play it on paessler.com.

The collected information about your PRTG installation makes the welcome page a good starting point for your daily monitoring activities. Of course, you can also set up your custom dashboards in PRTG. The **Maps** 2885 feature of PRTG enables you to create dashboards exactly like you want.

6.3.1 Customer Service

If you have any questions about license purchase, upgrade, or maintenance extension, you can directly contact the Paessler **Customer Service** from the **Help and Support Center** in the PRTG web interface. We will readily assist you with quotes or information about licensing and maintenance, and guide you through the purchasing process. Our Customer Services team will also gladly send you the contact information of a knowledeable PRTG partner in your region or research any technical specifications you might need beforehand.

PRTG transmits your feedback or questions securely to Paessler via the PRTG Cloud. Please make sure your PRTG server has access to the internet and can reach the URL https://api.prtgcloud.com:443 for successful transmission.



Customer Service Contact Form

Ask a Question or Give Us Your Feedback

Provide the following information in this section of the **Contact Paessler Customer Service** form:

- **Your Name**: Enter your full name for contact information.
- **Your Email Address**: Enter an email address under which we can reach you.
- **Your Country**: Select the country in which you run PRTG so we can provide you contact information for a partner near you.

- **Your Phone Number**: Enter a phone number under which we can reach you.
- **How can we help?** Select the scope of your question.
- **Emotional State**: If you want to, you can indicate your current feelings about PRTG and your purchase process.
- **Describe your question in one sentence**: Provide short information that indicates the topic of your request.
- **Do you have any further comments?** Enter your comments here. This can be feedback or any questions for our customer service.

Click **Submit** to send your question or feedback to our customer service. Click **Cancel** to close the customer service contact form without sending it.

If you have technical questions regarding your already existing PRTG setup, contact our technical support 3022.

6.4 General Layout

This manual section provides a general overview over the structure of PRTG's web interface. Central focus is the **Devices** view, which you can select via the main menu bar. The **Devices view** presents the monitoring results at a glance—you will widely use it.

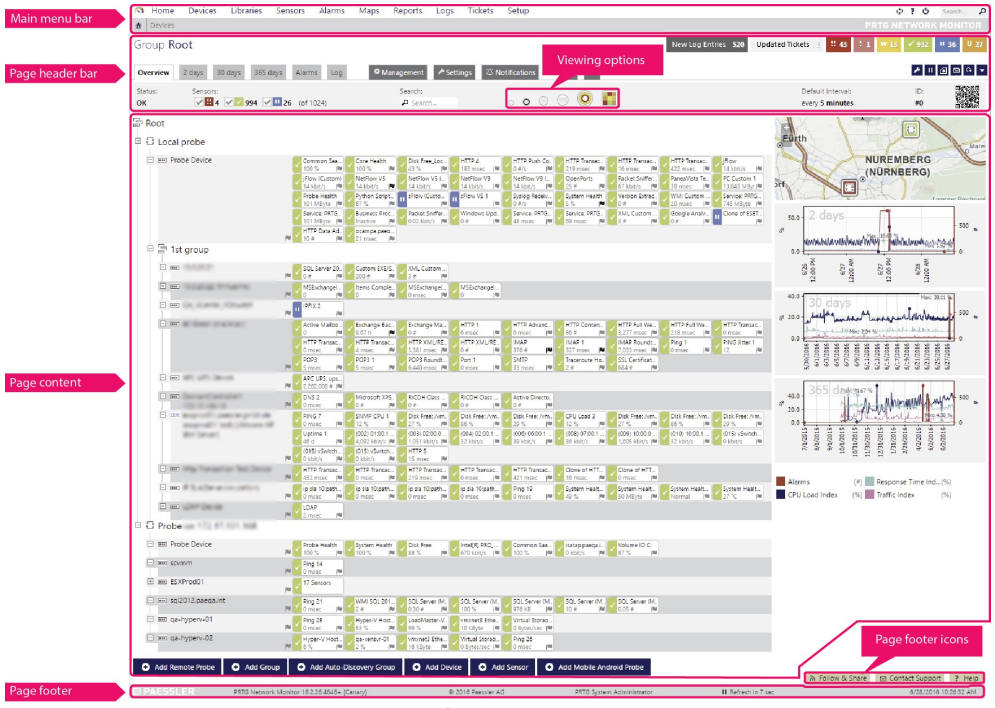
Welcome Page

When you log in to the PRTG web interface, by default you will see PRTG's **Welcome Page** 145. You can set another homepage in your account settings 2909, section **Web Interface**.

Click **View Results** to open the device tree window.

Tree View Layout

Click **View Results** on the welcome screen, to display the device tree window. This will be a good starting point for your everyday work with PRTG.



PRTG Device Tree

Click here to enlarge: https://media-s3.paessler.com/prtg-screenshots/General_Layout3_anotated.jpg

From top to bottom, the Device tree screen has several areas that will be covered in further detail in this section. For a general overview of the device tree consider the below table.

Page area name	Description
Global Header Area 153	This area contains the main menu at the very top, the global status bar, the path to the currently selected object, and a quick search box.
Page Header Bar 155	This area contains the page heading with the name of the current object, several tabs with settings, monitoring data of the current object, the object's status bar, quick action buttons, and the QR code that links to the current URL.
Viewing options 157	These buttons are part of the page header bar. Here you can adjust how your device tree is displayed.
Page Content 161	This area contains information about the current object and all other objects underneath in the tree hierarchy.
Page Footer Icons	With these icons you have quick access to the PRTG **Auto-Update** 3005 page, to PRTG's social network accounts, and to the contact support form 3022. There is also a link to context sensitive help. When running PRTG in a cluster, you will also see a cluster related element. It shows the name of the node that you are logged in to and displays whether this is a master or a failover node. Click the bar to show the **Cluster Status** 3010. In a failover node, you can review all data, but changes in the settings will not be saved. In order to change settings, please log in to the master node of your cluster.
Page Footer	Shows information about the current version of PRTG, the logged in PRTG user account, and the current time (depending on the timezone settings 2980 for the currently logged in user). A timer counts down how much time remains until the next automatic page refresh. You can pause the refresh timer with the pause icon and resume with the play icon. If you open another page while the refresh timer is paused, the timer will resume automatically, starting with the defined **Auto Refresh Interval** that you can configure in your account settings 2909.

Click an object to see its details page. In the page heading of the page header bar 155 you always see the name of the object that you have currently selected.

When navigating PRTG's web interface, the following paths are available:

- The main menu provides access to all important aspects of the software.
- The quick search is often the fastest way to find a specific object (for example a sensor or a device).
- Using the page tabs, you can switch between various sub-pages.
- Right-clicking objects will open a context menu 215.

- When pausing over objects, the tool tip appears, and after further hovering a quick-access window (Hover Popup 230) will open.
- You can drill down into the object hierarchy of probes, groups, devices, and sensors in the object tree by merely clicking a sub-object of the currently displayed object (for example, a sensor on the device page).

These navigation paths offer complete access to the functionality of PRTG, often you will find multiple means of accessing information or navigating to a certain setting.

In the following, the different areas of the web interface are described.

Global Header Area

Global Header Area

Click here to enlarge: https://media-s3.paessler.com/prtg-screenshots/General_Layout_area_anotated.jpg

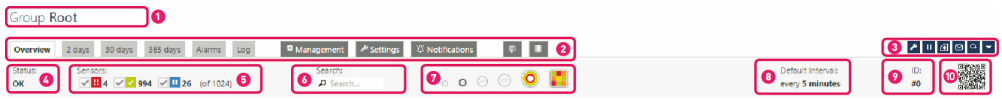
The header area of the web interface provides central, very condensed information about your installation and offers access to all content and every setting within PRTG. The following table lists the elements that the global header area is made up of.

This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

Screen Number	Part	Description
1	Main Menu Bar	For starting to navigate through the web interface, the main menu is the best starting point. We recommend that you take a few minutes to familiarize yourself with the menu bar and its sub-items. For a detailed description see the **Main Menu Structure** 231 section.
2	Icons Refresh, Help Center, Logout	Via the icons in the top-right corner, you can reload the current page, open the help center, or log out.
3	Search Box	To search for a monitoring object, enter a name, parts of a name, an IP address, a DNS name, or a tag in the search box on the right and confirm with enter. PRTG will perform a string search in your entire monitoring setup, including groups, devices, sensors, libraries, maps, reports, tickets, and object comments. A page with the items that are related to the search term will open—even displaying online help articles.
4	Breadcrumbs	Below the main menu, PRTG shows a path that retraces the steps back to the welcome screen (or your defined starting page). Use it to quickly jump back to where you came from. Breadcrumbs can also help you to orient yourself if you get lost. If you click a breadcrumb item, a dropdown menu opens that shows all objects on the same level. You can either search for an object, or select one directly. For example, you can use this to directly access all other sensors or a device, other devices within a group, and another group on the same probe. Other probes in your root group are also available.
5	New Alarms, New Log Entries, New Tickets	The information boxes show how many new alarms, new log entries, and updated tickets have occurred. Click the respective box to view the lists of **Alarms** 190, **Logs** 198, or **Tickets** 200.
6	Global Sensor Status Symbols	This area shows the accumulated states of all sensors you have configured for monitoring, divided according to the different sensor states 163. Depending on each respective status, you will see colored boxes with numbers that symbolize the amount of sensors that are in the respective status. For example, you can see how many sensors are in **Up**, **Down**, or **Warning** status. Click a box to view a list of all sensors in the respective status. For a detailed description, see the **Sensor States** 163 section.

Page Header Bar

The page header bar, below the global header area, consists of a number of elements shown in the table below.



Page Header Bar

Click here to enlarge: https://media-s3.paessler.com/prtg-screenshots/page_header_bar_annotated.jpg

Screen Number	Part	Description
1	Page Heading	This line displays the current object's type and name as page heading. In the screenshot above, it is a group that is called **Root**. Here you can also add the current object to favorites by clicking on the flag, as well as define the object's priority by clicking on one of the five stars (not available for the Root group). For details, see section **Priority and Favorites** 211.
2	Tabs	Via tabs you can navigate to the various sub-pages of an object, for example, to its monitoring data or settings. For more information, see sections **Review Sensor Data** 166 and **Change Device and Sensor Settings** 188.
3	Context Buttons	On the right side is a row of icons for several actions. Depending on the currently viewed page within PRTG, you can pause (and resume) or delete the respective object. You can also add another object (for example, a sensor to a device), send a link to the current page per email, perform an immediate scan, open a related ticket, or show the corresponding object history page 198. On device lists, there is also a button to open the QR codes of all devices on this list in a printable layout. Click the down arrow to open the context menu for the currently displayed object for further options. For more information, see **Context Menus** 215 section.
4	Object Status	This element displays the current status of the selected object.
5	Sensor Status Bar	This element is visible when viewing a probe, a group (including **Root**), or a device. It is not available when the sensor details page is open. The sensor status bar shows the accumulated states of all sensors for the current object, divided into different sensor states. They show the number of sensors in the respective status. For example, you can see how many sensors are in **Up**, **Down**, or **Warning** state. For a detailed description of sensor states, see the **Sensor States** 163 section. You can hide sensors that are in a certain state by removing the check mark in front of the respective status. To show them again, re-add the check mark.
6	Tree Search	In the white search box next to the tree view selection, enter a key word to search the device tree for matching items. The tree will highlight matching devices and sensors by graying-out all others. This can help to gain a quick overview over sensors monitoring a specific part of your network. For example, you can enter the keyword "firewall" to highlight devices and sensors matching this name.
7	Viewing options	This element is only visible when viewing a probe or a group. It is not available when you view device or sensor details. For a detailed description, see Switch Device Tree View 157 below.

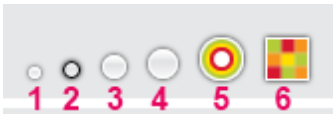
This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

Depending on the selected object type, the page header bar shows additional information:

- All objects underneath the Root group show their dependency 126.
- Groups and devices display the time elapsed since the last execution of the auto-discovery 249 on the selected object.
- Devices show their respective DNS/IP address as defined in the device settings 360 and the time elapsed since the last execution of the sensor recommendation 184 on this device.
- Sensors show additional monitoring statistics.

Switch Device Tree View

Wherever a probe or group is displayed, you can choose between a number of viewing options.

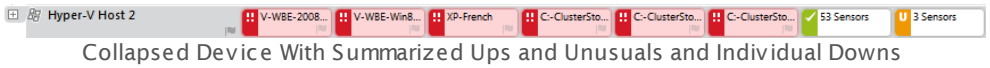


Device Tree Viewing Options

Switch Device Tree View—Classic Device Tree

Via the 'circle symbols' in the page header bar, you can adjust how much information will be included next to each object. Using the various buttons, you can switch from a very condensed view (small circle; marked "1" in the screenshot) to an extra spacious view (big circle; marked "4" in the screenshot).

In the classic device tree view you can collapse devices, groups, and probes. Click the minus box left of the object name. The sensor states will then be summarized. The states of all sensors on this object will be displayed. Right next to the status, the amount of sensors in this status will be displayed, with the exception of the states **Down**, **Down (Partial)**, and **Down (Acknowledged)**. In the default settings, the sensors will be grouped together if there are more than ten sensors with the same status, otherwise they will be displayed individually.



Collapsed Device With Summarized Ups and Unusuals and Individual Downs

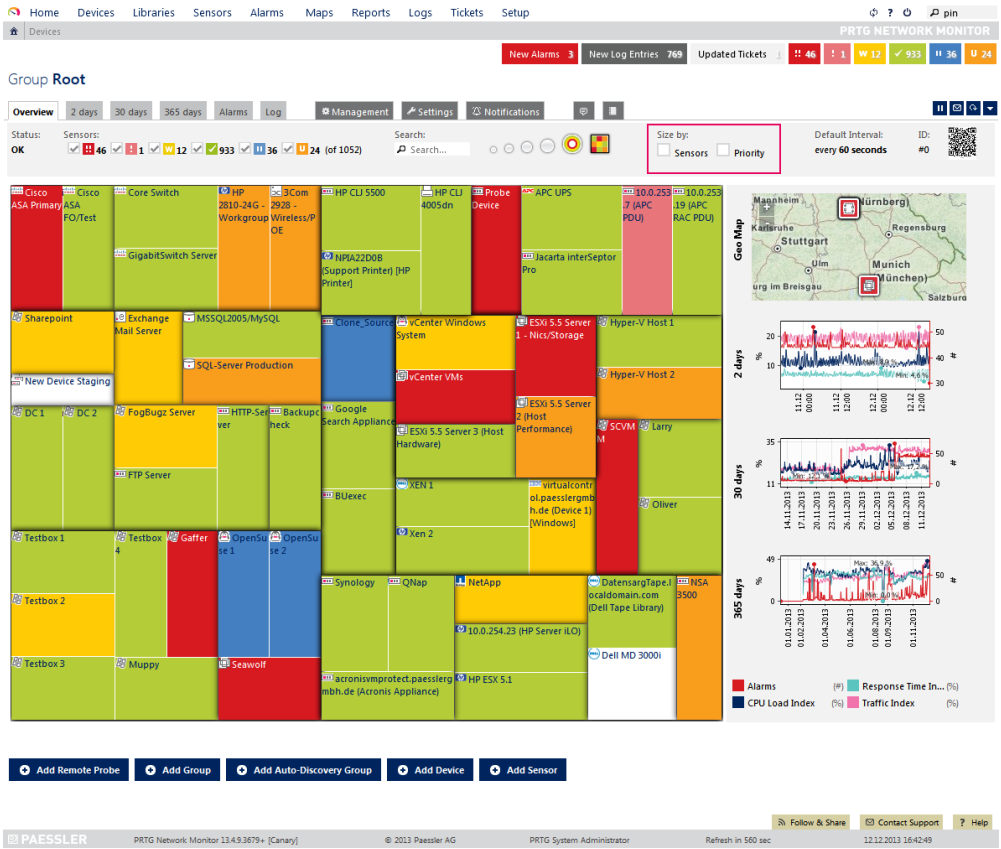
Click here to enlarge: https://media-s3.paessler.com/prtg-screenshots/General_Layout_treeview_collapsed.png

Switch Device Tree View—Extended Views

There are two additional options to the simple tree views that enable you to display the status of all sensors of your entire installation in a single overview. Choose one of the icons to change the view:

Tree Map View (6)

The tree map view displays all devices of your entire installation as tiles sorted into a square and arranged according to the groups they belong to. Each device dynamically changes color to reflect the overall status of the sensors on the device. You can also adjust the square size: either depending on a device's priority, or depending on the number of sensors on a device, or depending on both. To do this, add a check mark under the point **Size by:** in front of **Sensors** and/or **Priority** in the page header bar (see the mark in the screenshot below).



PRTG Tree Map View

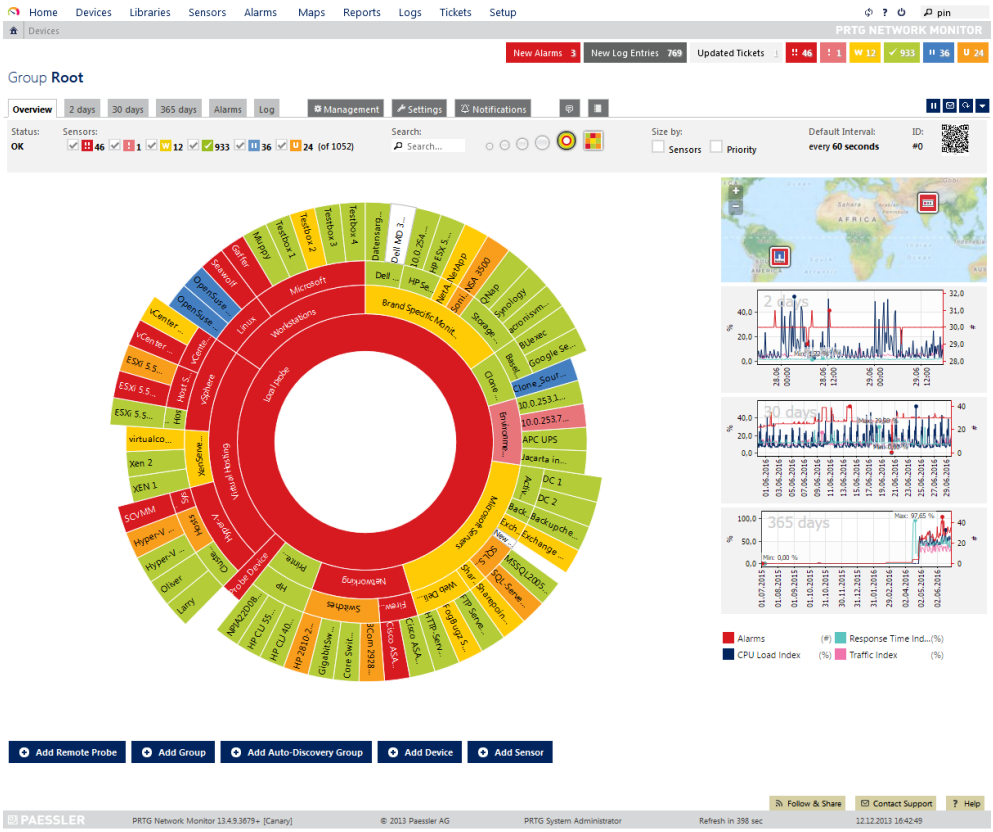
Click here to enlarge: https://media-s3.paessler.com/prtg-screenshots/tree_map_view.png

Sunburst View (5)

The sunburst view displays your entire installation as a circle diagram. The groups are represented as inner circles, and all devices contained within a group are shown as 'cake slices' attached to the outside of a circle element.

The sunburst is interactive:

- You can click elements to open the details view of your monitoring objects.
- You can zoom in and out by using the plus + and minus - buttons or your mouse wheel.
- You can change the position of the sunburst on the overview tab with drag & drop.



PRTG Sunburst View

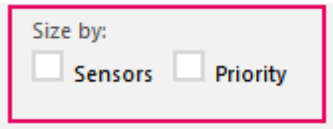
Click here to enlarge: https://media-s3.paessler.com/prtg-screenshots/sunburst_view.png

For both views:

- **Colors**
  A device (or group) element can have different colors, depending on the states of the sensors running on this device or group (see **Sensor States** 163). A higher status is regarded as more important and takes precedence (prioritized higher). For example, if a device currently has sensors in the states **Up** (green), **Paused** (blue), and **Warning** (yellow), according to the device prioritization, this tile would then be yellow, indicating that at least one sensor on this device is in **Warning** status. If a single sensor changes to **Down** status, the corresponding device tile will turn red. Correspondingly, the PRTG states (for both views) are shown here in order of their prioritization:

Flag	Flag Color	Object Status	Meaning
	Red	**Down**	At least one sensor 'belonging to' this object shows a red **Down** status. Point to an object's name to view the total number of alarms concerning this object.
	Bright-Red	**Down (Acknowledged)**	At least one sensor belonging to this object is **Down** and the status has been acknowledged by a PRTG user via the **Acknowledge Alarm** function. All of this devices **Down** states must have been acknowledged—if at least one sensor is not acknowledged, this object will be displayed as **Down**.
	Yellow	**Warning**	At least one sensor belonging to this object shows a yellow **Warning** status. There is no sensor in a **Down** or **Down (Acknowledged)** status concerning this object.
	Orange	**Unusual**	At least one sensor belonging to this object shows an orange **Unusual** status. There is no sensor in a **Down**, **Down (Acknowledged)**, or **Warning** status concerning this object.
	Green	**Up**	All sensors belonging to this object are in a green **Up** status. There is no sensor in a **Down**, **Down (Acknowledged)**, **Warning**, **Paused**, or **Unusual** status concerning this object.
	Blue	**Paused**	All sensors belonging to this object show a blue **Paused** status. There is no sensor in a **Down**, **Down (Acknowledged)**, **Warning**, **Unusual**, or **Up** status concerning this object.
	Black (Grey)	**Unknown**	All sensors belonging to this object have an **Unknown** status. There is no sensor in a **Down**, **Down (Acknowledged)**, **Warning**, **Unusual**, **Paused**, or **Up** status concerning this object.

- **Size by Sensors / Size by Priority**
  You can adjust the size of the different squares. They can be calculated by the amount of sensors running on a device or within a group, or by the sensors' priority (see **Priority and Favorites** 211), or both. Use the check boxes in the page header bar (see below) to change the view immediately, then use the setting that suits you best.



Sorting Checkboxes

Page Content

The page content of the general layout varies dependent on the selected object. It shows information about the current object and all other objects underneath in the tree hierarchy. The deeper down in the hierarchy you select an object, the more detailed is the displayed information.

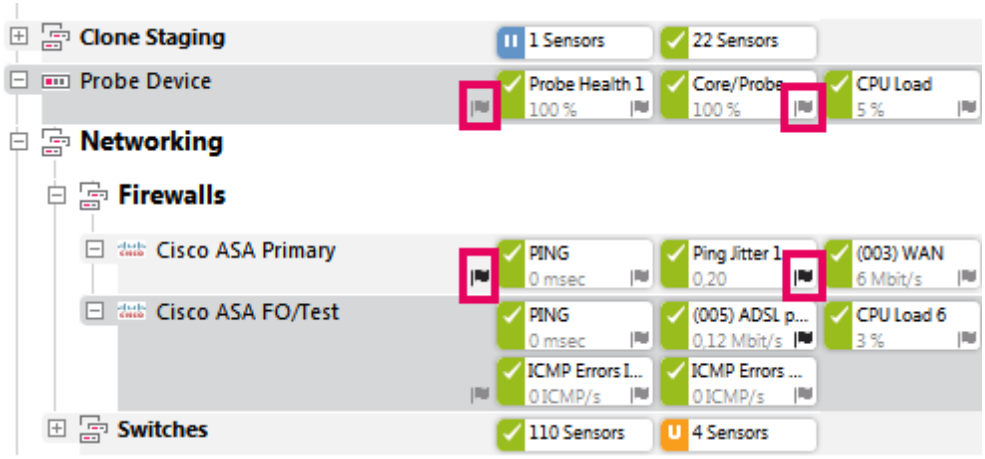
By default, a **Probe Device** is created in the device tree on the local probe. It represents the probe system running with your PRTG installation. PRTG automatically monitors the system health of the core server and each probe to discover overloading situations that may distort monitoring results. To monitor the system status of the probe computer, PRTG automatically creates a few sensors:

- Core Health Sensor 602
- Probe Health Sensor 1378
- System Health Sensor 2321
- Some further device specific sensors for disk usage and bandwidth

In a cluster installation, PRTG also creates a **Cluster Probe Device** with a **Cluster Health Sensor** 589 that monitors the cluster's system health.

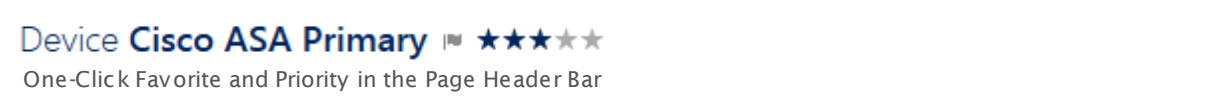
We recommend that you keep these sensors, but they all are removable.

You can tag a device or sensor as 'favorite' by clicking the flag displayed in its lower right corner (see the screenshot below). To untag devices, proceed the same way.



One-Click Favorites in the Device Tree

A quick and easy way of adjusting priority is located in the page header bar[155] right next to the object name (see screen number 1 in that subsection). Click the a stars to adjust priority (5 is highest 1 lowest).



A black flag indicates that the respective object is a favorite already. After clicking the black flag, the object will no longer be a favorite. A gray flag indicates that it is not yet a favorite. See the **Priority and Favorites**[211] chapter for further information.

For more details about page contents, please see the following sections:

- **Review Monitoring Data**[166]
- **Historic Data Reports**[175]
- **Object Settings**[188]
- **Compare Sensors**[172]
- **Geo Maps**[2824]

More

Knowledge Base: How can I change the width of the devices and group "boxes" shown in the PRTG device tree?

- https://kb.paessler.com/en/topic/24963

6.5 Sensor States

In the PRTG device tree you usually create several sensors for each device [360]. With sensors, you can monitor different aspects of your devices. Using a simple color code, they always show you what is going on in your network.

The color of a sensor always shows its current status. In the below table, you will find a list of states a sensor can show. This list also reflects the hierarchy of states whenever summarized sensor states are shown (in the device tree [151], or on geo maps [2824]): the higher a status is in the hierarchy, the higher will be its priority in displaying sensor states. For example, if all the sensors of a specific device are **Up**, but one of its sensors reaches a **Down** status, then the overall status of this device will be **Down** as well (for example, displayed red in the Tree Map View [157]), because this status is higher up in the hierarchy.

Down and **Down (Partial)** states are equal in the status hierarchy.

Sensor	Color	Status Name	Meaning
	Red	**Down**	1. PRTG is unable to reach the device, or the sensor has changed to the error state. See the **Sensor Warning and Down Behavior** [164] below for more information. By design, a sensor does not record any data in its channels while it shows this status. 2. Another reason for this status can be an error limit that is set in the **Sensor Channels Settings** [2782], or an error status due to a sensor **Lookup** [3183]. In this case, the sensor continues to record data in all sensor channels although the sensor shows an error.
	Green/ Red	**Down (Partial)**	In a cluster, at least one node reports this sensor as **Down**, while at least one other node reports the same sensor as **Up**. This status is not available for sensors on remote probes in a failover cluster [116].
	Bright-Red	**Down (Acknowledged)**	The sensor is **Down** and the status was acknowledged by a PRTG user, applying the **Acknowledge Alarm** function. This can be helpful to mark that an alarm has already been brought to attention. For acknowledged alarms no further notifications [2829] are sent. To set this sensor status, right-click the sensor in **Down** status and from the context menu [215], select **Acknowledge Alarm...**. Then enter a comment and click **OK**.

Sensor	Color	Status Name	Meaning
	Yellow	**Warning**	The sensor gives an error reading, but PRTG will try again. The sensor may soon change to a down status. See the **Sensor Warning and Down Behavior** 164 below for more information. Another reason for this status can be a warning limit set in a sensor's **Sensor Channels Settings** 2782.
	Orange	**Unusual**	The sensor reports unusual values for this weekday and time of day. The unusual detection is based on the historic average data and can be configured or disabled in the system administration 2956. You can also disable unusual detection for certain groups only (see **Group Settings** 357).
	Green	**Up**	The last scan was okay and the sensor currently receives data.
	Blue	**Paused**	The sensor is currently paused (for a certain timespan, indefinitely, or triggered by a dependency 126).
	Black (Gray)	**Unknown**	The sensor has not received any data yet or there is an error in (network) communication, likely on the probe system. If sensors show this status persistently, a PRTG restart may be necessary. For extended trouble shooting please see this Knowledge Base article: What to check if sensors are black (gray)?

Sensor Warning and Down Behavior

The **Down** status symbolizes that something is wrong with a monitored device. There can be various reasons for a down status, for example, an interruption in the physical connection to the device, an internet connection outage, or a crashed server.

After a failed request, PRTG tries to re-contact the device before setting a sensor to **Down** status (this is true for almost all types of sensors):

1. If a request to a device fails for the first time, the sensor will change to **Warning** status. PRTG repeats the request and attempts to re-scan the device immediately.
2. If the second request also fails, the sensor changes to **Down** status by default until the device is reachable again. You can change this behavior in the **Scanning Interval** 307 settings of any monitoring object. PRTG tries to reach the device with every scanning interval.

This procedure gives devices and services the chance to recover from a momentary overload and prevents false alarms. Still, you are informed promptly about any network issues.

The behavior described above does not apply to **Warning** or **Down** states that are activated due to a warning or error limit set in the **Sensor Channels Settings** 2782 or to channels using lookups 3183.

More

Video Tutorial: The PRTG Sensor States

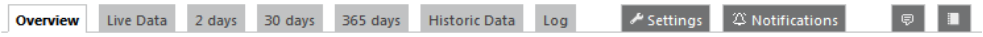
- https://www.paessler.com/support/videos/prtg-basics/sensor-states

Knowledge Base: What to check if sensors are black (gray)?

- https://kb.paessler.com/en/topic/25643

6.6 Review Monitoring Data

Probe, group, device, and sensor pages have tabs that you can use to navigate between the different options. For example, you can view your network's status, view monitoring results, or change settings.



Tabs Bar on Sensor Pages

Overview

The **Overview** tab shows an overview of the currently selected object and its sensors. The pages share a common structure, but some elements differ, depending on the type of object:

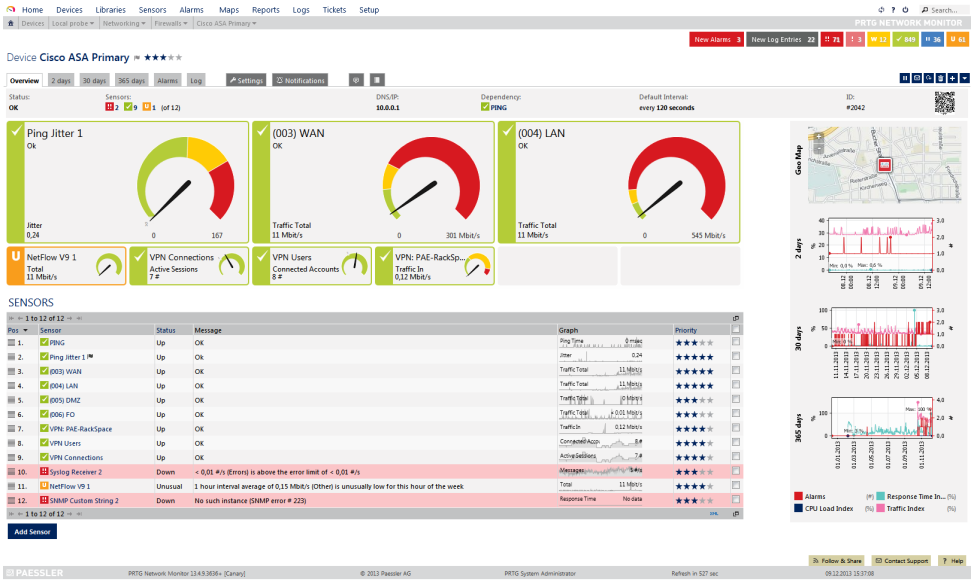
- For probes and groups, the **Overview** tab shows a tree-like view with devices and sensors, a Geo Map, as well as summary graphs for different timespans of the current probe or group.
- For devices, the **Overview** tab shows device details, a Geo Map, and summary graphs for different timespans, colored gauges for high priority sensors, as well as a table list of all sensors on this device. Additionally, you see a table list 207 with **Recommended Sensors** 184.

You can turn off the sensor recommendation (and disable this table list) in **System Administration—Monitoring** 2959.

Assign 4 star (****) or 5 star (*****) priorities to the sensors to display their gauges on your device overview pages. 5 star sensors are represented by larger gauges (upper row on the screenshot) rather than 4 star sensors (lower row on the screenshot).

- For sensors, the **Overview** tab shows sensor details, current status, colored gauges, sensor graphs for different timespans, a table with all sensor channels, as well as similar sensors 180 which show correlations in your network.
- Gauges and switches represent sensor values on **Overview** tabs of devices and channel values on **Overview** tabs of sensors. They visualize the current value of a sensor or a channel, so you can use them as a quick status indicator. The red and yellow sections of gauges correspond to the error and warning limits of the sensor channel settings 2782. Device overview tabs only show gauges of high priority sensors, sensors with priorities of 3 stars (***) or less are omitted here. Sensor overview tabs show gauges of all sensor channels (except the **Downtime** channel), regardless of priority. The primary channel is displayed with the large gauge. Sensor channels that display binary values such as on/off or successful/failing (due to your lookup 3183 configuration) are visualized as switches not gauges. Switches only show red or green for their respective two states.

For the gauge to remain legible, we recommend that you stay below 120 lookup 3183 values for primary channels, which belong to sensors with a 5 star priority. For sensors with a priority of 4 stars, the recommended limit is around 40 lookup values.



Device Overview Tab with Gauges for High Priority Sensors, Sensors Table List, Geo Map, and Mini Graphs

Click here to enlarge: https://media-s3.paessler.com/prtg-screenshots/device_overview_tab2.png

Toplists

Toplists are available for xFlow and Packet Sniffer sensors [386] only. Toplist graphs are displayed right on the sensor overview page. Please see the section **Toplists** [2806].

Live Data and Data By x Days

Select one of the tabs **Live Data** (available for sensors only), **2 days**, **30 days**, or **365 days** to display an object's monitoring data live (sensors only), or for different timespans and in more or less detail. The time that graph legends and data tables show depends on the time zone settings [2980] for the currently logged in user.

The days mentioned here is the default setting. You can change the shown days of the different graphs under **System Administration—User Interface** [2950].

2 Days Tab of a Firewall with Overview Graph and Sensor Mini Graphs

Click here to enlarge: https://media-s3.paessler.com/prtg-screenshots/2days_devicetab.png

Live Data and Data By x Days—Probes, Groups, and Devices

For probes, groups, and devices, each of the tabs shows a summary graph for the current object and mini graphs for all sensors on this object, as well as a data table for the current object. For performance reasons, PRTG never displays more than 50 mini graphs. Hover over a mini graph to display the graph legend.

Summary graphs show the number of alarms as well as three index graphs. These graphs indicate response time, CPU usage, and bandwidth usage for all sensors. Index graphs are similar to a stock index. The shown values are based on the readings of all sensors of this object. PRTG computes these values using statistics and by comparing the values to the highest and lowest readings ever recorded.

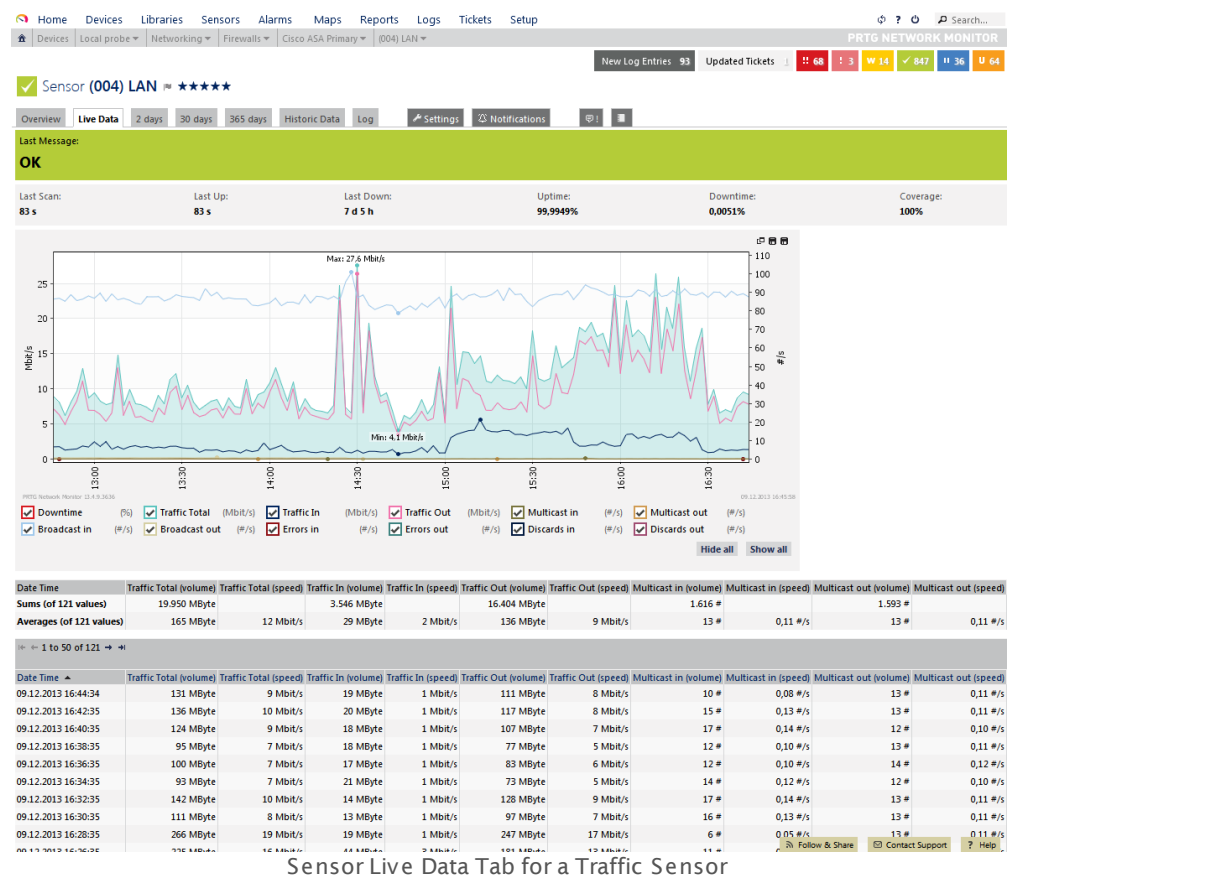
The three index graphs show overall (or global) trends in your network. If these values increase over a specific time frame, then CPU load, bandwidth load, or response time respectively have worsened during this time. For example, a CPU Load Index value of 90% means that the average CPU load for all CPU sensors of your current configuration is at 90% of the highest ever measured CPU usage value.

The following four channels are available in the summary graph:

- **Alarms**: Sums up the number of all down states of sensors on this object during the given time span. This graph provides you a bird's eye view of your network issues. It cannot be hidden.
- **Response Time Index**: Indicates the request times in your network.
- **CPU Load Index**: Indicates the CPU usage in your network.
- **Traffic Index**: Indicates the bandwidth usage in your network.

For more details about the index graphs, see the Knowledge Base: [How does PRTG compute CPU Index, Traffic Index and Response Time Index?]

You can hide all channels individually except the "Alarms" channel. To do this, remove the check mark symbol in front of a channel name besides the graph, and the corresponding channel's line will disappear. You can also **Show all** or **Hide all** channels by clicking on the buttons below the channel names. The graph view will be reset immediately.



Sensor Live Data Tab for a Traffic Sensor

Live Data and Data By x Days—Sensors

For sensors, each tab shows a graph and data table for the selected sensor. When viewing the data of a sensor running on a cluster probe, you can additionally select if you want to show the data of all nodes, or of one specific node only. Please use the **Select Cluster Member** bar below the tabs.

Multi-node graphs are never displayed as filled graphs, but are displayed with lines only. However, historic data reports can have filled multi-node graphs.

While viewing a sensor graph you can hide single sensor channels individually. Simply remove the check mark symbol in front of a channel name below the graph, and the according channel's line will disappear. You can also **Show all** or **Hide all** channels by clicking on the buttons besides the channel names.

Live Data and Data By x Days—Interactive Graphs

The graphs on a sensor's historic data tabs and in "zoomed graphs in new windows" (see below) belonging to other monitoring objects are all interactive. You can zoom in and scroll along the time axis with the corresponding buttons.

Graph Buttons

The following actions are available for graphs:

- << scrolls one graph window left and >> one graph window right. The scrolled time depends on the graph you select, for example, 2 days on a 2 days graph.
- < scrolls left and > right on the time axis. The scrolled time depends on the graph you select.
- + zooms into and - out of the graph. The displayed time depends on the graph selected. For example, you can zoom in a 30 days graph so that it shows data for 6 days.
- x resets the graph to the default view.

In the upper right corner of each graph, three small icons are located :

- **Zoom graph in new window**: Opens a larger version of the graph in a new browser window.
- **Download the graph (PNG or SVG)**: Shows a PNG or SVG file of the graph in a new browser window. You can then save or copy it for later use.

For each graph, you can also choose which specific channels (only on sensor pages) or indexes you want to see via the corresponding check boxes or the **Show all** and **Hide all** buttons.

Warning or error limits 2783 are only shown in graphs (highlighted in yellow or red) if you select exactly one channel with a limit.

Historic Data

The **Historic Data** tab is available for sensors only. Please see section **Historic Data Reports** 175.

Sensor Lists

Viewing lists of sensors is a great way to keep an eye on your network status because you can select which kind of sensors you would like to see. There are many different sensor list views available, such as a list of favorite sensors and top 10 lists, lists filtered by current sensor status, value, availability, tag or type, sensor cross reference, and many more.

Sensor lists are accessible via the main menu bar. Click the **Sensors** entry to show a table list of all sensors. In the table list 207 displayed here, you can re-arrange the items by clicking the column's header items (see section **Working with Table Lists** 207). Hover over it to show other menu options. For detailed information about the available options, see the **Main Menu Structure** 236 (**Sensors**) section.

Alarms

The **Alarms** tab is not available for sensors, but for probes, groups, and devices only. Please see the **Alarms** 190 section.

System Information

The **System Information** tab is available for devices only. Please see section **System Information** 193.

Log

The **Logs** tab shows past activities and events regarding the currently selected object. Please see the **Logs** 198 section.

Related Topics

- **Object Settings** 188
- **Compare Sensors** 172

More

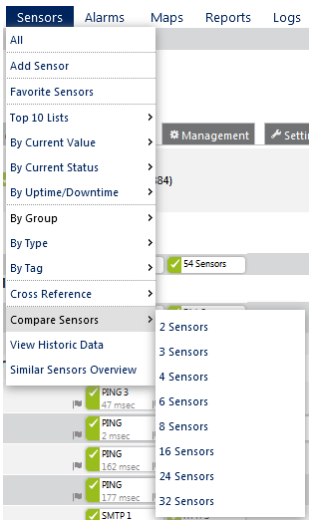
Knowledge Base: How does PRTG compute CPU Index, Traffic Index and Response Time Index?

- https://kb.paessler.com/en/topic/313

6.7 Compare Sensors

This function allows you to compare the graphs of any two or more sensors, regardless of their type. The selected graphs are displayed within one window, so you can have a look at all of them at the same time and visually compare them.

To compare graphs of several sensors, select **Sensors | Compare Sensors** from the main menu bar. Hover over it and select how many sensors you want to compare.



PRTG Main Menu: Compare Sensors

Choose the number of sensors that you wish to compare. This opens an assistant where you can choose your desired sensors and the time span the particular graphs will cover.

Compare Graphs of Two Sensors with 30 Days Time Span

Click here to enlarge: https://media-s3.paessler.com/prtg-screenshots/compare_graphs2.png

Compare Sensors Settings

OPTIONS

Time Span	Specify the time span the graphs should cover. Choose between: ▪ **2 days** ▪ **30 days** ▪ **365 days**

Data Comparison

Select the objects you want to show a graph for. Click the button **Click here to select an object!** to open the **Object Selector** 210. There are as many selection sections as you have defined before.

Select the Objects to be Compared

PRTG shows the graphs immediately after object selection. You can now cross-reference the graphs and adjust them as in the historic data tabs of sensors 170: select the channels you want to display and zoom and scroll in the graphs. Click **Select New Sensor** to choose a different sensor for comparison.

Related Topics

If you want to create a sensor that combines data from various sensors, see the following sensor types:

- **Business Process Sensor** 528
- **Sensor Factory Sensor** 1438

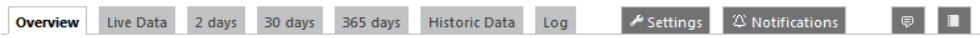
6.8 Historic Data Reports

For quick reviews of a sensor's monitoring data, use the historic data reports as an alternative to the comprehensive **Reports** 2862 function. You can run and view a report of the historic data for each single sensor, on demand. Additionally, you can export this sensor data as XML or CSV files to your computer for further processing with third party applications.

There are two ways to open PRTG's historic data reports: either you click the **Historic Data** tab on a sensor's detail page, or you choose **Sensors | View Historic Data** from the main menu 236.

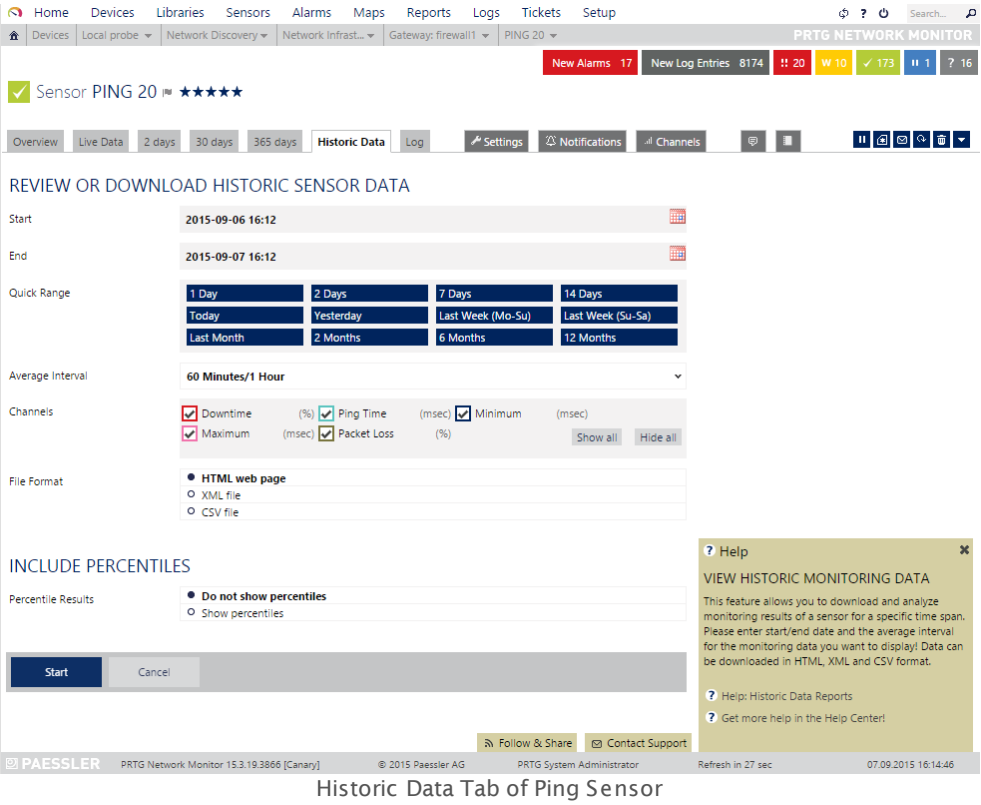
Historic Data (Sensor Tab)

Probe, group, device, and sensor pages have tabs that you can use to navigate between the different options. For example, you can view your network's status, view monitoring results, or change settings.



Tabs Bar on Sensor Pages

The **Historic Data** tab is available for sensors only (not for probes, groups, or devices). When you open the historic data tab of a sensor, there is no sensor selection available. If you want to select a different sensor for the report, select **Sensors | View Historic Data** from the main menu in the PRTG web interface.



Historic Data Tab of Ping Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/historic_data_tab_ping_sensor.png

Historic Monitoring Data (Sensors Main Menu)

When you open historic data reports via **Sensors | View Historic Data** in the main menu, PRTG will ask you to choose the sensor you want to create a report for with the **Object Selector** 210.

Historic Monitoring Data Settings

SETTINGS

Sensor	This field is only visible if you open the historic data function via the main menu. Select the sensor you want to create the report for: click the reading-glass symbol to open the object selector. For more information, see section **Object Selector** 210.
Start	Specify the start date and time of the data you want to review. Use the date time picker to enter the date and time. You cannot start the report generation if monitoring data has been purged 2972 after the defined start date. Please set the start for the report to a date where data is available.
End	Specify the end date and time of the data you want to review. Use the date time picker to enter the date and time.
Quick Range	In this section you can use several buttons for a faster selection of start and end dates. Click any of these links to change the **Start** and **End** values above. Choose between: ▪ **1 Day**, **2 Days**, **7 Days**, or **14 Days**: Set the date range to the respective day(s). The current time of the current day is the end date. ▪ **Today**, **Yesterday**, **Last Week (Mo-Su)**, **Last Week (Su-Sa)**, **Last Month**, **2 Months**, **6 Months**, **12 Months**: Set the date range to the last matching period. It starts at 00:00 and ends at 00:00 of the particularly following day.
Average Interval	With this option, you can activate and configure averaging. Select an interval for which PRTG will calculate the average value. You can choose between **No Interval** (no averaging is performed and only raw data displayed), a few seconds, minutes, hours, or a whole day (**24 Hours**). A shorter interval results in a more detailed report for this sensor.

SETTINGS

The best settings for you may vary, depending on the scanning interval of the sensor, the selected date period, and the intended use for the report. It might be useful to try different settings and compare what the results look like. Please also see the section Automatic Averaging 178 below.

Channels in Graph

Select the channels that you want to include in the graph of the report. You can select or deselect individual channels with the respective check boxes, and select or deselect all channels with the buttons **Show all** or **Hide all**. PRTG will only show the data of selected channels in the graph of the report.

The report table will always show the data of all channels.

Cluster Node

This field is only visible if the sensor is running on a cluster probe. Select the cluster node's data that PRTG will include in the report. Choose between:

- **All nodes**: Include the data of all cluster nodes in the report.
- [Several specific nodes]: Use a specific node's data for the report. The nodes you see are specific to your setup.

File Format

Select the output format for the report. Choose between:

- **HTML web page**: Display the result directly as HTML web page. This is also a good option to check results before exporting to another file format.
- **XML file**: Export the data as Extensible Markup Language (XML) file. Usually, your browser shows a download dialog when you use this option.
- **CSV file**: Export the data as Comma Seperated Values (CSV) file, for example, for import into Microsoft Excel. Usually, your browser shows a download dialog when you use this option.

INCLUDE PERCENTILES

Percentile Results

Define if you want to include an additional percentile calculation 3194 of your data in the report. Choose between:

- **Do not show percentiles:** PRTG does not use a percentile formula to calculate your monitoring results. It will show only the standard values.

INCLUDE PERCENTILES

	▪ **Show percentiles**: PRTG adds a column to the result data tables, which shows percentiles for every sensor channel. Percentiles are not available for all report templates. If a template does not support percentiles, they will simply not show up in the report, even when you enable this setting. Likewise, percentiles are not available in a cluster setup if you choose the option **All Nodes** in the **Cluster Node** setting in the sensor section above.
Percentile Type	This setting is only visible if you select **Show percentiles** above. Enter the percentile type you want PRTG to use for the calculation. If you choose, for example, to calculate the 95th percentile, enter "95" here and 5 % of peak values will be discarded. Please enter an integer value.
Percentile Average Interval	This setting is only visible if you select **Show percentiles** above. Enter a value to define the averaging interval on which PRTG bases the percentile calculation. The default value is 300 seconds (5 minutes). This means that PRTG takes 5 minute averages as basic values for the percentile calculation. Please enter an integer value.
Percentile Mode	This setting is only visible if you select **Show percentiles** above. Choose the mode for percentile calculation: ▪ **Discrete**: PRTG takes discrete values to calculate percentile results. ▪ **Continuous**: PRTG interpolates between discrete values and bases the calculation on interpolated values.

Click **Start** to generate a historic data report.

You cannot start the report generation if monitoring data has been purged 2972 after the defined start date. Please set the start for the report to a date where data is available.

Reports cannot show uptime or downtime data for the **Sensor Factory Sensor** 1438.

Data reporting is limited to 5 requests per minute.

Automatic Averaging

For performance reasons, PRTG automatically averages monitoring data when calculating data for large time spans. Data is then averaged regardless of the selected average interval.

TIME SPAN IN REPORT	MINIMUM LEVEL OF DETAIL (AVERAGE INTERVAL)
Up to 40 days	Any
40 to 500 days	60 minutes/1 hour or larger

Reports for time spans of more than 500 days are not possible. If you enter a longer time span, it will automatically be shortened to 365 days.

Related Topics

- **Review Monitoring Data** 166
- **Reports** 2862

More

Knowledge Base: Why is there missing data in historical data reports?

- https://kb.paessler.com/en/topic/61382

6.9 Similar Sensors

With PRTG you can detect relationships between different components in your network. This function is called similar sensors analysis, a heuristic calculation that shows similar behavior in your sensors. The analysis is completely automated and sensor type agnostic. It is based on mathematics and fuzzy logic. This feature helps you find interconnections in your network that you were not aware of and optimizes your sensor usage by tracking redundant monitoring of some aspects of your system.

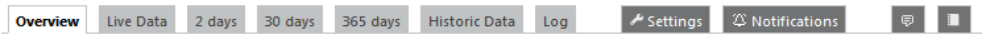
You can adjust the depth of similar sensors analysis or turn it off in **System Administration—Monitoring** 2958. You can also enable or disable the similarity analysis for specific probes, groups, and devices and specify inheritance 122 in the corresponding object settings 188, section **Automatic Monitoring Analysis**.

There are two options to view similar sensors:

- The overview page of sensors contains a similar sensors section. PRTG lists channels there that show similarities to channels of the current sensor.
- In addition, you can call a similar sensors overview page via **Sensors | Similar Sensors Overview** from the main menu 236.

Similar Sensors (Sensor Overview Tab)

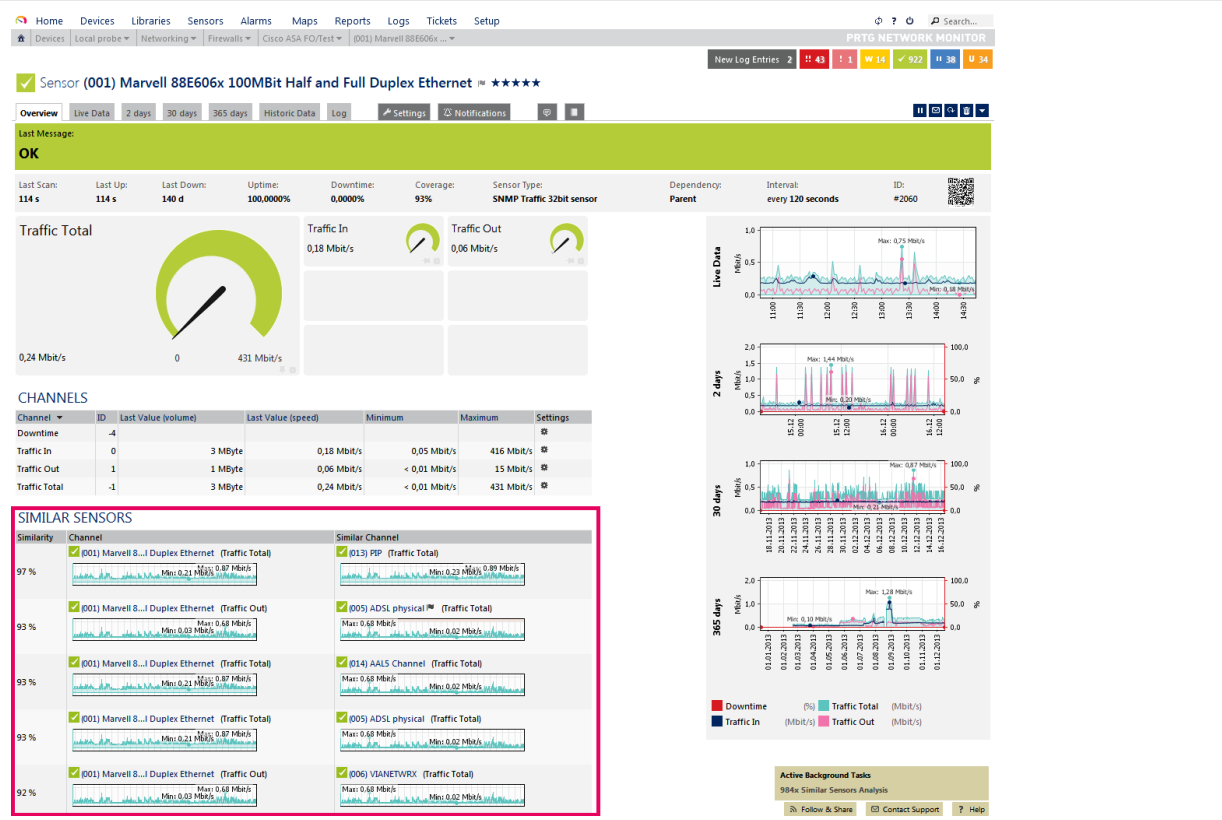
Probe, group, device, and sensor pages have tabs that you can use to navigate between the different options. For example, you can view your network's status, view monitoring results, or change settings.



Tabs Bar on Sensor Pages

On the overview tab of a sensor, PRTG lists channels that show similarities to channels of the currently selected sensor. The table is empty if PRTG detects no similarities regarding the selected sensor.

PRTG only shows similar sensors here when channels have at least 85% similarity. Furthermore, the analysis saves up to 15 entries per sensor at most.



Similar Sensors Section on a Sensor's Overview Tab

The similar sensors section provides the following information:

SIMILAR SENSORS

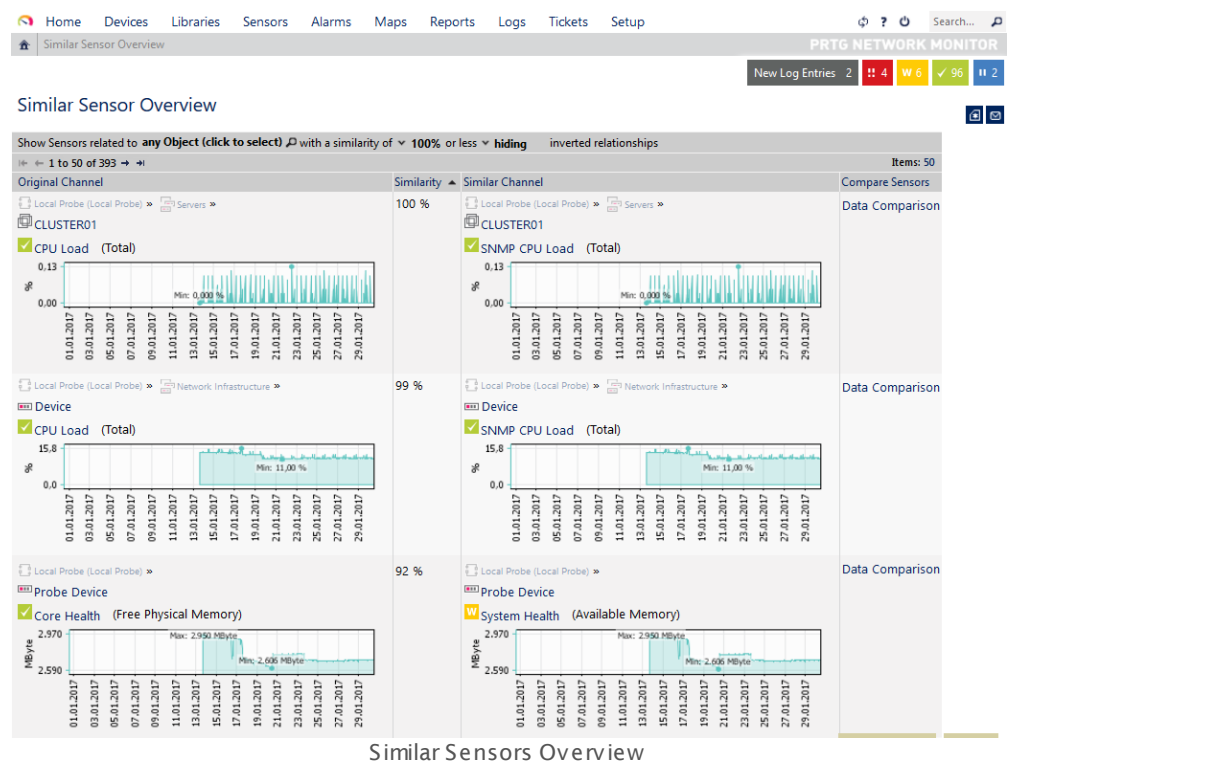
Similarity	Shows a measurement of similarity between two channels in percent.
Channel	Shows a channel of the currently selected sensor.
Similar Channel	Shows a channel of another sensor similar to a channel of the currently selected sensor (the one in the "Channel" column in the same row).

PRTG does not show the similar sensors section when the analysis is off or when you have exceeded 1,000 sensors and selected the automatic analysis depth option 2958. You will see a notice in this case.

Similar Sensors Overview (Sensors Menu)

This page shows the results of the similar sensors analysis from the entire monitoring database. PRTG lists all channels with similarities to another one here. On the table top, you have several filter options to display similar sensors as you need it. Choose the object of interest, the degree of similarity, and if you want to display back references. For more details, see also section Working with Table Lists 207.

PRTG only shows similar sensors here when channels have at least 85% similarity. Furthermore, the analysis saves up to 15 entries per sensor at most.



Similar Sensors Overview

You can sort the list by clicking the column headers. The similar sensors overview page provides the following information:

SIMILAR SENSORS OVERVIEW

Original Channel	Shows channels that other channels are compared to. Click the column header to sort the list according to the order in the device tree in ascending or descending order.
Similarity	Shows a measurement of similarity between two channels in percent. Click the column header to sort the list according to the similarities in ascending or descending order.

SIMILAR SENSORS OVERVIEW

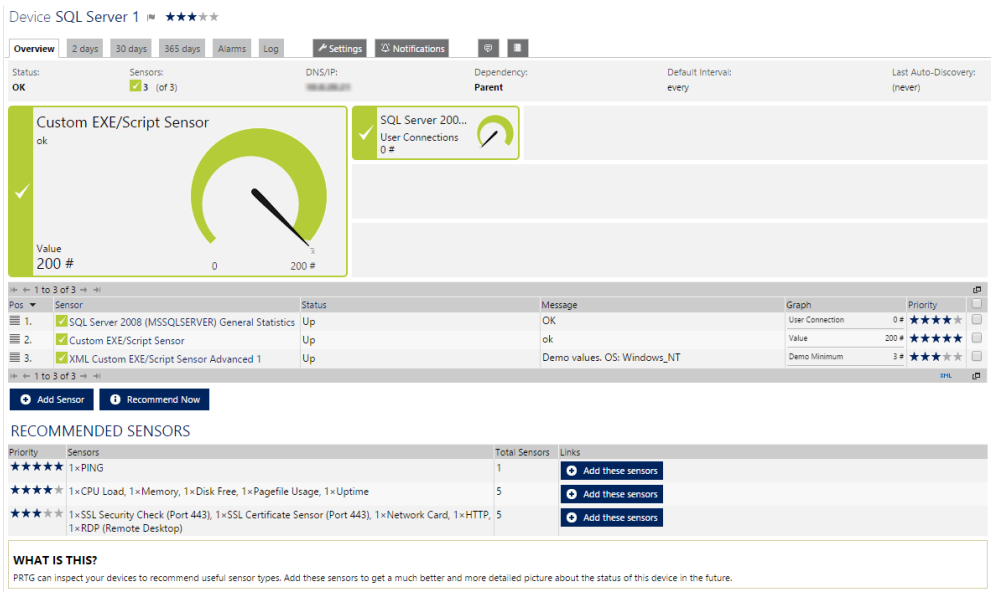
Similar Channel	Shows a channel compared to the original channel. Click the column header to sort the list according to the order in the device tree in ascending or descending order.
Compare Sensors	Click **Data Comparison** to compare graphs of two or more monitoring objects. Please see section **Similar Sensors** 180 for more information on comparing sensors.
Item Count	Define how many channel similarities are shown on this page. Choose between 50, 100, or 500.

PRTG does not show the similar sensors overview option in the main menu if you turned off the analysis or if you have exceeded 1,000 sensors and selected the automatic analysis depth option.

6.10 Recommended Sensors

The **Recommended Sensors** function is one of the options that PRTG supports you in setting up a comprehensive monitoring. PRTG can explore any device and check which sensors you have already created. If it finds useful sensors that can complete your monitoring [166] and are not yet created, you will find a list of recommended sensors for your specific device. By adding these sensors, you will not miss important monitoring data anymore!

You cannot use this feature with local probes in PRTG on demand. You can use this feature on remote probes [3196].



Recommended Sensors on Device Overview Tab

Click here to enlarge: http://media.paessler.com/prtg-screenshots/recommended_sensors.png

Get Sensor Recommendations

You want to know which sensors can complete the monitoring of your devices? By default, PRTG recommends sensors for any device that you add to PRTG and shows the suggested sensor types for it on the **Overview** tab of the device, as long as your installation contains less than 5,000 sensors in total. All you have to do is click the **Add These Sensors** button to enhance your monitoring experience.

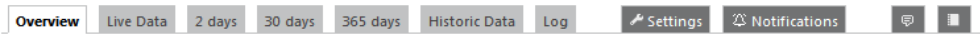
If you want to manually start the detection engine for sensor recommendations on any desired device, follow the steps below.

You can see the time passed since the last execution of the sensor recommendation in the page header bar [155] on the **Overview** tab of this device.

Step 1: Choose the Device

Open the **Overview** [166] tab of the device that you want to analyze.

Probe, group, device, and sensor pages have tabs that you can use to navigate between the different options. For example, you can view your network's status, view monitoring results, or change settings.



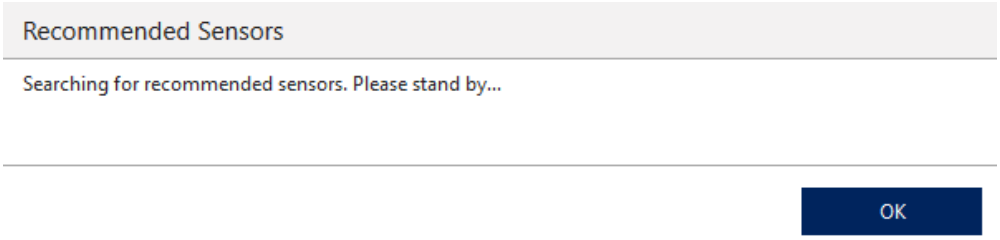
Tabs Bar on Sensor Pages

Step 2: Recommend Now

To start the analysis of your device, click the **Recommend Now** button directly below the sensor list or choose the option **Recommend Now** in the context menu 222.

If you do not see the **Recommend Now** option, make sure that the sensor recommendation is enabled in the **System Administration—Monitoring** 2959 settings. Probe devices do not offer this option.

Depending on the complexity of your device, it can take some time until you see the results of the analysis. Stay tuned!



Recommended Sensors Investigation

PRTG runs the device analysis in the background with low priority to prevent potential performance issues. Consequently, the recommended sensors analysis can take more time than expected if PRTG needs resources to ensure gapless monitoring of your network in the first place. By default, the sensor recommendation engine starts automatically when you add a new device, when you do not have more than 5,000 sensors, or when the last analysis was executed more than 30 days ago. You can change these settings in the **System Administration—Monitoring** 2959.

To recommend SNMP sensors 387 for a device, the detection engine uses the SNMP version that you defined in the **Credentials for SNMP Devices** 368 section of the device settings.

Step 3: Get the Results

After analyzing your device, PRTG suggests a list of sensors that are useful for a more comprehensive monitoring.

RECOMMENDED SENSORS

Priority	Sensors	Total Sensors	Links
★★★★★	1×PING	1	Add these sensors
★★★★☆	1×CPU Load, 1×Memory, 1×Disk Free, 1×Pagefile Usage, 1×Uptime	5	Add these sensors
★★★☆☆	1×SSL Security Check (Port 443), 1×SSL Certificate Sensor (Port 443), 1×Network Card, 1×HTTP, 1×RDP (Remote Desktop)	5	Add these sensors

List of Recommended Sensors

The list of recommended sensors provides the following information:

RECOMMENDED SENSORS

Priority	Shows which priority [211] the suggested sensors will have when you add them. The recommended sensors table is sorted by priority, beginning with top priority (5***** stars) in the first row. You can manually change the priority of a sensor after adding it.
Sensors	Shows the suggested sensors and the number of sensors from one type PRTG recommends for this device (for example, you might want to add a sensor from the type SNMP Traffic [2132] multiple times because of several network interfaces).
Total Sensors	Shows the total number of suggested sensors per table row. These sensors have the same priority.
Links	Displays an **Add These Sensors** button for every table row. Click to automatically add the sensors listed in this table row to the device.

The detection engine checks if a certain sensor type currently exists on your device and recommends that you add this sensor if it does not exist. If this sensor type already existed previously on the device but you have deleted it, PRTG will suggest this sensor type again. Please ignore the suggestion of this sensor type or follow Step 4 [186].

Step 4: Add Recommended Sensors

Click the **Add These Sensors** button in a table row to add all sensors in this row to the analyzed device.

If you want to add **all** suggested sensors regardless of their priority, click every **Add These Sensors** button in the recommended sensors table. If you want to add only **some** of the sensors of a certain priority and not all of them, please click **Add These Sensors** first and then delete [226] or pause [214] the ones you do not need.

Settings for the Recommended Sensors Analysis

You can also adjust the recommended sensors detection. Go to **System Administration—Monitoring** 2959 to select whether

- you want PRTG to decide on the sensor recommendation (default), or
- you want the recommended sensors to always be displayed, or
- you want to turn off the recommended sensors function.

If you use the default setting, PRTG uses an intelligent assistant that takes care of your specific network monitoring situation. PRTG automatically counts the number of sensors you have and decides whether to start the recommended sensors detection or not. It will not start if your PRTG installation comprises 5,000 sensors or more to prevent performance issues. We recommend that you set this default option so you do not miss any important monitoring data about your network, without risking running into performance issues.

Disable the recommended sensors feature if you encounter performance issues or if you do not want to display this information on device overview tabs.

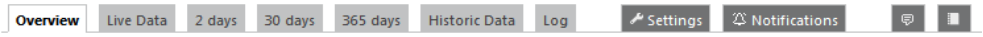
More

Do you want to get more help with choosing and creating useful sensors? This is possible in PRTG with the **Auto-Discovery** 249! You can activate it when adding a new device 276 to PRTG, manually at any time 250, or choose if you want PRTG to analyze a whole section 252 of your network, for example, devices covered by a certain IP range.

The auto-discovery has a higher priority than the recommended sensors detection. If both are active, PRTG will queue the sensor recommendation and execute the auto-discovery first.

6.11 Object Settings

Probe, group, device, and sensor pages have tabs that you can use to navigate between the different options. For example, you can view your network's status, view monitoring results, or change settings.



Tabs Bar on Sensor Pages

Device Tree Management

The **Management** tab is available when viewing probes or groups. After clicking this tab you can move devices and sensors directly in the tree view. If moving is not possible, the web interface will automatically start a clone process.

For more information, please see the Manage Device Tree 292 section.

General Settings

In the **Settings** tab you can define all settings for the current object. The available options vary, depending on the kind of object you're changing. Please see the following sections for information about the respective object types:

- Root Group Settings 294
- Probe Settings 312
- Group Settings 334
- Device Settings 360
- Sensor Settings 384

The available setting options are different for each sensor, but always the same for probes, groups, and devices. Sensor Channels Settings 2782 are not reachable via tab but directly on a sensor's overview page via channel gauges and the channels table.

Notifications Settings

In the **Notifications** tab, notification triggers can be set for every object. When using these settings for a probe, group, or device, they will be inherited to all sensors on these objects. Available notification trigger options are the same for all objects.

For more information, please see Sensor Notifications Settings 2791 section.

Comments

On the **Comments** tab you can enter free text for each object. You can use this function for documentation purposes or to leave information for other users.

Click **Save** to save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

History

In the **History** tab all changes in the settings of an object are logged with a timestamp, the name of the PRTG user who made the change, and a message. The history log retains the last 100 entries.

On some pages, you can access the history of subordinate objects via the corresponding context button in the page header bar 155. This includes **System Administration** 2943 and the overview pages of **User Accounts** 2975, **User Groups** 2982, **Reports** 2862, **Libraries** 2845, and **Maps** 2885. See the **Logs (Main Menu)** 198 for details.

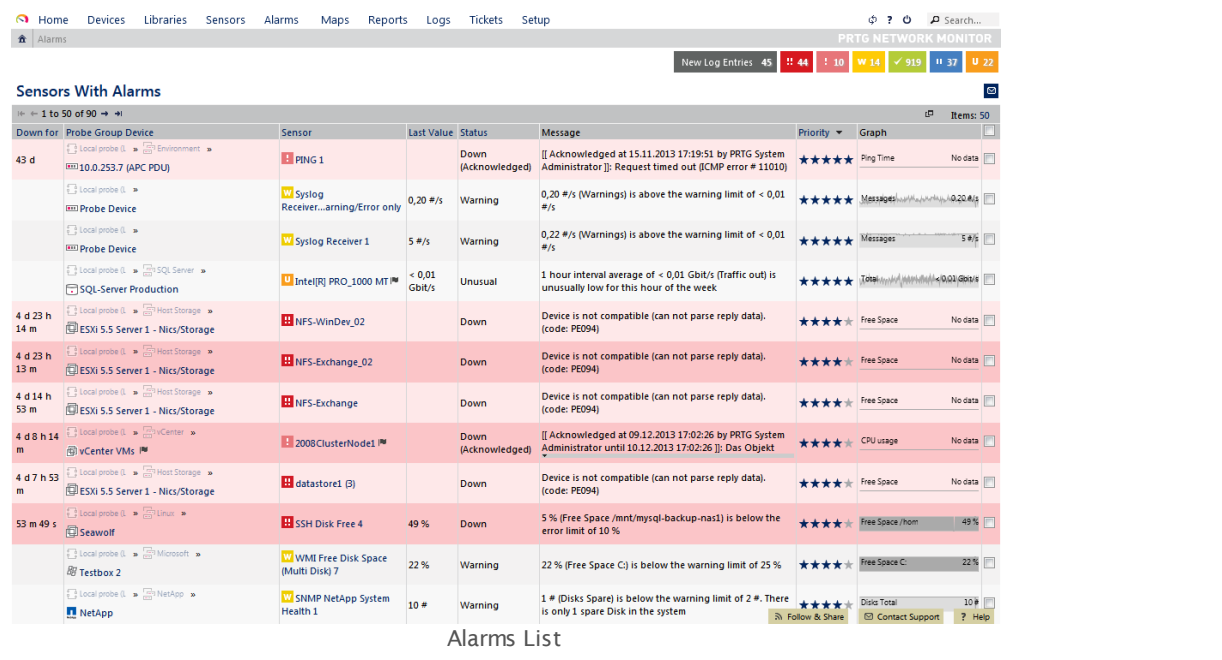
Related Topics

- **General Layout** 151
- **Review Monitoring Data** 166
- **Toplists** 2806

6.12 Alarms

The alarms list shows all sensors that are currently in a **Down**, **Down (Partial)**, **Down (Acknowledged)**, **Warning**, or **Unusual** status. Sensors in other states (for example, **Up**, **Paused**, or **Unknown**) do not appear here. This is useful for keeping track of all irregularities in your network.

In the table list [207], you can re-sort the items by clicking the column's header items.



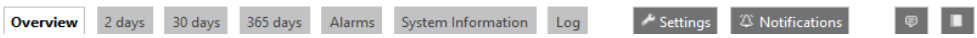
Alarms List

There are two ways to display the alarms list: either click the **Alarms** tab on the detail page of a probe, group, or device (not available for sensors), or click **Alarms** in the main menu bar [231].

By default, table lists with alarms are ordered by priority [211].

Alarms (Object Tab)

Probe, group, device, and sensor pages have tabs that you can use to navigate between the different options. For example, you can view your network's status, view monitoring results, or change settings.



Tabs Bar on Group and Probe Level

On an object's detail view, click the **Alarms** tab to show a table list of all sensors on this object that currently show a **Down**, **Down (Partial)**, **Warning**, or **Unusual** status. You will see a subset of sensors in an alarm status for the current object only. This is a subset of the entries available via the **Alarms | All** option in the main menu bar [239]. The tab is not available on a sensor's detail page.

Alarms (Main Menu)

Click **Alarms** in the main menu bar 239 to show a table list of all sensors in your configuration that currently show a **Down**, **Down (Partial)**, **Down (Acknowledged)**, **Warning**, or **Unusual** status. You can also show these sensors as gauges. Click **Alarms** in the main menu bar 231 and select another option to only show a subset of sensors in certain states. Choose between:

ALARMS	
All	Open a list of all sensors that are currently in **Down**, **Down (Partial)**, **Down (Acknowledged)**, **Warning**, or **Unusual** status 163.
Show as Gauges	Open a page with the gauges of all sensors that are currently in **Down**, **Down (Partial)**, **Down (Acknowledged)**, **Warning**, or **Unusual** status. The size of the sensor gauges corresponds to their respective priority.
Errors Only	Open a list of all sensors that are currently in **Down**, **Down (Partial)**, or **Down (Acknowledged)** status.
Warnings Only	Open a list of all sensors that are currently in **Warning** status.
Unusuals Only	Open a list of all sensors that are currently in **Unusual** status.

Acknowledge Alarm

An acknowledged alarm shows up in the alarms list as "acknowledged" (see **Sensor States** 163) and will not trigger 2791 any more notifications 2829.

If the alarm condition clears, the sensor usually returns to an **Up** status immediately with the next sensor scan.

To acknowledge an alarm, right-click a sensor entry and choose **Acknowledge Alarm...** from the context menu, enter a message and click the **OK** button. The message will appear in the last message value of the sensor. You can choose between: **Acknowledge Indefinitely...**, acknowledge **For 5 Minutes...**, **For 15 Minutes...**, **For 1 Hour...**, **For 3 Hours...**, **For 1 Day...**, or **Until...**.

If you choose **Until...** a dialog box appears:

ACKNOWLEDGE ALARM UNTIL

Selected Objects	Shows the sensor(s) that you want to acknowledge the alarm for. You can acknowledge alarms for more than one sensor using multi-edit 2814.
Message	Enter a text, for example, the reason why you acknowledge the alarm. Please enter a string or leave the field empty.
Until	Enter the date when the acknowledge status will end. Use the date time picker to enter the date and time. If the alarm condition still persists after the specified date, the sensor will show a **Down** status again.

Only users 2975 with write access rights may acknowledge alarms. You can give read-only users the right to acknowledge alarms, too. See section **User Accounts Settings** 2976, section **Account Control**.

More

Knowledge Base: Which audible notifications are available in PRTG? Can I change the default sound?

- https://kb.paessler.com/en/topic/26303

6.13 System Information

The **System Information** feature can show you various information about a device such as connected hardware, installed software, connected user accounts, running processes, and available Windows services with their current status. This is a great possibility to see at a glance what is currently running on the systems in your network. Together with your everyday monitoring you will receive a really profound knowledge about your IT infrastructure from only a single source—your PRTG Network Monitor!

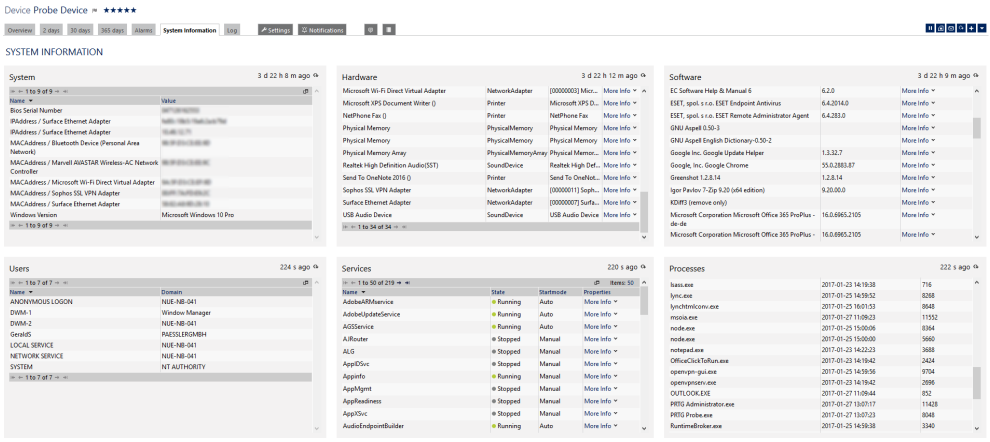
System information is available for all devices which you add to PRTG and run with an officially supported Windows version [25]. You can also retrieve system information from other devices with enabled Simple Network Management Protocol (SNMP). On the overview page of a device, click the **System Information** tab to see available information.

Basically you do not have to configure anything special to use the system information feature. PRTG uses the same technologies [3086] to request system information data as sensors that receive monitoring data from a device. If you already monitor a device with WMI [389] and SNMP sensors [387], the main preconditions for retrieving system information for this device are already met. The data will be displayed in the corresponding table automatically. Section **Preconditions** [194] below shows in detail what you need to get system information.

System information is not supported by the Enterprise Console [3028]. Please use the PRTG web interface [136] to access the system information of a device.

System information for your devices only has informational purposes. We cannot guarantee that the display in PRTG fully corresponds to the device parameters.

You cannot use this feature with local probes in PRTG on demand. You can use this feature on remote probes [3196].



System Information Tab on a Windows Device (Snippet)

Click here to enlarge: https://media-s3.paessler.com/prtg-screenshots/systeminfo-tab.png

Prerequisites

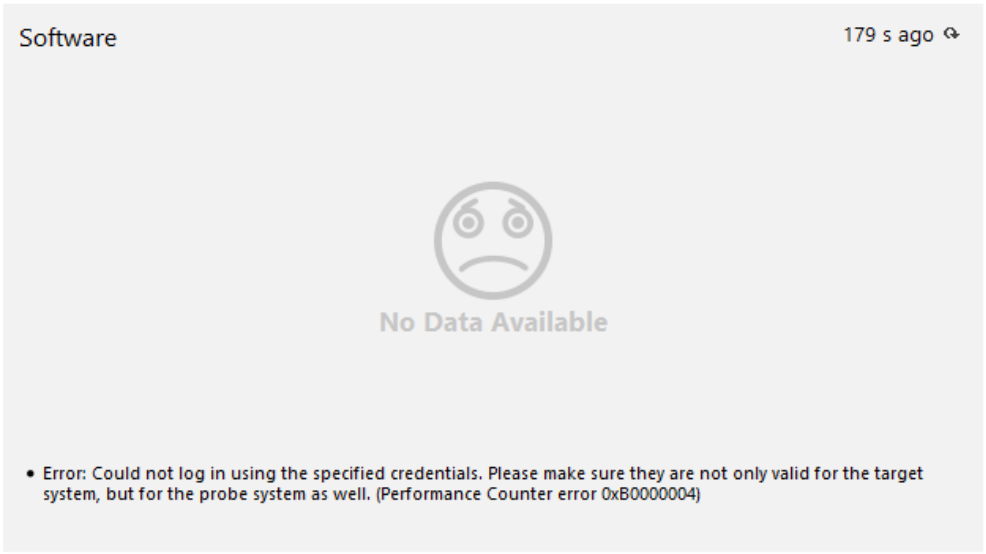
Fulfill the following requirements to show all available system information data for a device. It is not necessary to meet every single prerequisite but then some tables will not show all data or may even remain empty. For example, if you do not configure SNMP on the target device, you will get less information for the **System** table.

- **Valid credentials** in the device settings 360 (or inherited 118): Enter correct settings for the target device in the sections **Credentials for Windows Systems** and **Credentials for SNMP Devices**.
- **Remote Registry** Windows service: Enable the Remote Registry Windows service on the target computer, for example, via services.msc, and set the start type to automatic.
- **Remote Procedure Call (RPC)** Windows service: Enable the RPC Windows service on the target computer, for example, via services.msc, and set the start type to automatic.
- **WMI** on probe and target computer: Configure Windows Management Instrumentation (WMI) on the target computer and on the computer that runs the PRTG probe with the device. Especially configure the firewall of the target computer to allow WMI. For more details, see manual section **Monitoring via WMI** 3092 and the Knowledge Base article **General Introduction to WMI and PRTG**.
- **SNMP** on target computer: Configure Simple Network Management Protocol (SNMP) on the target computer. For more details, see manual section **Monitoring via SNMP** 3087 and the Knowledge Base article **General Introduction to SNMP and PRTG**.

Usually you will see data for a system information table after a few minutes, depending on the used protocols (WMI takes longer than SNMP). A system information table will show an according error message if PRTG cannot get data for a table because of misconfiguration.

For details about error messages, please see this Knowledge Base article: How can PRTG get data for System Information tables?

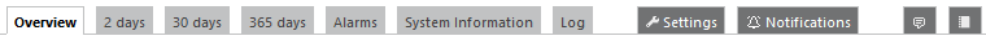
To show information data, you need to enable **System Information** in section **Advanced Network Monitoring** 382 in the device settings (or inherit it from an object higher in the hierarchy 118). This is the default setting. If system information is disabled, the **System Information** tab will not be available for the device.



No Data Available: Check the Preconditions

System Information (Device Tab)

Probe, group, device, and sensor pages have tabs that you can use to navigate between the different options. For example, you can view your network's status, view monitoring results, or change settings.



Tabs Bar on Device Level

On the details page of a device, click the **System Information** tab to show several tables with information about this device. Each table contains information about one category.

SYSTEM INFORMATION

System	Shows information about the device like BIOS serial number, IP addresses, MAC addresses, and Windows version.
Hardware	Shows hardware connected to the device like disk drives, CD/DVD, video controllers, processors, network adapters, sound devices, printers, and memory. You can see **Class** and **Caption** of a hardware device. In the **Properties** column you can get more information about the hardware (for example, the description).
Software	Shows installed software and the **Version** number on the device. In the **Properties** column you can get more information about the software (for example, the size). PRTG uses Uninstall registry keys to retrieve the list of installed software, so the displayed software might differ from the software that the target Windows system shows under Programs and Features.

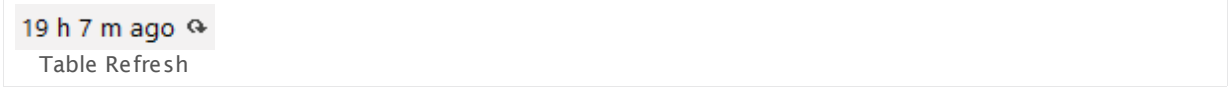
SYSTEM INFORMATION

The System Information scan for software on the probe device uses the credentials the probe [112] runs with and ignores credentials from the **Settings** tab.

Users	Shows the user accounts connected to the device and their **Domain**.
Services	Shows the available Windows services on the device. This table shows the **State** of the service (running, stopped) and the start type (**Startmode** automatic, manual, or disabled). In the **Properties** column you can get more information about a service (for example, the description).
Processes	Shows the processes that are currently running on the device as listed on the Processes tab of the Windows Task Manager. You can also see the **Start Time** and **Process ID** of a process.

Click the refresh button in the upper-right corner of a table to retrieve current information for this system information category. The timestamp shows the time passed since the last table refresh. PRTG automatically retrieves data for all tables, including **System**, **Hardware**, and **Software**, once every 24 hours. The tables **Users**, **Services**, and **Processes** refresh each time you open the **System Information** tab. PRTG also updates all system information tables when the PRTG server is restarted, for example, after an update.

PRTG can perform up to 24 system information scans simultaneously so it may take some time until the tables are filled after a server restart.



You can sort each table by clicking the column headers. Please see **Working with Table Lists** [207] section for more information.

PRTG user accounts with read-only access rights [129] to a device can view system information on this device but they cannot refresh tables manually.

Data Storage

PRTG stores data files with the retrieved system information in the **\System Information Database** subfolder of the PRTG data folder [3226] under the according categories. Please note that if you delete a device in PRTG, the system information files of this device will remain here unless you delete them manually from the folder.

The PRTG uses the following subfolders for system information data.

SYSTEM INFORMATION DATABASE: DATA FOLDERS

hardware	Data for the **Hardware** table
loggedonusers	Data for the **Users** table
processes	Data for the **Processes** table
services	Data for the **Services** table
software	Data for the **Software** table
system	Data for the **System** table

More

Knowledge Base: How can PRTG get data for System Information tables?

- https://kb.paessler.com/en/topic/67824

Knowledge Base: General Introduction to WMI and PRTG

- https://kb.paessler.com/en/topic/1043

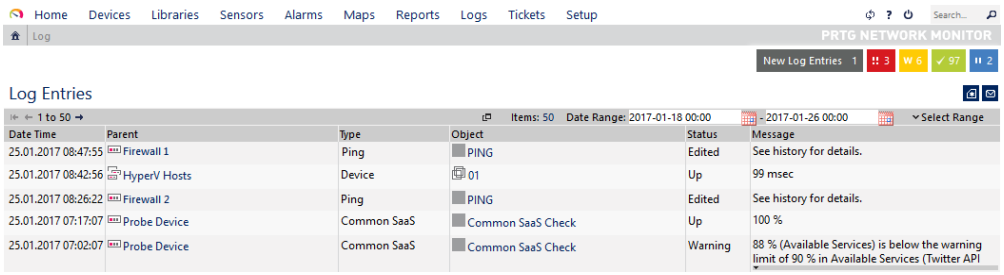
Knowledge Base: General Introduction to SNMP and PRTG

- https://kb.paessler.com/en/topic/46863

6.14 Logs

Logs show all past activities and events of your PRTG monitoring setup. This is useful for researching past user activities, system events, and, for example, to check whether messages were sent. In a typical setup, a huge amount of log data is produced. Because the activity of every single object is recorded, you can use this information to check if your setup works exactly as desired.

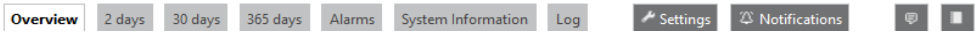
There are several filters available to make navigating the log entries easier. See the **Working with Table Lists** 207 section for more information.



List with Log Entries

There are two options to open the logs list: Either you click the **Log** tab on the detail page of a probe, group, device, or sensor, or you choose the **Logs** item in the main menu.

Probe, group, device, and sensor pages have tabs that you can use to navigate between the different options. For example, you can view your network's status, view monitoring results, or change settings.



Tabs Bar on Group and Probe Level

Click the **Log** tab to show a table list with all log information on this object. This is a more detailed log than the system log available via the **Logs | All** option in main menu 241.

Logs (Main Menu)

Click **Logs** in the main menu bar 241 to show a table list of all system log entries in your configuration. Hover over **Logs** and select another option to narrow down your log search. Choose between:

LOGS	
All	Open a table list 207 with log information for all objects in your configuration, newest first.

LOGS

By Group ›	Open a list with log information for objects in a certain group only, newest first. Hover over **By Group** to show other menu items. Select **All**, or follow the menu path (it is specific to your setup) to select a group you would like to show log information for.
Status Changes ›	Open a list with log information for certain status changes only. Hover over **Status Changes** to show other menu items. Follow the menu path to view log entries with a special value in the **Status** field only. Select between **Up & Down** (shows entries with either **Up** or **Down** in the **Status** field), **Down**, **Warning**, **Unusual**, **Up**, **Paused/Resumed** (shows entries with either **Paused** or **Resumed** in the **Status** field), or **Acknowledged Alarms**.
System Events ›	Open a list with log information regarding certain system event types only. Hover over **System Events** to show other menu items. Select between the following event types: **Probe Related**, **Cluster Related**, **Auto-Discovery**, **Notifications**, or **Status Messages**.
Object History	Open a list with log information about changes to the PRTG setup and deletions of subordinate system objects. The object history page has a tab-like interface. Using the tabs you can navigate through various sub-pages in order to view the changes to all related settings and deletions of objects. Select between the following tabs: **My Account**, **System Setup**, **Notifications**, **Schedules**, **User Accounts**, **User Groups**, **Reports**, **Libraries**, or **Maps**. You can open a specific tab directly with the context-button **History** in the page header bar 155 on the corresponding pages.

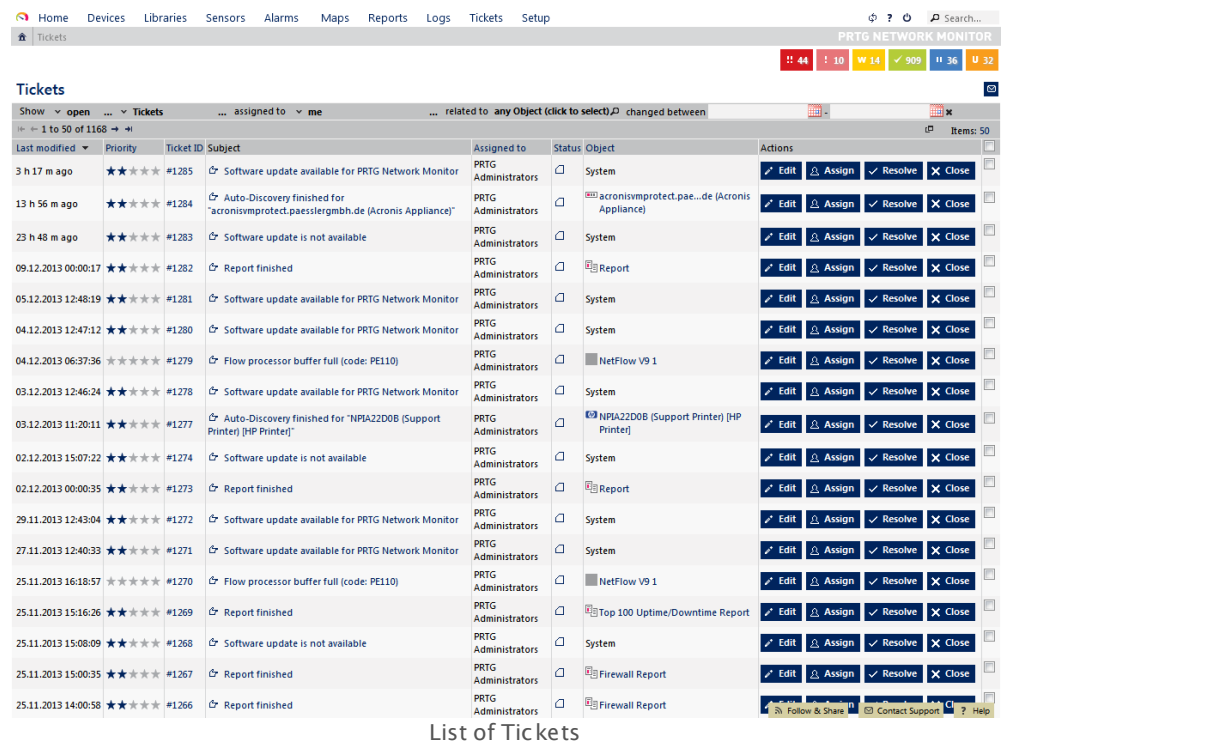
6.15 Tickets

PRTG Network Monitor includes its own ticket system. With tickets you can manage and maintain various issues that may appear while monitoring a network. A ticket in PRTG contains information about recent events in your PRTG installation that need a closer look by the administrator or another responsible person. You can see each ticket as a task for a particular PRTG user.

Each monitoring related task has a lifecycle in the ticket system. PRTG itself can create tickets, for example, when Auto-Discovery 249 has finished, and PRTG users can create tickets as well for every kind of issue. In addition, you can set up notifications that open a ticket when something uncommon occurs in your network. The task comes to life when a ticket is created. Responsible PRTG users then take care of this issue. Once the issue has been resolved, the ticket can be closed and the lifecycle of the task ends.

Every ticket has a unique ID, a priority, and a status, and you can take several actions on each ticket. You should view every ticket and take a corresponding action. This way, you always keep an overview about each task and its history in your PRTG installation.

PRTG can also send an email to you whenever a ticket is assigned to you or if one of your tickets has been changed. See section Tickets as Emails 204 for details and how to turn off emails about tickets.



List of Tickets

You can turn off the tickets system for particular user groups in **System Administration—User Groups** 2982 except for the PRTG Administrators group. The users in the admin group will not receive new ToDo tickets (and notifications about changes) by default, only the PRTG System Administrator user. You cannot change this behavior. However, you can turn off ticket emails 204 for every user account.

Types of Tickets

New tickets are created in the following cases:

- New devices or sensors have been created by the auto-discovery process.
  In the corresponding ticket, only device templates will be listed that PRTG used to create sensors.
- A new probe connects to the core and must be acknowledged.
- A new cluster node connects to the cluster and must be acknowledged.
- A new version of the software is available.
- A new report is ready for review.
- In a few other situations, such as when the system runs out of disk space, for licensing issues, when an error occurs, etc.
- A notification 2829 opened a ticket if set in the notification settings.
- A user opened a ticket.

Overall, there are three types of tickets:

- **User Tickets**: Tickets created by PRTG users, for example, to assign monitoring related tasks to a particular PRTG user (or user group)
- **ToDo Tickets**: Tickets created by PRTG to show important system information and in case of specific system events. They are assigned to the PRTG System Administrator user and cannot be turned off.
  The **Related Object** of ToDo tickets is **System**.
- **Notification Tickets**: Tickets created via **Notifications** 2829 in case of monitoring alerts

States of Tickets

Tickets can have three different states depending on the working process regarding the corresponding issue:

- **Open**: New tickets will be open as long as the corresponding issue exists as described in the ticket.
- **Resolved**: The issue as described in the ticket does not persist any longer. Someone took care of it.
- **Closed**: Usually, the ticket has been resolved before, the solution to the issue has been checked for correctness, and the ticket does not require any other action.

Tickets (Main Menu)

This option is only shown in the main menu bar if the user group of the current user is allowed to use the ticket system. You can turn off tickets for particular user groups in System Administration—User Groups 2982. Users with **read-only** rights are always excluded from the ticket system and cannot see the tickets entry in the main menu bar.

You have several options to display a list of tickets which is filtered to your needs. In the main menu bar 231, hover over **Tickets** to show all available filter options or click directly to show all tickets assigned to the current user. You can also create a new ticket via the main menu. Available options are:

- **My Tickets**
  Click to show all open tickets which are assigned to the current user. Hover over **My Tickets** show other menu items for filtering these tickets depending on their status:
  - **Open**
  - **Resolved**
  - **Closed**
  - **All**

- **All Tickets**
  Click to show all open tickets of all PRTG users. Hover over **All Tickets** to show other menu items for filtering these tickets depending on their status:
  - **Open**
  - **Resolved**
  - **Closed**
  - **All**

- **ToDo Tickets**
  Click to show all open tickets from the type 201 ToDo. Hover over **ToDo Tickets** to show other menu items for filtering these tickets depending on their status:
  - **Open**
    Click to show all open ToDo tickets. Hover over **Open** to show other menu items for filtering these tickets depending on their event type:
    - **Report Related**
    - **Auto-Discovery Related**
    - **Probe Related**
    - **System Errors**
    - **New Software Version**
  - **Resolved**
  - **Closed**

- **All**

- **Open Ticket**
  This will open the **New Ticket** dialog. In the first step, select the object on which you want to focus in the ticket via the **Object Selector** 210. Click **Continue**.
  You can leave this step out when using the context menu 215 of this object in the device tree to open the ticket.

  In step 2, provide the following information and confirm by clicking on **Save** to create a User Ticket:

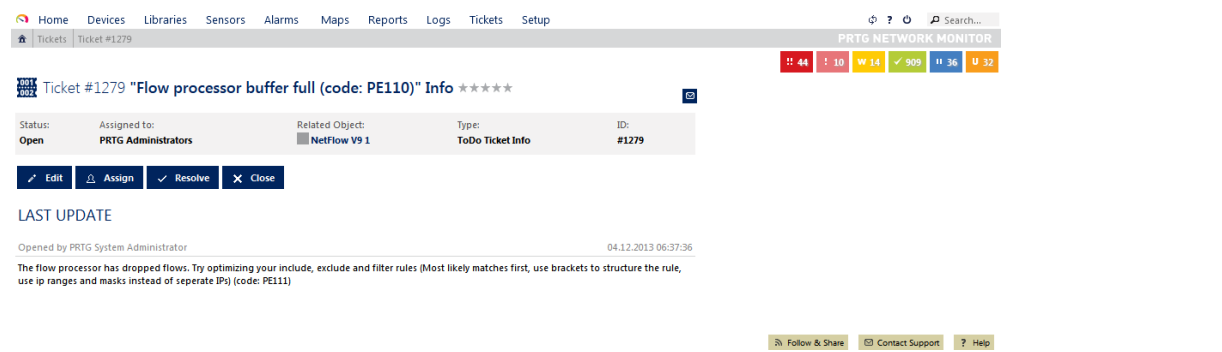
  - **Subject**: Enter a meaningful title for the ticket which indicates the topic of the issue.
  - **Assigned to**: Select a user (or user group) who will be responsible for this issue from the dropdown list.
  - **Priority**: Define a priority 211 from one to five stars.
  - **Comments**: Enter a text message. This message should describe the issue in detail.

After selecting the desired filter or opening a new user ticket, a corresponding list of tickets will appear. In this table list, you can re-sort the items by using the respective options 207. Additionally, you have several search options using the inline filter directly above the table. The following filters are available:

- **Ticket status**: all, open, resolved, closed
- **Ticket type**: User, ToDo, Notification
- **Concerned user(s)**: Show only tickets that are assigned to a specific user or user group. There are the following types:
  - **anyone**: no user filter is applied so all tickets on this PRTG server are shown
  - **me**: show tickets that are assigned to you (the user who is currently logged in)
  - **Groups**: show tickets that are assigned to a specific user group only
  - **Users**: show tickets that are assigned to a specific user only
  - **Disallowed**: users or user groups that do not have access rights to the selected object are displayed under Disallowed. This for your information only; you cannot select them!
- **Relationship** to a monitoring object: Choose groups, probes, devices, sensors with the **Object Selector** 210.
  ToDo tickets are related to **System**.

- **Time span** to view tickets by last edit of a ticket: Use the date time picker to enter the date and time.

Click on the subject of a ticket to open the ticket's detail page. There you can find all related information, as well as conduct several actions.



An Open ToDo Ticket with Instructions

Actions

For best experience with PRTG, check every ticket and select appropriate actions.

Only members of user groups that have the corresponding access rights 129 can view and edit tickets that are related to a certain monitoring object.

The following actions are available when viewing the tickets list or a specific ticket:

- **Edit**: Opens a dialog where you can change the subject and the priority of the ticket, as well as assign the ticket to another user. Furthermore, you can add a text message to this ticket. Confirm your changes by clicking **Save**.
- **Assign**: Opens a dialog where you can give the ticket to another user. Select a user (or user group) via the dropdown menu. Furthermore, you can add a text message to this ticket. Confirm your assignment by clicking **Save**.
- **Resolve**: Opens a dialog where you can resolve the ticket by clicking **Save**. The status resolved indicates that the issue as described in this ticket does not persist. Furthermore, you can add a text message to this ticket which indicates, for example, what has been done concerning the issue.
- **Close**: Opens a dialog where you can close the ticket by clicking **Save**. Usually, this ticket has been resolved before and the correct solution of the issue has been checked. Furthermore, you can add a text message to this ticket.
- **Reopen**: Opens a dialog where you can reopen a ticket after it has been resolved or closed. Do so, for example, if the solution of the issue turned out to be incorrect. Furthermore, you can add a text message to this ticket that indicates, for example, why you have opened the ticket again. Confirm reopening and assignment by clicking **Save**.

Tickets as Emails

You can receive all tickets that are assigned to you or to your user group as emails. You will also be notified via email each time this ticket is edited. This way, you will always be informed about new notifications (if set), important system information (if PRTG System Administrator), or within the communication with other PRTG users. You can turn off the setting **Tickets as Emails** in System Administration—User Accounts 2975. If you disable emails for tickets for a user account, this particular user will not receive any ticket emails anymore.

If you have defined to get tickets as emails and you are PRTG System Administrator, you will receive emails for ToDo tickets as well, although ToDo tickets are considered to be opened by the PRTG System Administrator.

More

Paessler Blog: A New Feature Was Assigned to You in PRTG: Ticket System Keeps Track of Network Monitoring Issues

- https://www.paessler.com/blog/2014/02/03/prtg/ticket-system-keeps-track-of-network-monitoring-issues

Ajax Web Interface—Basic Procedures—Topics

- Login 138
- SSL Certificate Warning 142
- Welcome Page 145
  - Customer Service 149
- General Layout 151
- Sensor States 163
- Review Monitoring Data 166
- Compare Sensors 172
- Historic Data Reports 175
- Similar Sensors 180
- Recommended Sensors 184
- Object Settings 188
- Alarms 190
- System Information 193
- Logs 198
- Tickets 200
- Working with Table Lists 207
- Object Selector 210
- Priority and Favorites 211
- Pause 214
- Context Menus 215
- Hover Popup 230
- Main Menu Structure 231

Other Ajax Web Interface Sections

- Ajax Web Interface—Device and Sensor Setup 248
- Ajax Web Interface—Advanced Procedures 2804

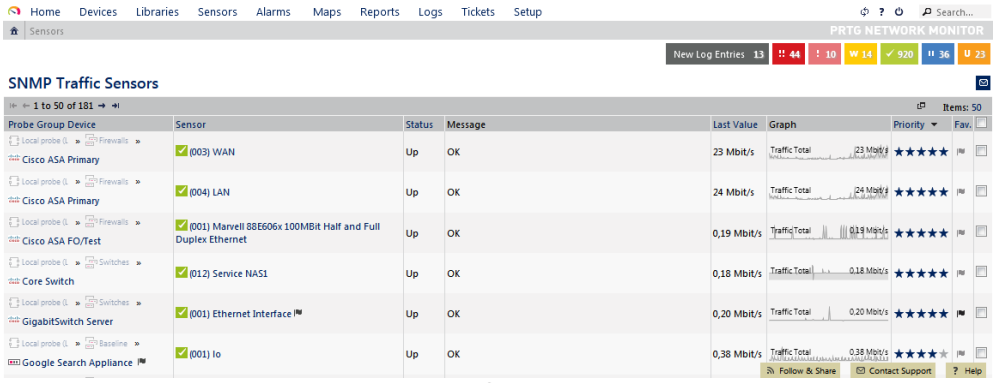
Related Topics

- Enterprise Console 3028
- PRTG Apps for Mobile Network Monitoring 3082

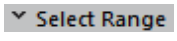
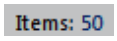
6.16 Working with Table Lists

Throughout the web interface you often see table lists of items, for example, sensor or device lists. Table lists are also available on the overview pages of Libraries 2845, Maps 2885, Reports 2862, Notifications 2829, and Schedules 2938, as well as in Logs 198 and Tickets 200. All these provide common functionality. Depending on the type of content in the list, tables show various information in their columns for each object.

On certain overview pages, like for sensors 236, tickets 202, and similar sensors 182, there is also an in-line filter available directly above the table. The filter options depend on the current page.



Example of a Table List

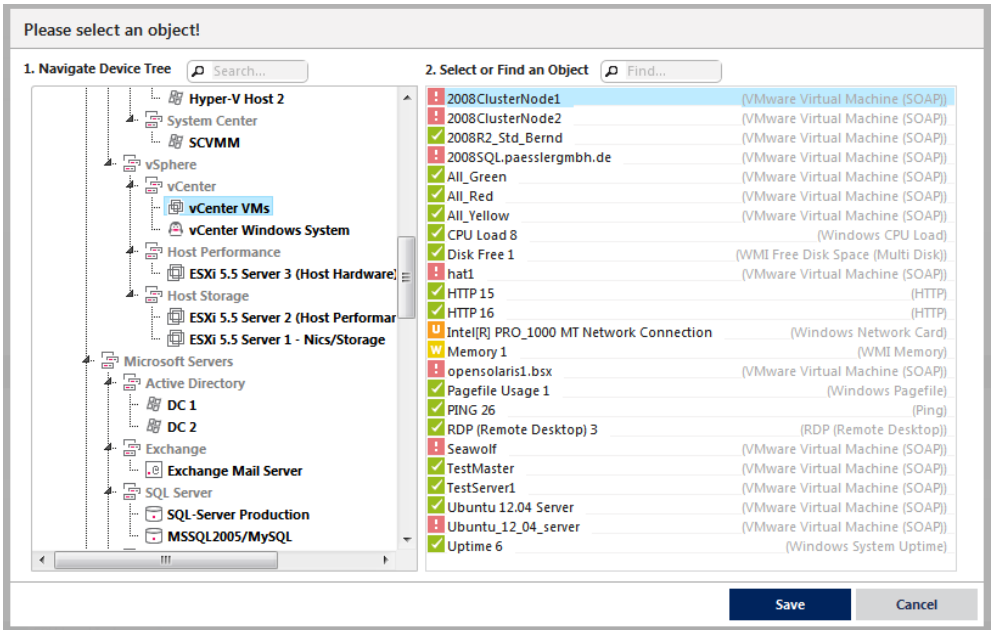
FEATURE	DISPLAY	WHAT IT DOES
Paging		The content of a table is displayed over several pages. Click the arrow symbols at the beginning or the end of a list to view other pages, or to jump to the beginning or the end of the list.
New Window		Click the window symbol at the beginning or end of a list to open the table in a new window.
Date Range		Use the date and time picker to show table list entries within a specific time span. Click the first date field for the start date and the second field for the end date. A calender dialog opens where you can select date and time. Click the **Done** button to apply the selected date and time.
Select Range		When viewing log lists (not available in other lists), click **Select Range** in the upper-right corner of the list to select the time span you want to show log entries for. Choose between **Today**, **Yesterday**, and several other time spans. Choose **Unlimited** to disable this filter again.
Items		Click **Items** at the beginning or end of the list to select how many rows are shown on each page. Choose between **50**, **100**, **500**, and **1000**.

Related Topics

- Multi-Edit Lists 2814

6.17 Object Selector

For some functions, the object selector is shown. It enables you to browse all objects in your configuration and select an object in two steps.



Object Selector

Step 1: Navigate Device Tree

On the left-hand side, you see a device tree specific to your setup that you can browse by clicking the corresponding nodes. Click a device to view its sensors on the right-hand side.

You can directly browse for objects in the device tree by entering a probe name, group name, or device name into the **Search...** field above the device tree navigation. You can also use a substring only. The resulting objects will be displayed immediately without any manual confirmation.

Step 2: Select an Object

If you have selected a device on the left-hand side, you will see the sensors on this device here, on the right-hand side. Also, the sensor type is shown. Hover over a sensor on the right side to view its parent device and group.

You can also directly search and find sensors by entering the sensor name, group name, device name, or tag into the **Find...** box above the sensor list.

Select an object and click the **Save** button.

6.18 Priority and Favorites

You can set priorities for all your monitoring objects and also categorize devices or sensors as favorites. Both settings affect how your objects are displayed.

Settings for priority and favorites are stored for the entire installation. They are not user specific.

Priority for All Objects

The priority setting affects the order in which your objects are displayed when you view table lists. PRTG lists objects with a higher priority first, others underneath, depending on their own priority. Furthermore, device overview pages display gauges 166 for sensors with a high priority.

To change priority settings, right-click an object to open the context menu 215 and select **Priority**. You can choose between 5 stars ***** (top priority) and one star * (lowest priority). By default, all objects are set to medium priority (3 stars ***). In the page header bar and in lists, you can set a priority directly with one click on a star, for example, for sensors on a device overview page.

Context Menu: Priority

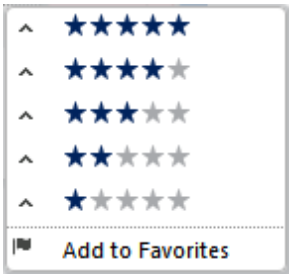
Select 4 or 5 stars for particular sensors to activate their gauges on device overview pages.

Select 5 stars for a map to show it as an entry in the main menu bar 231 under **Home**.

Favorites for Devices and Sensors

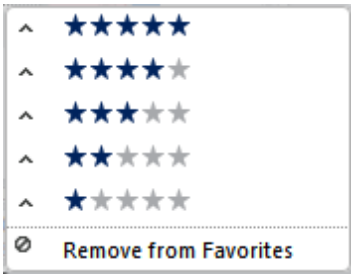
To call a list of all your favorite devices or sensors, select **Devices | Favorite Devices** or **Sensors | Favorite Sensors** from the main menu. These lists are sorted by priority as well.

You can mark any device or sensor as favorite to add it to the favorite list. Right-click it to open the context menu 215. Select **Priority/Favorite | Add to Favorites**. A small black flag symbol will be added next to the object's name.



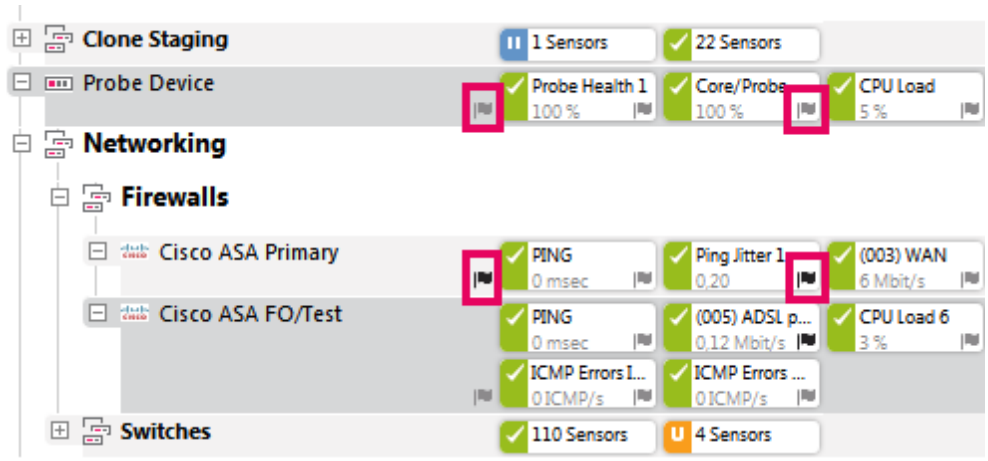
Context Menu:
Priority/Favorites (Add)

To remove an object from the favorites list, select **Priority/Favorite | Remove from Favorites** from the context menu 215.



Context Menu:
Priority/Favorites (Remove)

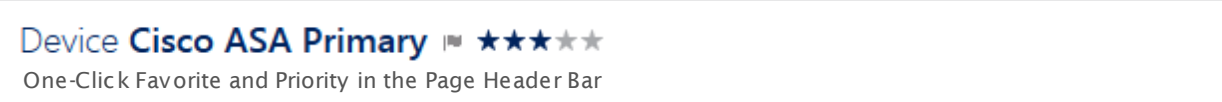
There is also the option to add a device or sensor to favorites with one click in the device tree. Just click the small flag symbol to the right of the respective object name. If the flag is black, the specific object is already a favorite; clicking the flag again will remove it from favorites and the flag will turn gray again.



One-Click Adding to Favorites in the Device Tree

Priority and Favorites in the Page Header Bar

You can add any device or sensor to favorites on its details page by clicking the small flag symbol in the page header bar[155]. If the flag is black, the selected object is already a favorite. Clicking the flag again will remove it from favorites and the flag will turn gray again. It is also possible to set the priority of the object by clicking one of the five stars in the page header; five stars ***** means top priority, one star * is the lowest priority.



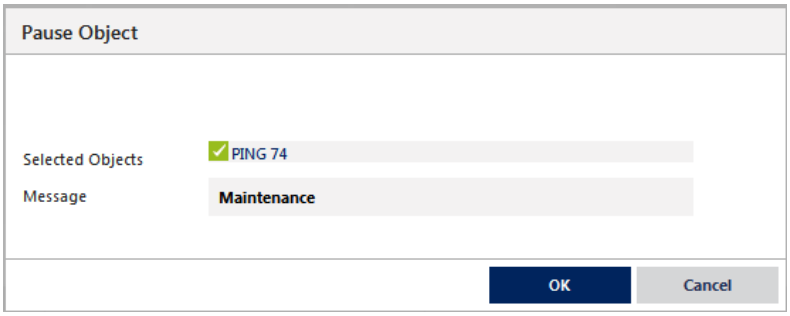
One-Click Favorite and Priority in the Page Header Bar

6.19 Pause

While a sensor is paused, it will not collect any monitoring data, will not change its status 163, and will not trigger any notifications 128. You can pause monitoring for every object by selecting **Pause** from the context menu 215 of a probe, a group, a device, or a sensor. All sensors on this object will then be paused. You can choose **Pause Indefinitely**, or select a time after which monitoring will resume automatically, such as **5** or **15 minutes**, **1** or **3 hours**, **1 day**, or **Until** a certain date. You can also set up a one-time maintenance window to pause sensors automatically at a specified time.

When selecting the **Pause** symbol from an object's hover popup 230 or while using multi-edit 2814, the object(s) will be paused indefinitely until resumed.

When selecting a pause option, you are prompted to enter a message. This will be shown in the status message of the object as long as it is paused. Confirm with **OK** to pause the object or click **Cancel** to not pause it.



PRTG Pause Message Prompt

Monitoring for objects can also be paused by applying a schedule (see **Account Settings—Schedules** 2938) in the **Object Settings** 188. If you pause a master object by schedule or manually, you do not trigger a status change by dependency 126.

Inheritance and Resume

If you pause monitoring for an object in the device tree 151, all child objects underneath will be paused as well. For example, when pausing a group, all sensors on all devices in it will also be paused. Once an object is paused, you can resume monitoring any time by selecting **Resume** from the context menu 215. However, you cannot resume monitoring for single child objects that are paused by a parent object, only for the object you originally set to pause.

Also after a restart of PRTG, a pause status will be kept.

6.20 Context Menus

Right-click on an object to view a context menu with many options for direct access to monitoring data and functions. You can also access many of the functionalities via the main menu 231 or the hover popup 230 window. However, using the context menus is the easier way in most cases.

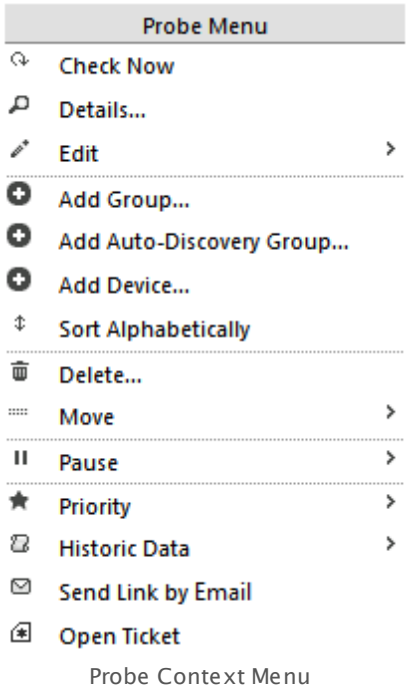
To view your browser's context menu, hold down the Ctrl key (Chrome) or the Shift key (Firefox) while right-clicking. You will then see the menu of your browser instead of the PRTG menu. This is not possible with Internet Explorer.

The content of the PRTG context menu varies, depending on the type of object you have selected. Please see the following subsections for an overview of the available options.

- Probe Context Menu 215
- Group Context Menu 219
- Device Context Menu 222
- Sensor Context Menu 226

Probe Context Menu

The **Probe Menu** contains actions for your local probe, remote probes, or mini probes 119.



Probe Context Menu

PROBE MENU

Check Now

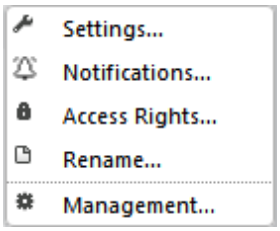
Perform an immediate scan for the selected probe. This queries the data for all devices and sensors underneath in the object hierarchy 118.

Details...

Show the overview tab 166 of the selected probe.

Edit ›

Hover over **Edit** to show the **Edit** menu.



Edit Menu

The following actions are available:

- **Settings...**
  Open the **Probe Settings** 312 tab of this probe.
- **Notifications...**
  Open the **Notifications** 2829 tab of this probe.
- **Access Rights...**
  Open an assistant to edit **User Access Rights** 129 for this probe.
- **Rename...**
  Open an assistant to edit the name of this probe.
- **Management...**
  Open the **Management** 292 tab of this probe.

Add Group...

Open an assistant that guides you through the process of adding a new group to the selected probe. For detailed instructions, please see **Add a Group** 268.

Add Auto-Discovery Group...

Open an assistant that guides you through the process of adding a new auto-discovery group to the selected probe. PRTG creates a new group and runs an auto-discovery in your network to add devices and sensors automatically. For more information, please see section **Using the Auto-Discovery** 249.

This option is not available for local probes in PRTG on demand.

PROBE MENU

Add Device...

Open an assistant that guides you through adding a new device to the selected probe. For detailed instructions, please see Add a Device 275.

Sort Alphabetically

Sort direct children (groups and devices) of the selected probe in alphabetical order.

The ordering is stored in the monitoring configuration and cannot be revoked.

Delete...

Delete the selected probe. PRTG will ask for confirmation before anything is actually deleted.

Move ›

Hover over **Move** to open the **Move** menu.

Move Menu

The following actions are available:

- **Top**: Move the probe to the top of the root group.
- **Up**: Move the probe one entry up under the root group.
- **Down**: Move the probe one entry down under the root group.
- **Bottom**: Move the probe to the bottom of the root group.
- **Management...**: Open the Management 292 tab of the probe.

Pause ›

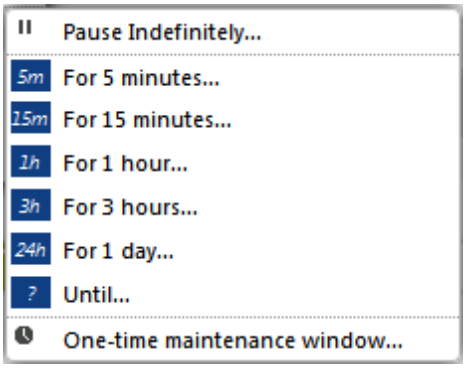
Hover over **Pause** to open the **Pause** menu.

—or—

Resume

If the probe is already in paused or in "simulate error" status, **Resume** appears. Click to restart monitoring on this probe.

PROBE MENU



Pause Menu

You can pause and resume monitoring on the selected probe. The monitoring for all sensors in the object hierarchy [118] underneath will be paused or resumed.

You can choose between: **Pause Indefinitely...**, pause **For 5 Minutes...**, **For 15 Minutes...**, **For 1 Hour...**, **For 3 Hours...**, **For 1 Day...**, or **Pause Until...**. If you choose **Pause Until...**, an assistant appears where you can define a date. Use the date time picker to enter the date and time. PRTG will resume monitoring after this date.

You can directly add a **One-time maintenance window** to pause monitoring during a planned downtime. In the appearing assistant, define the start and end date of the maintenance window for this probe. Use the date time picker to enter the date and time.

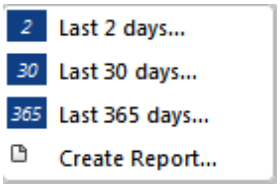
Priority › Hover over **Priority** to open the **Priority** menu.

Context Menu Priority

Define the priority of the selected probe. For details, please see Priority and Favorites [211].

Historic Data › Hover over **Historic Data** to open the **Historic Data** menu.

PROBE MENU



Context Menu Historic Data

The following actions are available:

- Open the historic data report tabs for the specified interval 168: **Last 2 days...**, **Last 30 days...**, or **Last 365 days...**
- **Create Report...**: Open an assistant to add a new report to PRTG. For details, please see **Reports Step by Step** 2866.

Send Link by Email	Send the link to the selected probe by email. Click to create a new email using your system's standard email client. It contains a direct link to the overview tab 166 of the selected probe.
Open Ticket	Open the **New Ticket** dialog. For details, please see the section **Tickets** 203.

Group Context Menu

The **Group Menu** contains actions for your groups 119.

The context menu of the **Root** group is special and differs from the other groups' menu.

GROUP MENU

Check Now	Perform an immediate scan for the selected group. This queries the data for all devices and sensors underneath in the object hierarchy 118.
Details...	Show the overview tab 166 of the selected group.
Edit ›	Hover over **Edit** to show the **Edit** menu. The following actions are available: ▪ **Settings...** Open the **Group Settings** 334 tab of this group.

GROUP MENU

- **Notifications...**
  Open the **Notifications** 2829 tab of this group.
- **Access Rights...**
  Open an assistant to edit **User Access Rights** 129 for this group.
- **Rename...**
  Open an assistant to edit the name of this group.
- **Management...**
  Open the **Management** 292 tab of this group.

Add Group...

Open an assistant that guides you through the process of adding a new group to the selected group. For detailed instructions, please see **Add a Group** 268.

Add Auto-Discovery Group...

Open an assistant that guides you through the process of adding a new auto-discovery group to the selected group. PRTG creates a new group and runs an auto-discovery in your network to add devices and sensors automatically. For more information, please see section **Using the Auto-Discovery** 249.

This option is not available for local probes in PRTG on demand.

Add Device...

Open an assistant that guides you through adding a new device to the selected group. For detailed instructions, please see **Add a Device** 275.

Auto-Discovery

This option is only available for auto-discovery groups. These are groups with automatic device identification or sensor creation enabled 335. Hover over **Auto-Discovery** to show its menu. The following actions are available:

- **Run Auto-Discovery**: Start an automatic search immediately to automatically add new sensors to the selected device. The search runs in the background and uses the option you set in the **Sensor Management** section of the group settings 335. If found, you see new devices with sensors after a few minutes (if found). For more information, please see **Auto-Discovery** 250 (**Run Auto-Discovery Now**).
- **Run Auto-Discovery with Template**: Open an assistant 252 to start an automatic search with a desired device template. This is the **Sensor Management** option **Automatic sensor creation using specific device template(s)**. Other automatic device identification options are not available. The option you set in the **Sensor Management** section of the group settings 335 will not apply.

GROUP MENU

	This option is not available for local probes in PRTG on demand.
Sort Alphabetically	Sort direct children (groups and devices) of the selected group in alphabetical order. The ordering is stored in the monitoring configuration and cannot be revoked.
Delete...	Delete the selected group. PRTG will ask for confirmation before anything is actually deleted.
Clone...	Open an assistant that guides you through cloning the selected group. For detailed instructions, please see **Clone Object** 2812.
Move ›	Hover over **Move** to open the **Move** menu. The following actions are available: ▪ **Top**: Move the group to the top of the mother node (here usually a probe or another group). ▪ **Up**: Move the group one entry up under the mother node. ▪ **Down**: Move the group one entry down under the mother node. ▪ **Bottom**: Move the group to the bottom of the mother node. ▪ **To Other Group...**: Move the group to another group to become a sub-group. ▪ **Management...**: Open the **Management** 292 tab of the group.
Pause › —or— **Resume**	Hover over **Pause** to open the **Pause** menu. If the group is already in paused or in "simulate error" status, **Resume** appears. Click to restart monitoring on this group. You can pause and resume monitoring on the selected group. The monitoring for all sensors in the object hierarchy 118 underneath will be paused or resumed. You can choose between: **Pause Indefinitely...**, pause **For 5 Minutes...**, **For 15 Minutes...**, **For 1 Hour...**, **For 3 Hours...**, **For 1 Day...**, or **Pause Until...**. If you choose **Pause Until...**, an assistant appears where you can define a date. Use the date time picker to enter the date and time. PRTG will resume monitoring after this date.

GROUP MENU

	You can directly add a **One-time maintenance window** to pause monitoring during a planned downtime. In the appearing assistant, define the start and end date of the maintenance window for this group. Use the date time picker to enter the date and time.
Priority ›	Hover over **Priority** to open the **Priority** menu. Define the priority of the selected group. For details, please see **Priority and Favorites** 211.
Historic Data ›	Hover over **Historic Data** to open the **Historic Data** menu. The following actions are available: ▪ Open the historic data report tabs for the specified interval 168: **Last 2 days...**, **Last 30 days...**, or **Last 365 days...** ▪ **Create Report...**: Open an assistant to add a new report to PRTG. For details, please see **Reports Step by Step** 2866.
Send Link by Email	Send the link to the selected group by email. Click to create a new email using your system's standard email client. It contains a direct link to the overview tab 166 of the selected group.
Open Ticket	Open the **New Ticket** dialog. For details, please see section **Tickets** 203.

Device Context Menu

The **Device Menu** contains actions for your devices 120.

DEVICE MENU

Check Now	Perform an immediate scan for the selected device. This queries the data for all sensors underneath in the object hierarchy 118.
Details...	Show the overview tab 166 of the selected device.
Edit ›	Hover over **Edit** to show the **Edit** menu. The following actions are available: ▪ **Settings...** Open the **Device Settings** 360 tab of this device. ▪ **Notifications...** Open the **Notifications** 2829 tab of this device.

DEVICE MENU

- **Access Rights...**
  Open an assistant to edit **User Access Rights** 129 for this device.
- **Rename...**
  Open an assistant to edit the name of this device. You can also select another device icon.

Add Sensor...

Open an assistant that guides you through adding a new sensor to the selected device. For detailed instructions, please see **Add a Sensor** 288.

Auto-Discovery

Hover over **Auto-Discovery** to show the **Auto-Discovery** menu. The following actions are available:

- **Run Auto-Discovery**: Start an automatic search immediately to automatically add new sensors to the selected device. The search runs in the background and uses the option you set in the **Sensor Management** section of the device settings 360. If found, you see new sensors on this device after a few minutes. For more information, please see **Auto-Discovery** 250 (**Run Auto-Discovery Now**).
  If you have set the option **Manual (no auto-discovery)** in the device settings section 362 **Sensor Management** and start the auto-discovery from the context menu, PRTG will run it using the standard device identification and change the device setting to **Automatic device identification (standard, recommended)**. Please note that the Enterprise Console 3072 behaves differently in this case.
- **Run Auto-Discovery with Template**: Open an assistant 251 to start an automatic search with a desired device template. This is the **Sensor Management** option **Automatic sensor creation using specific device template(s)**. Other automatic device identification options are not available, The option you set in the **Sensor Management** section of the device settings 362 will not apply.

  This option is not available for local probes in PRTG on demand.

Create Device Template...

Open an assistant that guides you through creating a new device template. The template is then available in auto-discovery 249. For detailed instructions, please see **Create Device Template** 2818.

Recommend Now

Start an analysis to get sensor recommendations for this device. When PRTG has finished the inspection of the device, you see the sensor recommendations in a table list on the device overview tab 166 where you can add the according sensor types directly.

DEVICE MENU

	This option is only available if the recommendation engine is enabled [2959].
Sort Alphabetically	Sort the sensors on the selected device in alphabetical order. The ordering is stored in the monitoring configuration and cannot be revoked.
Delete...	Delete the selected device. PRTG will ask for confirmation before anything is actually deleted.
Clone...	Open an assistant that guides you through cloning the selected device. For detailed instructions, please see **Clone Object** [2812].
Move ›	Hover over **Move** to open the **Move** menu. The following actions are available: ▪ **Top**: Move the device to the top of the mother node (here usually a probe or group). ▪ **Up**: Move the device one entry up under the mother node. ▪ **Down**: Move the device one entry down under the mother node. ▪ **Bottom**: Move the device to the bottom of the mother node. ▪ **To Other Group...**: Move the device to another group.
Pause › —or— **Resume**	Hover over **Pause** to open the **Pause** menu. If the device is already in paused or "simulate error" status, **Resume** appears. Click to restart monitoring on this device. You can pause and resume monitoring on the selected device. The monitoring for all sensors on this device will be paused or resumed. You can choose between: **Pause Indefinitely...**, pause **For 5 Minutes...**, **For 15 Minutes...**, **For 1 Hour...**, **For 3 Hours...**, **For 1 Day...**, or **Pause Until...**. If you choose **Pause Until...**, an assistant appears where you can define a date. Use the date time picker to enter the date and time. PRTG will resume monitoring after this date. You can directly add a **One-time maintenance window** to pause monitoring during a planned downtime. In the appearing assistant, define the start and end date of the maintenance window for this device. Use the date time picker to enter the date and time.

DEVICE MENU

Priority/Favorite ›

Hover over **Priority/Favorite** to open the **Priority/Favorite** menu. Define the priority of the selected device, or add to or remove it from the favorite devices list. For details, please see **Priority and Favorites** 211.

Historic Data ›

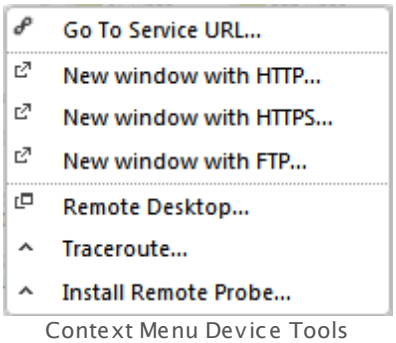
Hover over **Historic Data** to open the **Historic Data** menu. The following actions are available:

- Open the historic data report tabs for the specified interval 168: **Last 2 days...**, **Last 30 days...**, or **Last 365 days...**
- **Create Report...**: Open an assistant to add a new report to PRTG. For details, please see **Reports Step by Step** 2866.

Device Tools ›

Hover over **Device Tools** to open the **Device Tools** menu.

This option is not available for local probes in PRTG on demand.



Context Menu Device Tools

The following actions are available:

- **Go To Service URL...**
  Open the service page that you have defined in the **Device Settings** 360. If there is no service URL available for this device, you can enter an address in the appearing assistant.
- **New window with HTTP...**
  Open a new browser window with Hypertext Transfer Protocol (HTTP) and the IP address / DNS name of the device.
- **New window with HTTPS...**
  Open a new browser window with Hypertext Transfer Protocol Secure (HTTPS) and the IP address / DNS name of the device.
- **New window with FTP...**
  Open a new browser window with File Transfer Protocol (FTP) and the IP address / DNS name of the device.

DEVICE MENU

- **Remote Desktop...**
  Download an .rdp file. When you execute this file, a remote desktop will start with the IP address / DNS name of the device.
  In Firefox you have to use mstsc.exe (Microsoft Terminal Service) to open the file.
- **Traceroute...**
  Start a traceroute on the selected device. PRTG will display the route and measure transit delays of packets across the IP network.
- **Install Remote Probe...**
  Open an assistant to install a **Remote Probe** of PRTG on this device. For more details, please see **Remote Probe Quick Install** 3199
  This option is only available on devices on local probes.

This option is not available in PRTG on demand.

Find Duplicates...	Search in your PRTG configuration for devices with the same IP address or DNS name as the selected device. A window with the results will appear, either showing existing duplicates or a message indicating that there are no duplicates.
Send Link by Email	Send the link to the selected device by email. Click to create a new email using your system's standard email client. It contains a direct link to the overview tab 166 of the selected device.
Open Ticket	Open the **New Ticket** dialog. For details, please see section **Tickets** 203.

Sensor Context Menu

The **Sensor Menu** contains actions for your sensors 120.

SENSOR MENU

Check Now	Perform an immediate scan for the selected sensor.
Details...	Show the overview tab 166 of the selected sensor.

SENSOR MENU

Edit ›

Hover over **Edit** to show the **Edit** menu. The following actions are available:

- **Settings...**
  Open the **Sensor Settings** 384 tab of this sensor.
- **Notifications...**
  Open the **Notifications** 2829 tab of this sensor.
- **Access Rights...**
  Open an assistant to edit **User Access Rights** 129 for this sensor.
- **Rename...**
  Open an assistant to edit the name of this sensor.

Acknowledge Alarm ›

This option is available only in the sensor menu when you select a sensor in a **Down** or **Down (Partial)** status 163.

You can acknowledge an alarm for the selected sensor. An acknowledged alarm will show up in the alarms list as "acknowledged" (see **Sensor States** 163) and will not trigger 2791 any more notifications 2829.

You can choose between: **Acknowledge Indefinitely...**, acknowledge **For 5 Minutes...**, **For 15 Minutes...**, **For 1 Hour...**, **For 3 Hours...**, **For 1 Day...**, or **Until...**. If you choose **Until...** an assistant appears where you can define a date. Use the date time picker to enter the date and time. If the alarm condition still exists after this date, the sensor will show a **Down** status again.

If the alarm condition clears, the sensor usually returns into an **Up** status immediately with the next sensor scan. For details about acknowledging an alarm, please see **Alarms** 191 section.

Delete...

Delete the selected sensor. PRTG will ask for confirmation before anything is actually deleted.

Clone...

Open an assistant that guides you through cloning the selected sensor. For detailed instructions, please see **Clone Object** 2812.

Move ›

Hover over **Move** to open the **Move** menu. The following actions are available:

- **Top**: Move the sensor to the top of the device on which it runs.
- **Up**: Move the sensor one entry up on the device.
- **Down**: Move the sensor one entry down on the device.
- **Bottom**: Move the sensor to the bottom of the device.

SENSOR MENU

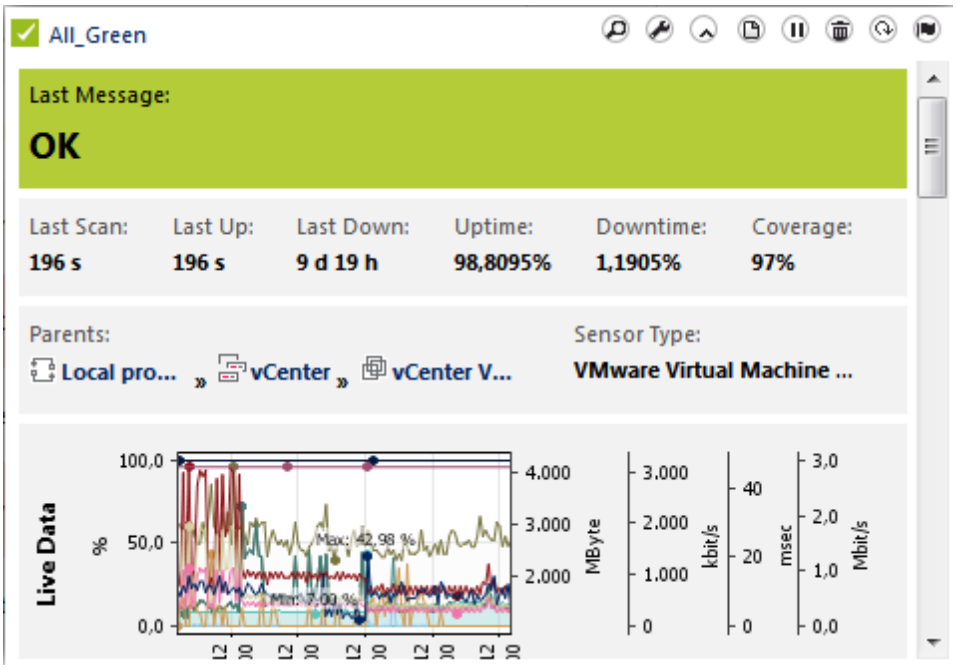
Pause › —or— **Resume**	Hover over **Pause** to open the **Pause** menu. If the sensor is already in paused status[163] or in **Simulate Error Status**, **Resume** appears. Click **Resume** to restart monitoring on this sensor. You can pause and resume monitoring of the selected sensor. Choose between: **Pause Indefinitely...**, pause **For 5 Minutes...**, **For 15 Minutes...**, **For 1 Hour...**, **For 3 Hours...**, **For 1 Day...**, or **Pause Until...**. If you choose **Pause Until...**, an assistant appears where you can define a date. Use the date time picker to enter the date and time. PRTG will resume monitoring after this date. You can directly add a **One-time maintenance window** to pause monitoring during a planned downtime. In the appearing assistant, define the start and end date of the maintenance window for this sensor. Use the date time picker to enter the date and time. Inheritance of the **Schedules, Dependencies, and Maintenance Window** setting from a parent device, group, or probe will be suspended for this timeframe and set again afterwards.
Simulate Error Status	Set the selected sensor to a **Down** status[163]. Like for the paused status, **Resume** will appear in the context menu if a the selected sensor is already in a simulated error status. "Simulate error status" does not work for sensors that run on a PRTG Mini Probe.
Priority/Favorite ›	Hover over **Priority/Favorite** to open the **Priority/Favorite** menu. Define the priority of the selected sensor, or add or remove it from the favorite devices list. For details, please see **Priority and Favorites**[211].
Historic Data ›	Hover over **Historic Data** to open the **Historic Data** menu. The following actions are available: ▪ Open the historic data tab for the specified interval[170]: **Live Data...**, **Last 2 days...**, **Last 30 days...**, or **Last 365 days...** ▪ **Compare...**: Open the **Compare Sensors**[172] assistant with the currently selected sensor. ▪ **View Historic Data**: Open the **Historic Data**[175] tab of this sensor. ▪ **Create Report...**: Open an assistant to add a new report to PRTG. For details, please see **Reports Step by Step**[2866].
Send Link by Email	Send the link to the selected sensor by email. Click to create a new email using your system's standard email client. It contains a direct link to the overview tab[166] of the selected sensor.

SENSOR MENU

Open Ticket	Open the **New Ticket** dialog. For details, please see section Tickets 203.

6.21 Hover Popup

Whenever you rest the mouse pointer for a second over an object's icon in the device tree 151, a hover popup window will appear, showing details about this object. It contains information from the object's overview tab 166, as well as several graphs. The exact information provided depends on the kind of object you are hovering over.



Hover Menu Example: VMware Virtual Machine Sensor

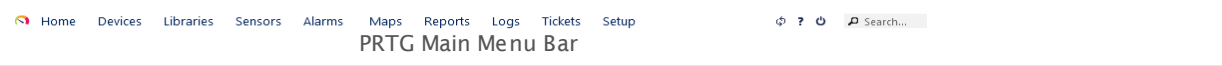
The hover popup only appears if your browser is the currently focused window on your desktop. It disappears with every (automatic) page refresh.

Menu Icons

At the top of the hover popup window, several icons are shown that enable you to view or edit the current object. These are the most important options from this object's context menu 215 which is shown when right-clicking it.

6.22 Main Menu Structure

You can access all functions of PRTG using the main menu. In this section, you find descriptions about the most important menu items. Often, you can either click an item directly, or hover over it to show more items.



PRTG Main Menu Bar

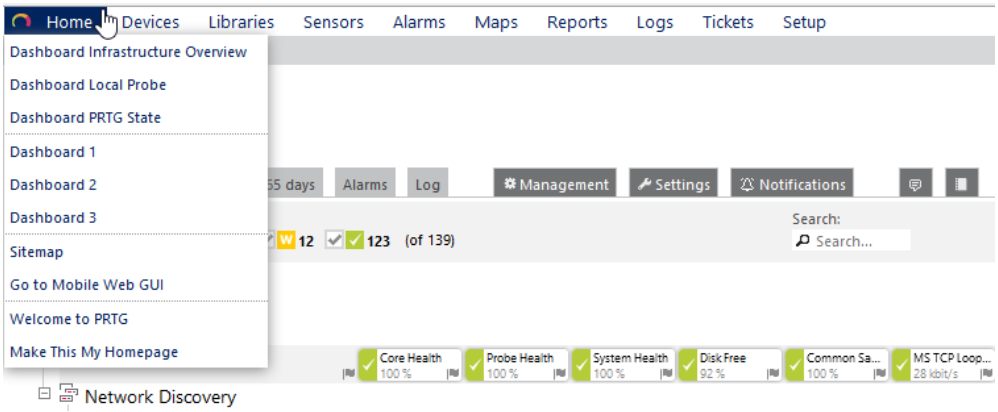
This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

The following menu items are available:

- Home 231
- Devices 233
- Libraries 235
- Sensors 236
- Alarms 239
- Maps 240
- Reports 240
- Logs 241
- Tickets 242
- Setup 243
- Refresh (Arrows Symbol) 245
- Help Center (? Symbol) 245
- Logout (Off Symbol) 246
- Search Box 246

Home

Click to open the user's homepage. The default setting is the PRTG welcome page 151. You can change the homepage in the user account settings 2909. Point to **Home** to show other menu items.



PRTG Main Menu: Home

HOME

Sample Dashboard

Open a preconfigured dashboard to view monitoring data in another layout. Dashboards provide different preset overviews with the status of your sensors. This dashboard is one of the default **Maps** [2885] that PRTG creates automatically with a new installation.

The **Home** menu shows maps that have a 5***** priority [211]. You can include up to 10 map entries in this menu.

You can change the appearance of the default dashboard with the **Map Designer** [2893]. To not show the sample dashboard in the menu, define a priority [211] lower than 5***** for this map.

This option is not available in PRTG on demand.

Dashboard 1 – Dashboard 3

Choose a preconfigured dashboard to view monitoring data in another layout. Dashboards provide different preset overviews with the status of your sensors.

These dashboards are not customizable. You can create your own overview pages using the **Maps** [2885] feature. New installations of PRTG do not include these dashboards anymore.

This option is not available in PRTG on demand.

Switch Cluster Node ›

This option is only available if PRTG runs in **Clustering** [116] mode. Show available cluster nodes. Hover over **Switch Cluster Node** to show other menu items. Follow the menu path (it is specific to your setup) to select another cluster node. The current Master node is shown in bold letters. Click on a node's name to leave the current node and connect to the other, showing the same page there.

HOME

This option is not available in PRTG on demand.

Sitemap

Open the sitemap, which contains a flat text view of all menu items. You can easily search for key words using the search function in your browser (usually shortcut CTRL+F).

Welcome to PRTG

Open the **Welcome Page** 145 that shows the Paessler news feed and various information about your PRTG installation, and it provides quick links to major sections of the web interface.

This is the default homepage of the PRTG web interface.

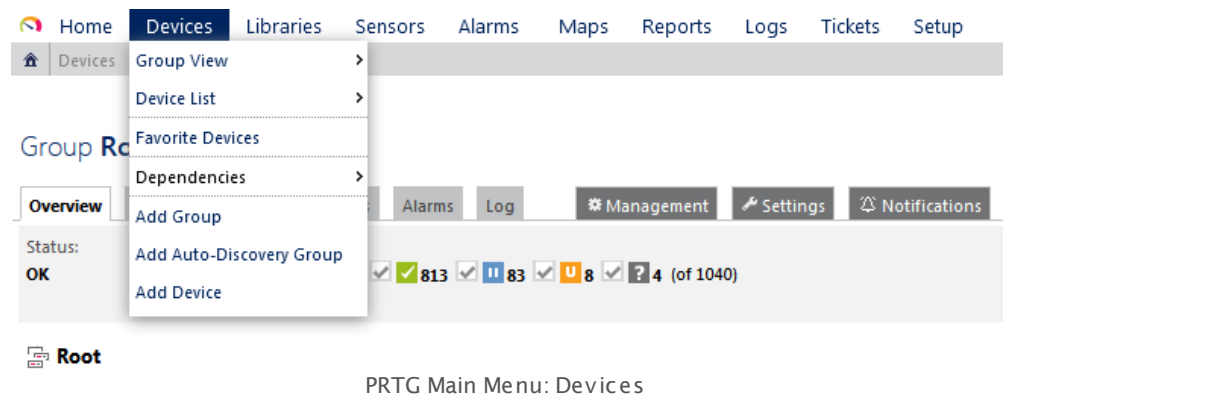
Make This My Homepage

Change the page that is loaded when you click the **Home** button in the main menu. Select this command on any page to set its URL as the current user's homepage. This setting is user sensitive. The default homepage is /welcome.htm.

You can change this setting any time by clicking this command again, or by changing the **Homepage URL** in the **My Account** 2909 settings.

Devices

Click to show a group view of all your devices, starting with the **Root** group, which contains all other groups of your setup. Hover over **Devices** to show other menu items.



PRTG Main Menu: Devices

DEVICES

All	Open the **Overview** tab of the **Root** 118 group that shows a group view of all your devices (the device tree).
Group View ›	Open a tree view of all probes and groups in your setup. Click to show a group view of all your devices, starting with the **Root** 118 group, which contains all other groups of your setup. Hover over **Group View** to show other menu items. Follow the menu path (it is specific to your setup) to view the devices in a specific probe or group only.
Device List ›	Open a list view of all devices in your setup. Click to show a table list of all devices in your setup. Hover over **Device List** to show other menu items. Choose **Favorite Devices** to show a list of all devices marked as **Favorite** 211. Follow the menu path (it is specific to your setup) to view a table list of the devices in a specific probe or group only. ⓘ In the table list 207 that appears, you can re-sort the items by clicking the column's header items. ⓘ In device lists, you can use the **Print QR-Codes** button to show the QR codes of all devices in this list in a printable layout. You can change the size of the QR codes by changing the values of the according parameters width, height, and margin in the URL.
Favorite Devices	Open a table list of all devices marked as **Favorite** 211. Click the **Print QR-Codes** button to show a printable list of the QR codes of all your favorite devices. ⓘ To mark any device as a favorite device, select **Priority / Favorite	Add to Favorites** from its context menu or click the small flag on a device's details page.
Dependencies ›	Open an overview list of the **Dependencies** 126 configured for the objects in your setup. Hover over the menu item to show other menu items. Choose between **Selected Dependencies** and **Master Dependencies** to view a list of all dependencies or explicit ones. You can select dependencies and define master dependencies in the **Schedules, Dependencies, and Maintenance Windows** settings of a monitoring object 188 (not available for the **Root** group). Click **Dependencies Graph** 2822 to visualize the dependencies between objects in your configuration. Follow the menu path (it is specific to your setup) to view dependencies of the objects in a specific probe or group only.

DEVICES

Add Group

Start an assistant that guides you through the process of adding a new group to your setup. For more information, please see section Create Objects Manually 267.

You can create new groups much faster by choosing **Add Group...** from a probe's or group's context menu.

Add Auto-Discovery Group

Start an assistant that guides you through the process of adding a new auto-discovery group to your setup. PRTG will create a new group and run an auto-discovery in your network to add devices and sensors for these devices automatically. For more information, please see section Using the Auto-Discovery 249

You can create new groups much faster by choosing **Add Auto-Discovery Group...** from a probe's or group's context menu.

This option is not available for local probes in PRTG on demand.

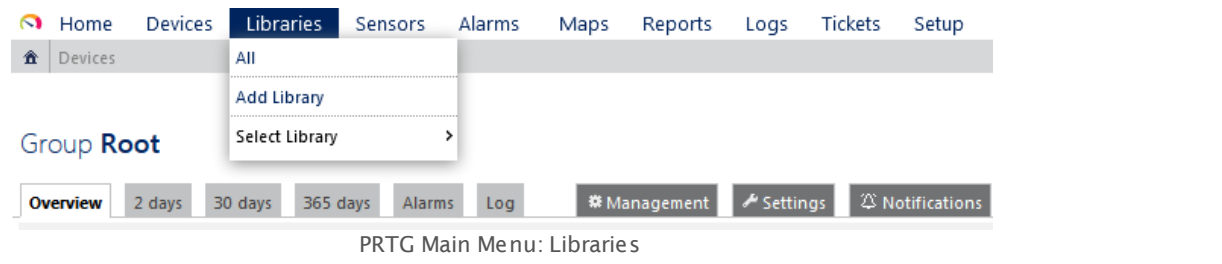
Add Device

Start an assistant that guides you through the process of adding a new device to an existing group. During the process, you can choose if PRTG will run an auto-discover for the new device to add sensors automatically. For more information, please see section Create Objects Manually 267.

You can create new devices much faster by choosing **Add Device...** from a group's context menu.

Libraries

Click to open the Libraries overview list where you can view or add custom views of your network status and monitoring data. For more information, please see Libraries 2845 section. Hover over **Libraries** to show other menu items.



PRTG Main Menu: Libraries

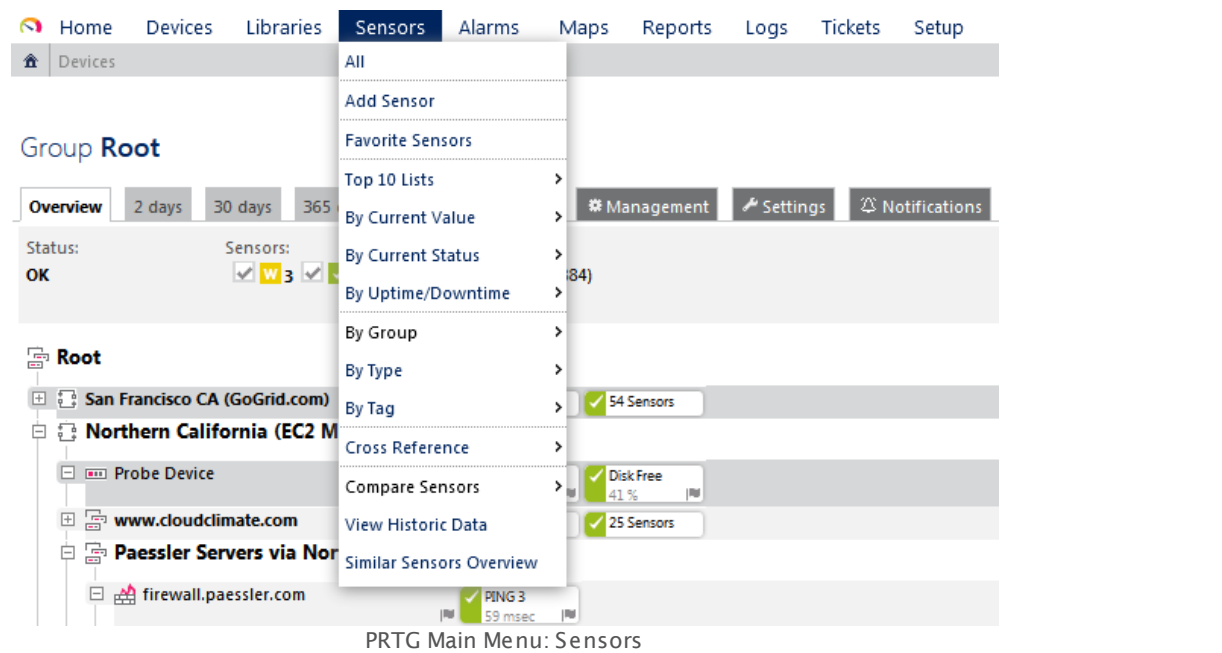
LIBRARIES	
All	Open the Libraries overview list where you can view or add custom device tree views of your network status and monitoring data.
Add Library	Open an assistant to directly create 2848 a new library.
Select Library	Open an existing library. Hover over **Select Library** to show other menu items. Follow the menu path (it is specific to your setup) to select a library and open it.

Sensors

Click to show a table list of all sensors 120. In the table list 207 that appears, you can re-sort the items by clicking the column's header items and you can filter the list by related object and tag with the inline filter directly above the table. Hover over **Sensors** in the main menu bar to show other menu items.

The column **Last Value** shows only the last value of the sensor's **primary channel**.

For most sensor lists, you can use **Multi-Edit** 2814 to change the settings of more than one sensor at once.



PRTG Main Menu: Sensors

SENSORS

All

Open a table list 207 of all sensors 120. In the table list appearing, you can re-sort the items by clicking the column's header items.

The column **Last Value** shows only the last value of the sensor's **primary channel**.

Add Sensor

Start an assistant that guides you through the process of adding a new sensor to an existing device. For more information, please see section **Add a Sensor** 288. During the process, you can also choose to create a new device via the **Add a Device** 275 assistant (that you can also open from the "Devices" menu 233 directly).

Favorite Sensors

Open a table list of all sensors which you marked as **Favorite** 211.

To mark any sensor as a favorite sensor, select **Priority / Favorite | Add to Favorites** from its context menu or click the small flag on a device's details page.

Top 10 Lists ›

Open a dashboard view with different top 10 lists which show best or worst uptime, Ping, bandwidth usage, website response times, CPU usage, disk usage, memory usage, and system uptime. Click to show top 10 lists for all sensors. Hover over **Top 10 Lists** to show other menu items. Follow the menu path (it is specific to your setup) to view top 10 lists for a specific probe or group only.

The shown sensors are selected by default tags.

By Current Value ›

Open a list of sensors filtered by value. Hover over **By Current Value** to show other menu items. Follow the menu path to view table lists 207 of **Fastest** or **Slowest** sensors for

- **Ping**
- **Port**
- **Webpages**
- **IMAP/POP3/SMTP**
- **FTP**

as well as a list of sensors with **Most Used** or **Least Used**

- **Bandwidth Sensors**
- **CPUs**
- **Disks**
- **Memory**

The shown sensors are selected by default tags.

SENSORS

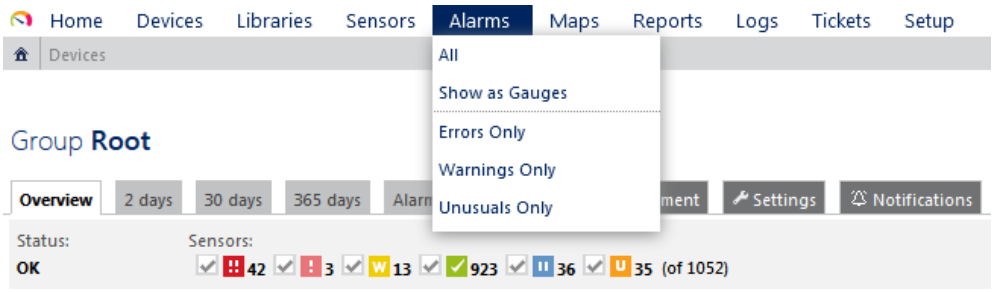
By Current Status ›	Open a list of sensors filtered by status. Hover over **By Current Status** to show other menu items. Follow the menu path to view table lists 207 of all sensors in a certain status. For more information about sensor states, please see **Sensor States** 163 section.
By Uptime/Downtime ›	Open a list of sensors filtered by different parameters. Hover over **By Uptime/Downtime** to show other menu items. Follow the menu path to view table lists 207 of all sensors sorted by ▪ **Best Uptime (%)** ▪ **Highest Uptime (Time)** ▪ **Worst Downtime (%)** ▪ **Highest Downtime (Time)**
By Group ›	Open a list of sensors filtered by their parent group. Hover over **By Group** to show other menu items. Follow the menu path (it is specific to your setup) to view a sensor table list 207 of a specific probe or group only.
By Type ›	Open a list of sensors filtered by sensor type 385. Hover over **By Type** to show other menu items. Follow the alphabetical menu path (it is specific to your setup) to view a sensor table list 207 containing only sensors of one specific sensor type.
By Tag ›	Open a list of sensors filtered by tag 124. Hover over **By Tag** to show other menu items. Follow the alphabetical menu path (it is specific to your setup) to see available tags. Select a tag to view a table list 207 containing only sensors marked with this tag.
Cross Reference ›	Open the sensor cross reference to show information about all sensors including priority and favorite status 211, scanning interval 307, access rights 129, notification trigger settings 188, schedule 127, and dependency 126. Click to show a sensor cross reference for all sensors. Hover over **Cross Reference** to show other menu items. Follow the menu path (it is specific to your setup) to view cross reference information for sensors in a specific probe or group only, or to view them by type or tag.
Compare Sensors ›	Compare the data graphs of two or more sensors. Hover over **Compare Sensors** to show other menu items. Follow the menu path to open an assistant for comparing several monitoring objects. For more information, please see **Compare Sensors** 172 section.

SENSORS

View Historic Data	Open an assistant for a quick generation of sensor data reports. For more information, please see **Historic Data Reports** 175 section.
Similar Sensors Overview	Open an overview page with a list of similar sensors. For more information, please see **Similar Sensors** 180 section.

Alarms

Click to show all sensors that currently show a **Down**, **Down (Partial)**, **Warning**, or **Unusual** status. In the table list 207 that appears, you can re-sort the items by clicking the column's header items. If you select **Show as Gauges**, this command displays the sensor gauges 166 in a size corresponding to their priority. Hover over **Alarms** to show other menu items.



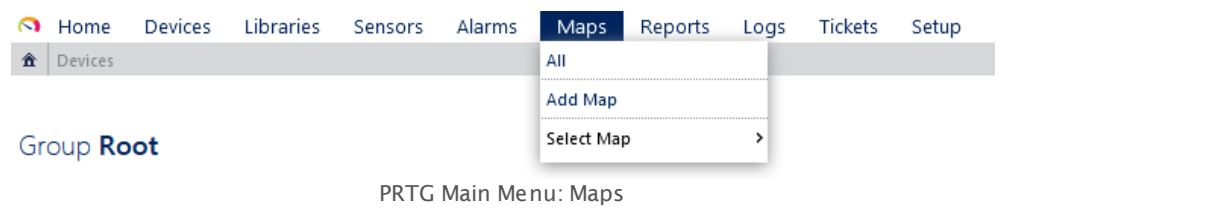
PRTG Main Menu: Alarms

ALARMS

All	Open a list of all sensors that are currently in **Down**, **Down (Partial)**, **Down (Acknowledged)**, **Warning**, or **Unusual** status 163.
Show as Gauges	Open a page with the gauges of all sensors that are currently in **Down**, **Down (Partial)**, **Down (Acknowledged)**, **Warning**, or **Unusual** status. The size of the sensor gauges corresponds to their respective priority.
Errors Only	Open a list of all sensors that are currently in **Down**, **Down (Partial)**, or **Down (Acknowledged)** status.
Warnings Only	Open a list of all sensors that are currently in **Warning** status.
Unusuals Only	Open a list of all sensors that are currently in **Unusual** status.

Maps

Click to open the Maps overview page where you can view or add custom views of your network status and monitoring data. For more information, please see **Maps** 2885 section. Hover over **Maps** to show other menu items.



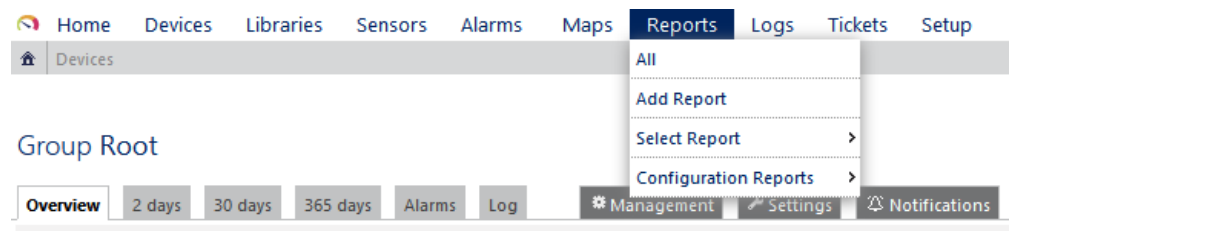
PRTG Main Menu: Maps

MAPS

All	Open the Maps overview page where you can view or add custom views of your network's status and monitoring data.
Add Map	Open an assistant to directly add 2890 a new map.
Select Map ›	Open an existing map. Hover over **Select Map** to show other menu items. Follow the menu path (it is specific to your setup) to select a map.

Reports

Click to open the Reports overview page where you can view or add reports of your monitoring data. For more information, please see **Reports** 2862 section. Hover over **Reports** to show other menu items.



PRTG Main Menu: Reports

REPORTS

All	Open the Reports overview page where you can view or add reports of your monitoring data.

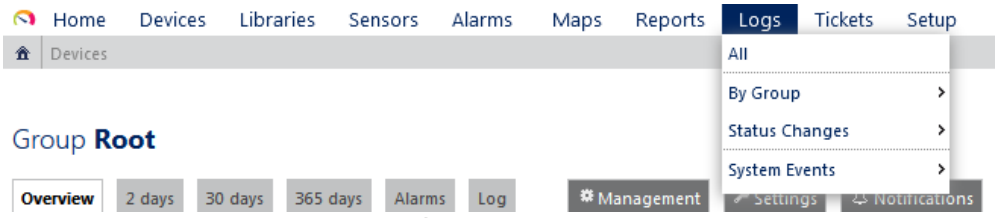
REPORTS

Add Report	Open an assistant to directly add 2866 a new report.
Select Report ›	Open an existing report. Point to **Select Report** to show other menu items. Follow the menu path (it is specific to your setup) to select a report.
Configuration Reports ›	Create reports for maps, reports, users & user groups, and system configuration to document changes to the configuration. Point to **Reports | Configuration Reports** to see the available configuration reports 2865.

Logs

Click to show log information for all objects in your configuration, newest first. In the table list 207 appearing, you can filter the items by using the respective options 207. Hover over **Logs** to show other menu items. For more information, please see **Logs** 198 section.

Logs for monitoring objects (for example, sensors) are available as long as you define **Logfile Records** in the **Historic Data Purging** settings under **System Administration—Core & Probes** 2972.



PRTG Main Menu: Logs

LOGS

All	Open a table list 207 with log information for all objects in your configuration, newest first.
By Group ›	Open a list with log information for objects in a certain group only, newest first. Hover over **By Group** to show other menu items. Select **All**, or follow the menu path (it is specific to your setup) to select a group you would like to show log information for.

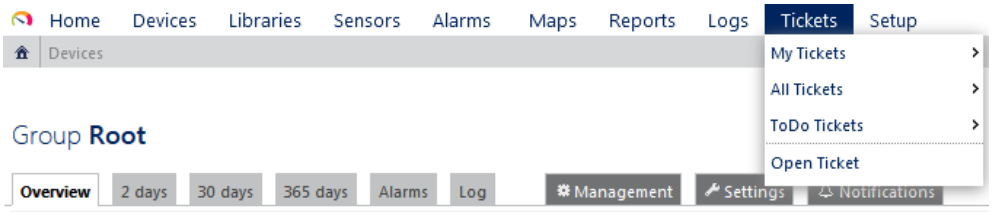
LOGS

Status Changes ›	Open a list with log information for certain status changes only. Hover over **Status Changes** to show other menu items. Follow the menu path to view log entries with a special value in the **Status** field only. Select between **Up & Down** (shows entries with either **Up** or **Down** in the **Status** field), **Down**, **Warning**, **Unusual**, **Up**, **Paused/Resumed** (shows entries with either **Paused** or **Resumed** in the **Status** field), or **Acknowledged Alarms**.
System Events ›	Open a list with log information regarding certain system event types only. Hover over **System Events** to show other menu items. Select between the following event types: **Probe Related**, **Cluster Related**, **Auto-Discovery**, **Notifications**, or **Status Messages**.
Object History	Open a list with log information about changes to the PRTG setup and deletions of subordinate system objects. The object history page has a tab-like interface. Using the tabs you can navigate through various sub-pages in order to view the changes to all related settings and deletions of objects. Select between the following tabs: **My Account**, **System Setup**, **Notifications**, **Schedules**, **User Accounts**, **User Groups**, **Reports**, **Libraries**, or **Maps**. You can open a specific tab directly with the context-button **History** in the page header bar 155 on the corresponding pages.

Tickets

Click to show all tickets that are assigned to the current user. In the table list 207 that appears, you can re-sort the items by clicking the column's header items, and you can filter the list with the inline filter directly above the table. Hover over **Tickets** to show other menu items.

Tickets show important system information or action steps to take for the administrator. For best experience with PRTG, check every ticket and conduct appropriate actions. For more information, please see section **Tickets** 200.



PRTG Main Menu: Tickets

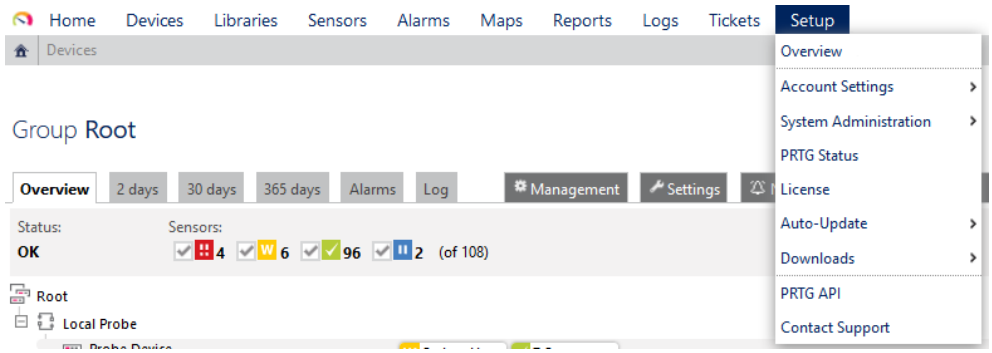
You have several options to display a list of tickets, which is filtered to your needs. You can also create a new ticket via the main menu.

TICKETS

All	Open a list of all open tickets that are assigned to the current user.
My Tickets	Open a list of all open tickets that are assigned to the current user. Hover over **My Tickets** to show other menu items for filtering these tickets depending on their status.
All Tickets	Open a list of all open tickets of all PRTG users. Hover over **All Tickets** to show other menu items for filtering these tickets depending on their status.
ToDo Tickets	Open a list of open tickets from the type **ToDo**. Hover over **ToDo Tickets** to show other menu items for filtering these tickets depending on their status.
Open Ticket	Open the **New Ticket** dialog. Provide the needed information and confirm by clicking **Save** to create a **User Ticket**. For more information about available options, please refer to section Tickets 200.

Setup

Click to show the setup page. Hover over **Setup** to show other menu items. For more information, please see **Setup** 2907 section.



PRTG Main Menu: Setup

SETUP

Overview	Open the setup page 2907.

SETUP

Account Settings ›	Open the **My Account** 2909 settings. Hover over **Account Settings** to show and open the tabs of account settings directly. Choose from: ▪ My Account 2909 ▪ Notifications 2916 ▪ Notification Contacts 2934 ▪ Schedules 2938
System Administration ›	Open the **System Administration** 2943 settings. Hover over **System Administration** to show and open the tabs of the system administration settings directly. Choose from: ▪ Manage Subscriptions 69 (PRTG on demand only) ▪ User Interface 2943 ▪ Monitoring 2955 ▪ Notification Delivery 2961 ▪ Core & Probes 2967 ▪ Cluster 2992 (PRTG on premises only) ▪ User Accounts 2975 ▪ User Groups 2982 ▪ Administrative Tools 2987
PRTG Status	Open the **PRTG Status—System Status** 2994 page. When running a cluster, hover over **PRTG Status** to show other menu items. Choose from: ▪ System Status 2994 ▪ Cluster Status 3010
License	Open the **license activation status** 3012 page. This option is not available in PRTG on demand.
Auto-Update	Open information about the **Software Auto-Update** 3005 status of your PRTG installation. On this page, you can also download and install available updates. Hover over **Auto-Update** to show other menu items. Choose from: ▪ **Status** 3005 to view the update status and to manually check for the latest update.

SETUP

- **Settings** 3007 to define your update settings.

This option is not available in PRTG on demand.

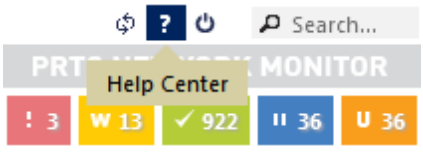
Downloads ›	Open the downloads page 3018 of PRTG for additional downloads. Choose from: ▪ Client App for Windows (Enterprise Console) 3018 (PRTG on premises only) ▪ Client Apps for Mobile Devices 3018 ▪ Remote Probe Installer 3018 ▪ PRTG Tools 3019 ▪ Desktop Notifications 3020
PRTG API	Open the documentation of the **Application Programming Interface (API) Definition** 3174 for your installation.
Contact Support	Open the **Contact Paessler Support / Send Your Feedback to Paessler** 3022 form.

Refresh (Arrows Symbol)

PRTG Main Menu: Refresh Button

Click this symbol to refresh all elements on the current page to display current data. Unlike the reload function of your browser, this only refreshes the single page elements, not the whole page.

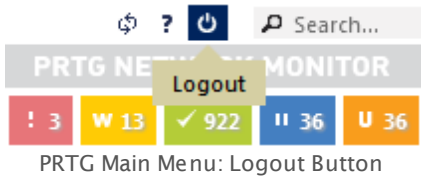
Help Center (? Symbol)



PRTG Main Menu: Help Button

Open the **Help and Support Center** to get help if you have any questions regarding your PRTG setup.

Logout (Off Symbol)



PRTG Main Menu: Logout Button

Log out the current user and return to the login screen 138.

Search Box

Use the search box to find objects in your monitoring setup. Click into the field to enlarge it, enter your search term, and start the search with the enter key. PRTG will perform a string search in your entire monitoring setup, including groups, devices, sensors, libraries, maps, reports, tickets, and object comments, as well as in the PRTG user manual. You will see all search results on a new page.

You can only search for names that are actually displayed. For example, to search for a specific user, use their display name. The login name or email address of a user account will not be used.

Context Menu

Additionally, there are **Context Menus** 215 available for all objects. Right-click an object to open it.

Part 7

Ajax Web Interface—Device and Sensor Setup

7 Ajax Web Interface—Device and Sensor Setup

The Ajax-based web interface is your access to PRTG. Use it to configure devices and sensors, to set up notifications, as well as to review monitoring results, and to create reports. This web interface is highly interactive and uses Asynchronous Java Script and XML (AJAX) to deliver a powerful and easy-to-use user experience. While you are logged in 138, the PRTG web interface continuously refreshes the data on the screen (via Ajax calls) so it always shows the current monitoring results (you can set 2975 refresh interval and method individually).

Because the web interface works as a Single Page Application (SPA), you rarely see a full page refresh to avoid a performance impact due to redundant processing. Only single page elements are refreshed when necessary. The AJAX web interface shows all object setting dialogs as pop-up layers, so you never lose the current context. This speeds up the user experience appreciably and makes the configuration of objects in PRTG comprehensible. The responsive design of the web interface ensures that it always adjusts to the size of your screen so that you see more information at a glance.

The following sections introduce device and sensor setup in the Ajax Graphical User Interface (GUI).

Ajax Web Interface—Device and Sensor Setup—Topics

- Auto-Discovery 249
- Create Objects Manually 267
- Manage Device Tree 292
- Root Group Settings 294
- Probe Settings 312
- Group Settings 334
- Device Settings 360
- Sensor Settings 384—List of Available Sensor Types 385
- Additional Sensor Types (Custom Sensors) 2778
- Sensor Channels Settings 2782
- Sensor Notifications Settings 2791

Other Ajax Web Interface Sections

- Ajax Web Interface—Basic Procedures 136
- Ajax Web Interface—Advanced Procedures 2804

Related Topics

- Enterprise Console 3026
- PRTG Apps for Mobile Network Monitoring 3082

7.1 Auto-Discovery

The PRTG auto-discovery is a great way to automatically create a sophisticated and concise set of sensors for your complete network. It is mainly suitable for LAN discovery because it involves a lot of SNMP and WMI.

PRTG already runs a quick initial auto-discovery as soon as you finish the installation of PRTG to automatically show you several available devices in your network.

You cannot use this feature with local probes in PRTG on demand. You can use this feature on remote probes 3196.

How Auto-Discovery Works

The PRTG auto-discovery process has three stages:

- **Step 1**
  Scanning a network segment for devices using Ping (for groups only).
- **Step 2**
  Assessing the device type for all devices discovered in Step 1 (using SNMP, WMI, and other protocols).
- **Step 3a**
  Creating sensor sets that match the discovered device types of step 2. This is done based on built-in device templates with recommended sensors for many device types.

  Step 3b (optional)
  Creating sensor sets using device templates that PRTG users created (see **Create Device Template** 2818 section).

You can use the auto-discovery on group level for a range of IP addresses, or for individual devices that you have created manually. You can run the auto-discovery just once, on demand via the context menu, or scheduled every hour, day, or week. Running the auto-discovery daily or weekly on group level automatically creates new devices when they are connected to the network and adds according sensors. As soon as PRTG discovers new devices or sensors, it will create notifying **Tickets** 200 (which are mailed to the PRTG system administrator user by default).

Please be aware of the following restrictions of the auto-discovery:

- PRTG cannot discover devices that cannot be pinged, because Step 1 uses pings. If, for example, a firewall blocks echo requests, PRTG cannot discover a device behind it.
- Please define authentication settings for **Windows Systems**, **Linux (SSH/WBEM) Systems**, **VMware/XEN Servers**, **SNMP Devices**, **Database Management Systems**, and **Amazon CloudWatch** to fully benefit from the power of this feature. We recommend that you define these settings in the Root group 294.
- If a device has more than one IP address, it may show up more than once in the discovery results, even though PRTG tries to identify these situations.

- If a device already exists on the same probe, the auto-discovery will skip this device and not create a duplicate. If a device with the same IP address as a found device already exists on another probe, it will be added to the probe where the auto-discovery runs nevertheless. This is because new remote probes might run in another network.
- Auto-discovery on group level will not create new sensors on devices that already exist in PRTG but only on newly discovered devices. If you want to automatically add sensors to an existing device, please run the auto-discovery on this device.
- Using frequent auto-discoveries of large network segments can lead to performance issues. Because of this we recommend that you only schedule regular auto-discoveries where necessary. For detailed information, see this Knowledge Base article: Why can automatic auto-discoveries evoke performance issues?
- PRTG automatically adds suitable device icons to discovered devices. PRTG uses a device's MAC address for this purpose, which it determines via ARP (Address Resolution Protocol). This only works via IPv4 and not with IPv6. Usually, ARP works only in the local network unless your router supports ARP and you configure it accordingly.
- If you use Multi-Edit 281 to automatically create sensors using specific device template(s), the Auto-Discovery is not automatically started. To manually start the Auto-Discovery, right-click the individual devices and select **Auto-Discovery** | **Run Auto-Discovery**.

HTTP sensors indicate the access type to the target device with their names (HTTP, HTTP (8080), and HTTPS). This approach helps to distinguish HTTP sensors if the auto-discovery adds more than one instance to a device.

Run Auto-Discovery Now

You can run an auto-discovery at any time for a group or a device. To do so, right-click the object to analyze and select **Run Auto-Discovery** from the context menu 215. PRTG immediately starts searching for new objects that can be added to the device tree. If you use it for an auto-discovery group, PRTG will add devices with according sensors, if found. If you use it for a device, PRTG will add new sensors, if found. You can always see in the corresponding page header bar 155 when PRTG ran the last auto-discovery on a selected group or device.

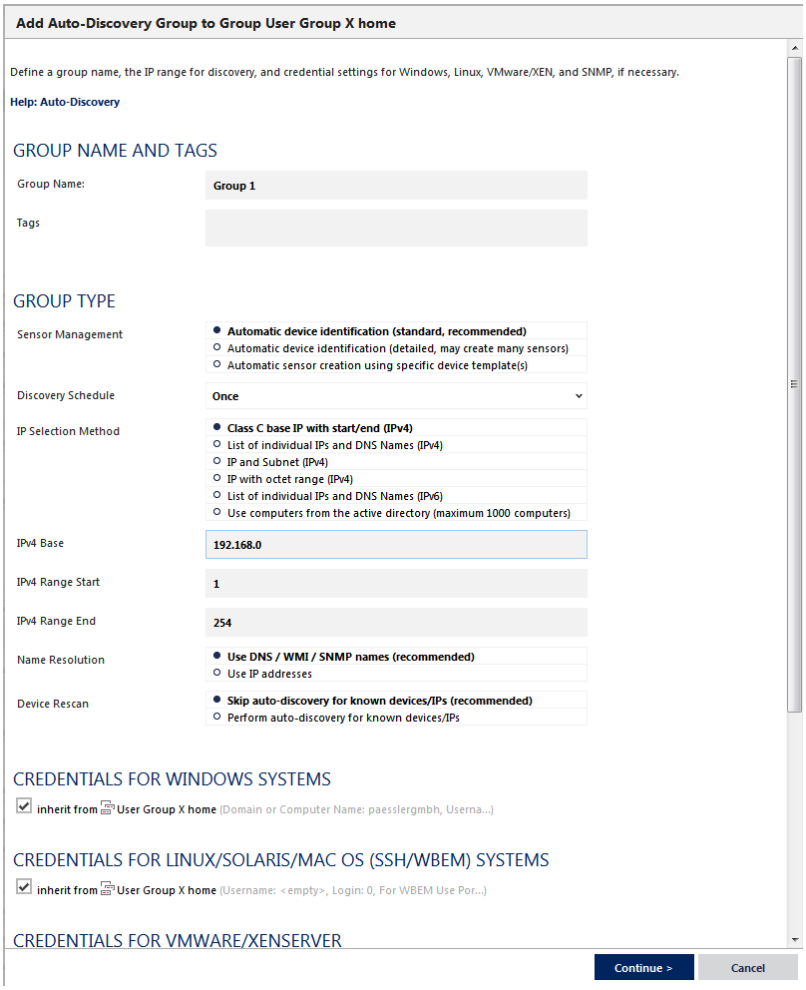
The auto-discovery will also re-add devices or sensors you have manually deleted. If you do not want this, please create objects manually 267 only.

Creating an Auto-Discovery Group

There are several ways to start auto-discovery:

- Select **Devices** | **Add Auto-Discovery Group** from the main menu bar 231. To start an automatic detection of devices and sensors in your network an assistant will appear, leading you through two steps.
- For faster setup, you can select **Add Auto-Discovery Group...** in the context menu 215 of a probe or group to which you want to add the new group. This will skip step 1 and lead you directly to step 2.

This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.



Add Auto-Discovery Group Dialog

- **Step 1**
  Please choose a probe or group you want to add the new group to. Click **Continue**.
- **Step 2**
  Add auto-discovery settings as described below.

Add Auto-Discovery Group Settings

GROUP NAME AND TAGS

Group Name	Enter a meaningful name to identify the group. The name will be shown by default in the devices tree and in all alarms.
Tags	Enter one or more tags. Confirm each tag by hitting the space, comma, or enter key. You can use tags to group objects and use tag-filtered views later on. Tags are not case sensitive. Tags are automatically inherited 124.

GROUP TYPE

Sensor Management	Select the method for automatic network discovery. Choose between: ▪ **Automatic device identification (standard, recommended)**: Detect mainly based on Ping, SNMP, and WMI. This option works fine for most installations. ▪ **Automatic device identification (detailed, may create many sensors)**: Detect in a more detailed way and create more sensors. This option uses all standard device templates for auto-discovery. It is suitable for small network segments and whenever you want to monitor the maximum number of sensors available. ▪ **Automatic sensor creation using specific device template (s)**: Manually define the device templates used for auto-discovery. From the list below, select one or more templates.

Device Template(s)	This option is only visible if you enable using specific device templates above. Choose one or more templates by adding a check mark in front of the respective template name. You can also select and deselect all items by using the check box in the table head. PRTG will use the selected templates for auto-discovery on the current device. Choose from: ▪ **ADSL** ▪ **Amazon Cloudwatch** ▪ **Buffalo TeraStation NAS** ▪ **Cisco ASA VPN** ▪ **Cisco Device (Generic)** ▪ **Dell EqualLogic** ▪ **Dell MDI Disk** ▪ **DNS Server** ▪ **Environment Jacarta** ▪ **Environment Poseidon** ▪ **FTP Server** ▪ **Generic Device (PING only)** ▪ **Generic Device (SNMP-enabled)** ▪ **Generic Device (SNMP-enabled, Detailed)** ▪ **HTTP Web Server**

- Hyper V Host Server
- IPMI enabled devices
- Juniper NS Device
- Linux/UNIX Device (SNMP or SSH enabled)
- Mail Server (Generic)
- Mail Server (MS Exchange)
- Microsoft Sharepoint 2010
- NAS LenovoEMC
- NAS QNAP
- NAS Synology
- NetApp
- NTP Server
- Printer (HP)
- Printer Generic
- RDP Server
- RMON compatible device
- Server (Compaq/HP agents)
- Server (Dell)
- Sever Cisco UCS
- Server IBM
- SonicWALL
- SSL Security Check
- Switch (Cisco Catalyst)
- Switch (Cisco IOS Based)
- Switch (HP Procurve)
- UNIX/Linux Device
- UPS Health (APC)
- UPS Health (Generic)
- UPS Health (Leibert)
- VMware ESX / vCenter Server
- Webserver
- Windows (Detailed via WMI)
- Windows (via Remote Powershell)

	▪ **Windows (via WMI)** ▪ **Windows IIS (via SNMP)** ▪ **XEN Hosts** ▪ **XEN Virtual Machines** Once the auto-discovery is finished, PRTG will create a new ticket [200] and list the device templates that it used to create new sensors. The ticket will not show templates that were not applied.
Discovery Schedule	Define when PRTG will run the auto-discovery. Choose between: ▪ **Once**: Perform auto-discovery only once. PRTG will add new devices and sensors once. If you select this option, you have to start the auto-discovery manually [250], it will not run automatically. ▪ **Hourly**: Perform auto-discovery for new devices and sensors every 60 minutes. Please use this option with caution! Frequently executed auto-discoveries might cause performance issues, especially when large network segments are scanned every hour. ▪ **Daily**: Perform auto-discovery for new devices and sensors every 24 hours. The first auto-discovery will run immediately, all other discoveries will start at the time defined in the **Auto-Discovery Settings** section of the System Administration—Monitoring [2959] settings. ▪ **Weekly**: Perform auto-discovery for new devices and sensors every 7 days. The first auto-discovery will run immediately, all other discoveries will start at the time defined in the **Auto-Discovery Settings** section of the System Administration—Monitoring [2959] settings.
IP Selection Method	Define how you want to define the IP range for auto-discovery. Choose between: ▪ **Class C base IP with start/end (IPv4)**: Define an IPv4 class C address range. ▪ **List of individual IPs and DNS names (IPv4)**: Enter a list of individual IPv4 addresses or DNS names. ▪ **IP and subnet (IPv4)**: Enter an IPv4 address and subnet mask. ▪ **IP with octet range (IPv4)**: Enter an IPv4 address range for every IP octet individually. With this, you can define very customizable IP ranges. ▪ **List of individual IPs and DNS names (IPv6)**: Enter a list of individual IPv6 addresses or DNS names.

	▪ **Use computers from the active directory (maximum 1000 computers)**: Search in the active directory for computers to perform auto-discovery. ⓘ Define your active directory domain in advance in the system administration. See **System Administration—Core & Probes** 2971. ⓘ Only subnets with up to 65,536 IP addresses can be discovered! If you define a range with a higher number of addresses, discovery will stop before it is completed.
IPv4 Base	This field is only visible if you select Class C network detection above. Enter a class C network as IP base for the auto-discovery. Enter the first three octets of an IPv4 IP address, for example, **192.168.0**
IPv4 Range Start	This field is only visible if you select Class C network detection above. Enter the IP octet of the class C network specified above from which PRTG will start the auto-discovery. This will complete the IP base above to an IPv4 address. For example, enter **1** to discover from **192.168.0.1**.
IPv4 Range End	This field is only visible if you select Class C network detection above. Enter the IP octet of the class C network specified above at which PRTG will stop the auto-discovery. This will complete the IP base above to an IPv4 address. For example, enter **254** to discover up to **192.168.0.254**.
IPv4/DNS Name List IPv6/DNS Name List	This field is only visible if you select the IP list option above. Enter a list of IP addresses or DNS names which the auto-discovery will scan. Enter each address in a separate line.
IPv4 and Subnet (IPv4)	This field is only visible if you select the IP and subnet option above. Enter an expression in the format **address/subnet**, for example, 192.168.3.0/255.255.255.0. You can also use the short form like 192.168.3.0/24 in this example. PRTG will scan the complete host range (without network and broadcast address) defined by the IP address and the subnet mask.
IP with Octet Range	This field is only visible if you select the octet range option above. Enter an expression in the format **a1.a2.a3.a4**, where a1, a2, a3, and a4 are each a number between 0-255, or a range with two numbers and a hyphen like 1-127. All permutations of all ranges are calculated. For example, 10.0.1-10.1-100 results in 1,000 addresses that PRTG will scan during auto-discovery.

Organizational Unit	This field is only visible if you select active directory above. Enter an organizational unit (OU) to restrict the active directory search to computers that are part of this OU. Just enter the name of the OU without any other term (so without "OU" in front). If you leave this field empty, there will not be any restriction. Make sure that the OU contains a host. If the OU is empty, you will receive an error message. If you have sub-OUs, consider the correct syntax in the format **Y,OU=X**: OUs that are part of another OU have to be listed together with their parent(s). Enter the sub-OU followed by ,OU= and the name of the parent OU. Examples: ▪ Assuming that the organizational unit 'Y' is part of the OU named 'X'. Then the syntax would be Y,OU=X ▪ For three OUs 'X', 'Y' part of 'X', and 'Z' part of 'Y', the syntax would be Z,OU=Y,OU=X The order is important, sub-OUs have to be listed left of their particular parents!
Name Resolution	Define how to monitor newly discovered devices. This affects only new devices. The setting for existing devices will remain unchanged. Depending on your selection the **IP Address/DNS Name** field of an added device shows the DNS name or IP address which PRTG uses to access the target device. Choose between: ▪ **Use DNS names (recommended)**: Monitor newly discovered devices via their DNS names (if available). ▪ **Use IP addresses**: Monitor newly discovered devices via their IP address. We recommend that you use the default value. This setting does not affect how PRTG shows the devices in the device tree.
Device Rescan	Define if you want to add devices that already exist in your PRTG installation also to the currently selected group. Choose between: ▪ **Skip auto-discovery for known devices/IPs (recommended)**: Do not re-scan known devices or IP addresses, only add devices with new IPs or DNS names when auto-discovering. PRTG will not add devices that are already included elsewhere in your configuration, for example, in other groups.

- **Perform auto-discovery for known devices/IPs**: Re-scan devices with known IP addresses with every auto-discovery. This option will add devices that already exist in other groups also to this group and runs the auto-discovery on the newly added devices.
  The auto-discovery will not run on devices that already exist in this group. If you want to run the auto-discovery for an existing device, you have to start the auto-discovery on this device.

We recommend that you use the default value.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

If you have not set credentials yet, set them now before starting the auto-discovery to fully exploit the power of this feature!

CREDENTIALS FOR WINDOWS SYSTEMS

Domain or Computer Name	Define the authority for Windows access. This is used for Windows Management Instrumentation (WMI) and other Windows sensors. If you want to use a Windows local user account on the target device, enter the computer name here. If you want to use a Windows domain user account (recommended), enter the (Active Directory) domain name here. If not explicitly defined, PRTG will automatically add a prefix in order to use the NT LAN Manager (NTLM) protocol. Do not leave this field empty.
User	Enter the username for Windows access. Usually, you will use credentials with administrator privileges.
Password	Enter the password for Windows access. Usually, you will use credentials with administrator privileges.

CREDENTIALS FOR LINUX/SOLARIS/MAC OS (SSH/WBEM) SYSTEMS

User	Enter a login name for the access via SSH and WBEM. Usually, you will use credentials with administrator privileges.

CREDENTIALS FOR LINUX/SOLARIS/MAC OS (SSH/WBEM) SYSTEMS

Login	Define the authentication method to use for login. Choose between: ▪ **Login via Password**: Provide a password for login. Enter below. ▪ **Login via Private Key**: Provide a private key for authentication. PRTG can only handle keys in OpenSSH format that are not encrypted. You cannot use password protected keys here. In the text field, paste the entire private key, including the "BEGIN" and "END" lines. Please make sure the according public key is provided on the target machine. For details, please see **Monitoring via SSH** 3095.
Password	This field is only visible if you select password login above. Enter a password for the Linux access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
Private Key	This field is only visible if you select private key login above. Paste a private key into the field (OpenSSH format, unencrypted). Usually, you will use credentials with administrator privileges. If you do not insert a private key for the first time, but change the private key, you need to restart your PRTG core server service 2988 in order for the private key change to take effect! For details, please see **Monitoring via SSH** 3095.
For WBEM Use Protocol	Define the protocol to use for WBEM. This setting is only relevant if you use WBEM sensors. Choose between: ▪ **HTTP**: Use an unencrypted connection for WBEM. ▪ **HTTPS**: Use an SSL-encrypted connection for WBEM.
For WBEM Use Port	Define the port to use for WBEM. This setting is only relevant if you use WBEM sensors. Choose between: ▪ **Set automatically (port 5988 or 5989)**: Use one of the standard ports, depending on whether you choose unencrypted or encrypted connection above. ▪ **Set manually**: Use a custom port. Define below.
WBEM Port	This setting is only visible if you enable manual port selection above. Enter the WBEM port number.
SSH Port	Enter the port number to use for SSH connections. By default, PRTG uses this setting automatically for all SSH sensors 390, unless you define a different port number in the sensor settings.

CREDENTIALS FOR LINUX/SOLARIS/MAC OS (SSH/WBEM) SYSTEMS

SSH Rights Elevation	Define the rights that you want to use to execute the command on the target system. Choose between: ▪ **Run the command as the user connecting (default)**: Use the rights of the user who establishes the SSH connection, as defined above. ▪ **Run the command as another user using 'sudo' (with password)**: Use the rights of another user with a password required for sudo to run commands on the target device, for example, as root user. ▪ **Run the command as another user using 'sudo' (without password)**: Use the rights of another user without a password required for sudo to run commands on the target device, for example, as root user. ▪ **Run the command as another user using 'su'**: Use the rights of another user with su to run commands on the target device.
Target User	This field is only visible if you choose sudo or su above. Enter a username to run the specified command as a user other than root. If you leave this field empty, you will run the command as root. Ensure you set the Linux password even if you use a public or private key for authentication. This is not necessary if the user is allowed to execute the command without a password.
Password Target User	This field is only visible if you choose to run the commands using su or sudo with password above. Enter the password for the specified target user.
SSH Engine	Select the method you want to use to access data with SSH sensors 3095. We strongly recommend that you keep the default engine! For now, you still can use the legacy mode to ensure compatibility with your target systems. Choose between: ▪ **Default (recommended)**: This is the default monitoring method for SSH sensors. It provides best performance and security. ▪ **Compatibility Mode (deprecated)**: Try this legacy method only if the default mode does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions and is deprecated. We will remove this legacy option soon, so please try to get your SSH sensors running with the default SSH engine. ⓘ You can also individually select the SSH engine for each SSH sensor in the sensor settings.

CREDENTIALS FOR VMWARE/XENSERVER

User	Enter a login name for access to VMware and Xen servers. Usually, you will use credentials with administrator privileges.
Password	Enter a password for access to VMware and Xen servers. Usually, you will use credentials with administrator privileges. Single Sign-On (SSO) passwords for vSphere do not support special characters. Please see the manual sections for VMware sensors for details.
VMware Protocol	Define the protocol used for the connection to VMware and XenServer. Choose between: ▪ **HTTPS (recommended)**: Use an SSL-encrypted connection to VMware and XenServers. ▪ **HTTP**: Use an unencrypted connection to VMware and XenServers.
Session Pool	Define if you want to use session pooling for VMware sensors. Choose between: ▪ **Reuse session for for multiple scans (recommended)**: Select this option to use session pooling. With session pooling, a VMware sensor uses the same session as created in advance to query data and needs not to log in and out for each sensor scan. We recommend that you choose this option because it reduces network load and log entries on the target device, resulting in better performance. ▪ **Create a new session for each scan**: If you select this option and disable session pooling, a VMware sensor has to log in and out for each sensor scan. We recommend that you use the session pooling option above for better performance.

CREDENTIALS FOR DATABASE MANAGEMENT SYSTEMS

The settings you define in this section apply to the following sensor types:

- ADO SQL v2 Sensor 418
- Microsoft SQL v2 Sensor 1135
- MySQL v2 Sensor 1151
- Oracle SQL v2 Sensor 1253

CREDENTIALS FOR DATABASE MANAGEMENT SYSTEMS

- PostgreSQL Sensor 1363

Port for Databases	Define which ports PRTG will use for connections to the monitored databases. Choose between: ▪ **Set automatically (default port, recommended)**: PRTG automatically determines the type of the monitored database and uses the corresponding default port to connect. See below for a list of default ports. ▪ **Define one custom port valid for all database sensors**: Choose this option if your database management systems do not use the default ports. Define the port for database connections manually below. If you choose this option, PRTG will use the custom port for all database sensors. If you choose the automatic port selection, PRTG uses the following default ports: ▪ Microsoft SQL: 1433 ▪ MySQL: 3306 ▪ Oracle SQL: 1521 ▪ PostgreSQL: 5432
Custom Database Port	Enter the number of the port that PRTG will use for database connections. Please enter an integer value. All database sensors on this device will use this port to connect.
Authentication Mode	Select the authentication method for the connection to the SQL database. Choose between: ▪ **Windows authentication with impersonation**: If you select this option, PRTG uses the Windows credentials as defined in the particular device settings 365 for the database connection. The user whose credentials are used needs to have permissions to log on to the system on which the PRTG probe with a database sensor runs. This is required for the impersonation. ▪ **SQL server authentication**: Choose this option if you want to use explicit credentials for database connections.
User	This field is only visible if you select SQL server authentication above. Enter the username for the database connection.

CREDENTIALS FOR DATABASE MANAGEMENT SYSTEMS

Password	This field is only visible if you select SQL server authentication above. Enter the password for the database connection.
Timeout (Sec.)	Enter a timeout in seconds for the request. Please enter an integer value. If the reply takes longer than this value defines, the sensor cancels the request and triggers an error message. The maximum timeout value is 300 seconds (5 minutes).

CREDENTIALS FOR AMAZON CLOUDWATCH

Access Key	Enter your Amazon Web Services (AWS) access key. Please see the corresponding Amazon CloudWatch sensor 391 documentation to learn more about the rights that are required for querying AWS CloudWatch metrics.
Secret Key	Enter your Amazon Web Services (AWS) secret key. Please see the corresponding Amazon CloudWatch sensor 391 documentation to learn more about the rights that are required for querying AWS CloudWatch metrics.

CREDENTIALS FOR SNMP DEVICES

SNMP Version

Select the SNMP version for the device connection. Choose between:

- **v1**: Use the simple v1 protocol for SNMP connections. This protocol only offers clear-text data transmission, but it is usually supported by all devices.
  SNMP v1 does not support 64-bit counters which may result in invalid data when monitoring traffic via SNMP.
- **v2c (recommended)**: Use the more advanced v2c protocol for SNMP connections. This is the most common SNMP version. Data is still transferred as clear-text, but it supports 64-bit counters.
- **v3**: Use the v3 protocol for SNMP connections. It provides secure authentication and data encryption.

CREDENTIALS FOR SNMP DEVICES

When using SNMP v3 you can only monitor a limited number of sensors per second due to internal limitations. The limit is somewhere between 1 and 50 sensors per second (depending on the SNMP latency of your network). This means that using an interval of 60 seconds limits you to between 60 and 3000 SNMP v3 sensors for each probe. If you experience an increased Interval Delay or Open Requests with the **Probe Health Sensor** 1378, distribute the load over multiple probes 3196. SNMP v1 and v2 do not have this limitation.

Community String

This setting is only visible if you select SNMP version **v1** or **v2c** above. Enter the community string of your devices. This is a kind of "clear-text password" for simple authentication. We recommend that you use the default value.

Authentication Type

This setting is only visible if you select SNMP version **v3** above. Choose between:

- **MD5**: Use Message-Digest Algorithm 5 (MD5) for authentication.
- **SHA**: Use Secure Hash Algorithm (SHA) for authentication.

The type you choose must match the authentication type of your device.

If you do not want to use authentication, but you need SNMP v3, for example, because your device requires context, you can leave the field **Password** empty. In this case, SNMP_SEC_LEVEL_NOAUTH is used and authentication deactivated entirely.

User

This setting is only visible if you select SNMP version **v3** above. Enter a username for secure authentication. This value must match the username of your device.

Password

This setting is only visible if you select SNMP version **v3** above. Enter a password for secure authentication. This value must match the password of your device.

Encryption Type

This setting is only visible if you select SNMP version **v3** above. Select an encryption type. Choose between:

- **DES**: Use Data Encryption Standard (DES) as encryption algorithm.
- **AES**: Use Advanced Encryption Standard (AES) as encryption algorithm.

AES 192 and AES 256 are not supported by Net-SNMP because they lack RFC specification.

CREDENTIALS FOR SNMP DEVICES

	The type that you choose must match the encryption type of your device.
Data Encryption Key	This setting is only visible if you select SNMP version **v3** above. Enter an encryption key here. If you provide a key in this field, SNMP data packets are encrypted using the encryption algorithm selected above, which provides increased security. The key that you enter here must match the encryption key of your device. If the key you enter in this field does not match the key configured on the target SNMP device, you will not get an error message about this! Please enter a string or leave the field empty.
Context Name	This setting is only visible if you select SNMP version **v3** above. Enter a context name only if it is required by the configuration of the device. Context is a collection of management information accessible by an SNMP device. Please enter a string.
SNMP Port	Enter the port for the SNMP communication. We recommend that you use the default value.
SNMP Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than the value you enter here, the request is aborted and an error message triggered.

PROXY SETTINGS FOR HTTP SENSORS

HTTP Proxy Settings	The proxy settings determine how a sensor connects to a given URL. You can enter data for an HTTP proxy server that sensors will use when connecting via HTTP or HTTPS. This setting affects monitoring only and determines the behavior of HTTP sensors. To change proxy settings for the core server, please see **System Administration—Core & Probes** 2967. The **SSL Certificate Sensor** 2289 and the **SSL Security Check Sensor** 2299 do not support HTTP proxies, but you can configure connections via SOCKS proxies in their sensor settings.
Name	Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.

PROXY SETTINGS FOR HTTP SENSORS

Port	Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.
User	If the proxy requires authentication, enter the username for the proxy login. Only basic authentication is available! Please enter a string or leave the field empty.
Password	If the proxy requires authentication, enter the password for the proxy login. Only basic authentication is available! Please enter a string or leave the field empty.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object that you are editing. A table with user groups and rights is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object does not show up in lists. ▪ **Read**: Users in this group can see the object and review its settings. ▪ **Write**: Users in this group can see the object, as well as review and edit its settings. However, they cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, as well as review and edit its settings as well as edit access rights. You can create new user groups in the **System Administration—User Groups** 2982 settings.

Click the **Continue** button to save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Auto-Discovery in Progress

While auto-discovery is running you may experience a lower system performance as usual, because PRTG works in the background to discover your network. Depending on the IP ranges defined (up to 65,536 addresses), the discovery may run up to several days before it is complete. You can review the status of the discovery process as follows:

- In the device tree, behind the group or device name, you will see a percentage value showing the progress of auto-discovery.
- During auto-discovery, the web interface will display a box in the lower-right corner that shows the number of active auto-discovery tasks.
- To stop a running auto-discovery, right-click the group or device, and select **Pause | For 5 minutes...** from the context menu 215. PRTG will pause 214 monitoring for 5 minutes and stop auto-discovery tasks.

Related Topics

- **Create Device Template** 2818

More

Knowledge Base: Why can automatic auto-discoveries evoke performance issues?

- https://kb.paessler.com/en/topic/14423

7.2 Create Objects Manually

We recommend that you use the auto-discovery 249 function to create a basic monitoring setup for your network. Afterwards, you can manually create devices that could not be discovered, or arrange 2811 detected devices in groups.

The procedure depends on the kind of object you want to add. Choose between:

- **Add a Group** 268
- **Add a Device** 275
- **Add a Sensor** 288

Add a Remote Probe

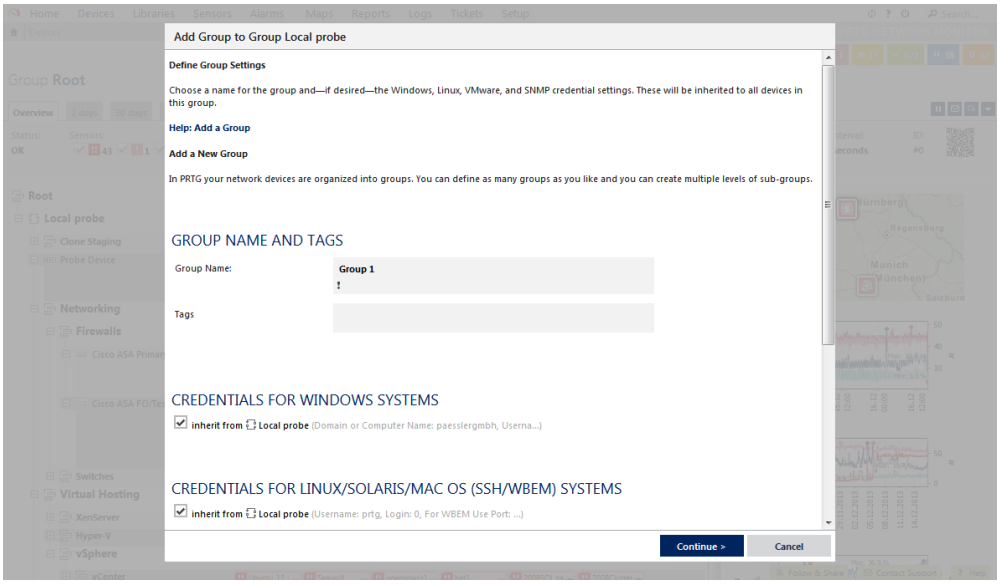
Please see section **Multiple Probes and Remote Probes** 3195 for more information.

7.2.1 Add a Group

This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

In order to add a group manually, select **Devices | Add Group** from the main menu. An assistant will appear, leading you through two steps. For faster setup, you can select **Add Group...** in the context menu 215 of a probe or group to which you want to add the new group. This will skip step 1 and lead you directly to step 2.

- **Step 1**
  Please choose a probe or group you want to add the new group to. Click on **Continue**.



Add Group Assistant Step 2

- **Step 2**
  Add group settings as described below.

Add Group Settings

GROUP NAME AND TAGS

Group Name	Enter a meaningful name to identify the group. The name will be shown by default in the devices tree and in all alarms.
Tags	Enter one or more tags. Confirm each tag by hitting the space, comma, or enter key. You can use tags to group objects and use tag-filtered views later on. Tags are not case sensitive. Tags are automatically inherited 124.

CREDENTIALS FOR WINDOWS SYSTEMS

Domain or Computer Name	Define the authority for Windows access. This is used for Windows Management Instrumentation (WMI) and other Windows sensors. If you want to use a Windows local user account on the target device, enter the computer name here. If you want to use a Windows domain user account (recommended), enter the (Active Directory) domain name here. If not explicitly defined, PRTG will automatically add a prefix in order to use the NT LAN Manager (NTLM) protocol. Do not leave this field empty.
User	Enter the username for Windows access. Usually, you will use credentials with administrator privileges.
Password	Enter the password for Windows access. Usually, you will use credentials with administrator privileges.

CREDENTIALS FOR LINUX/SOLARIS/MAC OS (SSH/WBEM) SYSTEMS

User	Enter a login name for the access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
Login	Define the authentication method to use for login. Choose between: ▪ **Login via Password**: Provide a password for login. Enter below. ▪ **Login via Private Key**: Provide a private key for authentication. PRTG can only handle keys in OpenSSH format that are not encrypted. You cannot use password protected keys here. In the text field, paste the entire private key, including the "BEGIN" and "END" lines. Please make sure the according public key is provided on the target machine. For details, please see **Monitoring via SSH** 3095.
Password	This field is only visible if you select password login above. Enter a password for the Linux access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
Private Key	This field is only visible if you select private key login above. Paste a private key into the field (OpenSSH format, unencrypted). Usually, you will use credentials with administrator privileges. If you do not insert a private key for the first time, but change the private key, you need to restart your PRTG core server service 2988 in order for the private key change to take effect! For details, please see **Monitoring via SSH** 3095.

CREDENTIALS FOR LINUX/SOLARIS/MAC OS (SSH/WBEM) SYSTEMS

For WBEM Use Protocol	Define the protocol to use for WBEM. This setting is only relevant if you use WBEM sensors. Choose between: ▪ **HTTP**: Use an unencrypted connection for WBEM. ▪ **HTTPS**: Use an SSL-encrypted connection for WBEM.
For WBEM Use Port	Define the port to use for WBEM. This setting is only relevant if you use WBEM sensors. Choose between: ▪ **Set automatically (port 5988 or 5989)**: Use one of the standard ports, depending on whether you choose unencrypted or encrypted connection above. ▪ **Set manually**: Use a custom port. Define below.
WBEM Port	This setting is only visible if you enable manual port selection above. Enter the WBEM port number.
SSH Port	Enter the port number to use for SSH connections. By default, PRTG uses this setting automatically for all SSH sensors 390, unless you define a different port number in the sensor settings.
SSH Rights Elevation	Define the rights that you want to use to execute the command on the target system. Choose between: ▪ **Run the command as the user connecting (default)**: Use the rights of the user who establishes the SSH connection, as defined above. ▪ **Run the command as another user using 'sudo' (with password)**: Use the rights of another user with a password required for sudo to run commands on the target device, for example, as root user. ▪ **Run the command as another user using 'sudo' (without password)**: Use the rights of another user without a password required for sudo to run commands on the target device, for example, as root user. ▪ **Run the command as another user using 'su'**: Use the rights of another user with su to run commands on the target device.
Target User	This field is only visible if you choose sudo or su above. Enter a username to run the specified command as a user other than root. If you leave this field empty, you will run the command as root. Ensure you set the Linux password even if you use a public or private key for authentication. This is not necessary if the user is allowed to execute the command without a password.

CREDENTIALS FOR LINUX/SOLARIS/MAC OS (SSH/WBEM) SYSTEMS

Password Target User	This field is only visible if you choose to run the commands using su or sudo with password above. Enter the password for the specified target user.
SSH Engine	Select the method you want to use to access data with SSH sensors 3095. We strongly recommend that you keep the default engine! For now, you still can use the legacy mode to ensure compatibility with your target systems. Choose between: ▪ **Default (recommended)**: This is the default monitoring method for SSH sensors. It provides best performance and security. ▪ **Compatibility Mode (deprecated)**: Try this legacy method only if the default mode does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions and is deprecated. We will remove this legacy option soon, so please try to get your SSH sensors running with the default SSH engine. ⓘ You can also individually select the SSH engine for each SSH sensor in the sensor settings.

CREDENTIALS FOR VMWARE/XENSERVER

User	Enter a login name for access to VMware and Xen servers. Usually, you will use credentials with administrator privileges.
Password	Enter a password for access to VMware and Xen servers. Usually, you will use credentials with administrator privileges. ⓘ Single Sign-On (SSO) passwords for vSphere do not support special characters. Please see the manual sections for VMware sensors for details.
VMware Protocol	Define the protocol used for the connection to VMware and XenServer. Choose between: ▪ **HTTPS (recommended)**: Use an SSL-encrypted connection to VMware and XenServers. ▪ **HTTP**: Use an unencrypted connection to VMware and XenServers.
Session Pool	Define if you want to use session pooling for VMware sensors. Choose between:

CREDENTIALS FOR VMWARE/XENSERVER

- **Reuse session for for multiple scans (recommended)**: Select this option to use session pooling. With session pooling, a VMware sensor uses the same session as created in advance to query data and needs not to log in and out for each sensor scan. We recommend that you choose this option because it reduces network load and log entries on the target device, resulting in better performance.
- **Create a new session for each scan**: If you select this option and disable session pooling, a VMware sensor has to log in and out for each sensor scan. We recommend that you use the session pooling option above for better performance.

CREDENTIALS FOR SNMP DEVICES

SNMP Version

Select the SNMP version for the device connection. Choose between:

- **v1**: Use the simple v1 protocol for SNMP connections. This protocol only offers clear-text data transmission, but it is usually supported by all devices.
  SNMP v1 does not support 64-bit counters which may result in invalid data when monitoring traffic via SNMP.
- **v2c (recommended)**: Use the more advanced v2c protocol for SNMP connections. This is the most common SNMP version. Data is still transferred as clear-text, but it supports 64-bit counters.
- **v3**: Use the v3 protocol for SNMP connections. It provides secure authentication and data encryption.

When using SNMP v3 you can only monitor a limited number of sensors per second due to internal limitations. The limit is somewhere between 1 and 50 sensors per second (depending on the SNMP latency of your network). This means that using an interval of 60 seconds limits you to between 60 and 3000 SNMP v3 sensors for each probe. If you experience an increased Interval Delay or Open Requests with the **Probe Health Sensor** 1378, distribute the load over multiple probes 3196. SNMP v1 and v2 do not have this limitation.

Community String

This setting is only visible if you select SNMP version **v1** or **v2c** above. Enter the community string of your devices. This is a kind of "clear-text password" for simple authentication. We recommend that you use the default value.

CREDENTIALS FOR SNMP DEVICES

Authentication Type	This setting is only visible if you select SNMP version **v3** above. Choose between: ▪ **MD5**: Use Message-Digest Algorithm 5 (MD5) for authentication. ▪ **SHA**: Use Secure Hash Algorithm (SHA) for authentication. The type you choose must match the authentication type of your device. ⓘ If you do not want to use authentication, but you need SNMP v3, for example, because your device requires context, you can leave the field **Password** empty. In this case, SNMP_SEC_LEVEL_NOAUTH is used and authentication deactivated entirely.
User	This setting is only visible if you select SNMP version **v3** above. Enter a username for secure authentication. This value must match the username of your device.
Password	This setting is only visible if you select SNMP version **v3** above. Enter a password for secure authentication. This value must match the password of your device.
Encryption Type	This setting is only visible if you select SNMP version **v3** above. Select an encryption type. Choose between: ▪ **DES**: Use Data Encryption Standard (DES) as encryption algorithm. ▪ **AES**: Use Advanced Encryption Standard (AES) as encryption algorithm. ⓘ AES 192 and AES 256 are not supported by Net-SNMP because they lack RFC specification. ⓘ The type that you choose must match the encryption type of your device.
Data Encryption Key	This setting is only visible if you select SNMP version **v3** above. Enter an encryption key here. If you provide a key in this field, SNMP data packets are encrypted using the encryption algorithm selected above, which provides increased security. The key that you enter here must match the encryption key of your device. ⓘ If the key you enter in this field does not match the key configured on the target SNMP device, you will not get an error message about this! Please enter a string or leave the field empty.

CREDENTIALS FOR SNMP DEVICES

Context Name	This setting is only visible if you select SNMP version **v3** above. Enter a context name only if it is required by the configuration of the device. Context is a collection of management information accessible by an SNMP device. Please enter a string.
SNMP Port	Enter the port for the SNMP communication. We recommend that you use the default value.
SNMP Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than the value you enter here, the request is aborted and an error message triggered.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object that you are editing. A table with user groups and rights is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object does not show up in lists. ▪ **Read**: Users in this group can see the object and review its settings. ▪ **Write**: Users in this group can see the object, as well as review and edit its settings. However, they cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, as well as review and edit its settings as well as edit access rights. You can create new user groups in the **System Administration—User Groups** 2982 settings.

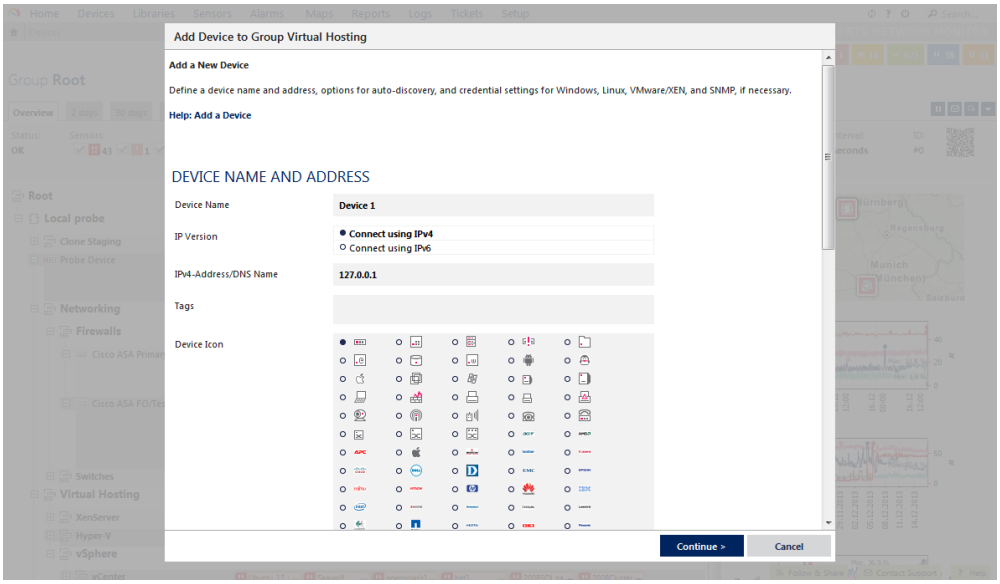
Click the **Continue** button to save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

7.2.2 Add a Device

This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

To manually add a device, select **Devices | Add Device** from the main menu. An assistant will appear, leading you through two steps. For faster setup, you can select **Add Device...** in the context menu[215] of a group to which you want to add the new device. This will skip step 1 and lead you directly to step 2.

- **Step 1**
  Please choose a group you want to add the new device to. Click on **Continue**.



Add Device Assistant Step 2

- **Step 2**
  Add device settings as described below.

Add Device Settings

DEVICE NAME AND ADDRESS

Device Name	Enter a meaningful name to identify the device. The name will be shown by default in the device tree and in all alarms.
IP Version	Define which IP protocol PRTG will use to connect to this device. The setting is valid for all sensors created on this device. Choose between: ▪ **Connect using IPv4**: Use IP version 4 for all requests to this device.

DEVICE NAME AND ADDRESS

	▪ **Connect using IPv6**: Use IP version 6 for all requests to this device.
IP Address/DNS Name	Enter the IP address (either v4 or v6, depending on your selection above) or DNS name for the device. Most sensors created on this device will inherit this setting and they will try to connect to this address for monitoring. ⓘ There are some sensor types that still have their own setting for IP address/DNS name. Those sensors will use their own settings.
Tags	Enter one or more tags; confirm each tag by hitting the space, comma, or enter key. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. Tags are automatically inherited.
Device Icon	Choose a device icon from the list. It will be shown in the device tree.

DEVICE TYPE

Sensor Management	Select which type of auto-discovery you would like to perform for this device. Choose between: ▪ **Manual (no auto-discovery)**: Select this if you want to only create sensors manually. ▪ **Automatic device identification (standard, recommended)**: Use a small set of auto-discovery templates. This will scan your LAN and usually create a set of standard sensors on your device. ▪ **Automatic device identification (detailed, may create many sensors)**: Use an extended set of auto-discovery templates. This will scan your LAN and usually create many sensors on your device. ▪ **Automatic sensor creation using specific device template (s)**: Use specific auto-discovery templates only. Please select templates below. This will scan your LAN and add sensors defined in the template.
Discovery Schedule	This option is only visible if you select one of the auto-discovery options above. Define when the auto-discovery will run. Choose between:

DEVICE TYPE

- **Once**: Perform auto-discovery only once. For existing devices, this will initiate a one-time sensor update for the current device. If you select this option, you have to start the auto-discovery manually 250, it will not run automatically.
- **Hourly**: Perform auto-discovery for new sensors every hour.
- **Daily**: Perform auto-discovery for new sensors every day.
- **Weekly**: Perform auto-discovery for new sensors every week.

Device Template(s)

This option is only visible if using specific device templates (last option) is enabled above. Choose one or more templates by adding a check mark in front of the respective template name. You can also select and deselect all items by using the check box in the table head. These will be used for auto-discovery on the current device. Choose from:

- **ADSL**
- **Amazon Cloudwatch**
- **Buffalo TeraStation NAS**
- **Cisco ASA VPN**
- **Cisco Device (Generic)**
- **Dell EqualLogic**
- **Dell MDI Disk**
- **DNS Server**
- **Environment Jacarta**
- **Environment Poseidon**
- **FTP Server**
- **Generic Device (PING only)**
- **Generic Device (SNMP-enabled)**
- **Generic Device (SNMP-enabled, Detailed)**
- **HTTP Web Server**
- **Hyper V Host Server**
- **IPMI enabled devices**
- **Juniper NS Device**
- **Linux/UNIX Device (SNMP or SSH enabled)**
- **Mail Server (Generic)**

DEVICE TYPE

- **Mail Server (MS Exchange)**
- **Microsoft Sharepoint 2010**
- **NAS LenovoEMC**
- **NAS QNAP**
- **NAS Synology**
- **NetApp**
- **NTP Server**
- **Printer (HP)**
- **Printer Generic**
- **RDP Server**
- **RMON compatible device**
- **Server (Compaq/HP agents)**
- **Server (Dell)**
- **Sever Cisco UCS**
- **Server IBM**
- **SonicWALL**
- **SSL Security Check**
- **Switch (Cisco Catalyst)**
- **Switch (Cisco IOS Based)**
- **Switch (HP Procurve)**
- **UNIX/Linux Device**
- **UPS Health (APC)**
- **UPS Health (Generic)**
- **UPS Health (Leibert)**
- **VMware ESX / vCenter Server**
- **Webserver**
- **Windows (Detailed via WMI)**
- **Windows (via Remote Powershell)**
- **Windows (via WMI)**
- **Windows IIS (via SNMP)**
- **XEN Hosts**

DEVICE TYPE

- **XEN Virtual Machines**

Once the auto-discovery is finished, PRTG will create a new ticket 200 and list the device templates that were actually used to create new sensors. Templates that were not applied will not be shown in the ticket.

CREDENTIALS FOR WINDOWS SYSTEMS

Domain or Computer Name	Define the authority for Windows access. This is used for Windows Management Instrumentation (WMI) and other Windows sensors. If you want to use a Windows local user account on the target device, enter the computer name here. If you want to use a Windows domain user account (recommended), enter the (Active Directory) domain name here. If not explicitly defined, PRTG will automatically add a prefix in order to use the NT LAN Manager (NTLM) protocol. Do not leave this field empty.
User	Enter the username for Windows access. Usually, you will use credentials with administrator privileges.
Password	Enter the password for Windows access. Usually, you will use credentials with administrator privileges.

CREDENTIALS FOR LINUX/SOLARIS/MAC OS (SSH/WBEM) SYSTEMS

User	Enter a login name for the access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
Login	Define the authentication method to use for login. Choose between: ▪ **Login via Password**: Provide a password for login. Enter below. ▪ **Login via Private Key**: Provide a private key for authentication. PRTG can only handle keys in OpenSSH format that are not encrypted. You cannot use password protected keys here. In the text field, paste the entire private key, including the "BEGIN" and "END" lines. Please make sure the according public key is provided on the target machine. For details, please see Monitoring via SSH 3095.

CREDENTIALS FOR LINUX/SOLARIS/MAC OS (SSH/WBEM) SYSTEMS

Password	This field is only visible if you select password login above. Enter a password for the Linux access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
Private Key	This field is only visible if you select private key login above. Paste a private key into the field (OpenSSH format, unencrypted). Usually, you will use credentials with administrator privileges. If you do not insert a private key for the first time, but change the private key, you need to restart your PRTG core server service 2988 in order for the private key change to take effect! For details, please see **Monitoring via SSH** 3095.
For WBEM Use Protocol	Define the protocol to use for WBEM. This setting is only relevant if you use WBEM sensors. Choose between: ▪ **HTTP**: Use an unencrypted connection for WBEM. ▪ **HTTPS**: Use an SSL-encrypted connection for WBEM.
For WBEM Use Port	Define the port to use for WBEM. This setting is only relevant if you use WBEM sensors. Choose between: ▪ **Set automatically (port 5988 or 5989)**: Use one of the standard ports, depending on whether you choose unencrypted or encrypted connection above. ▪ **Set manually**: Use a custom port. Define below.
WBEM Port	This setting is only visible if you enable manual port selection above. Enter the WBEM port number.
SSH Port	Enter the port number to use for SSH connections. By default, PRTG uses this setting automatically for all SSH sensors 390, unless you define a different port number in the sensor settings.
SSH Rights Elevation	Define the rights that you want to use to execute the command on the target system. Choose between: ▪ **Run the command as the user connecting (default)**: Use the rights of the user who establishes the SSH connection, as defined above. ▪ **Run the command as another user using 'sudo' (with password)**: Use the rights of another user with a password required for sudo to run commands on the target device, for example, as root user.

CREDENTIALS FOR LINUX/SOLARIS/MAC OS (SSH/WBEM) SYSTEMS

	▪ **Run the command as another user using 'sudo' (without password)**: Use the rights of another user without a password required for sudo to run commands on the target device, for example, as root user. ▪ **Run the command as another user using 'su'**: Use the rights of another user with su to run commands on the target device.
Target User	This field is only visible if you choose sudo or su above. Enter a username to run the specified command as a user other than root. If you leave this field empty, you will run the command as root. Ensure you set the Linux password even if you use a public or private key for authentication. This is not necessary if the user is allowed to execute the command without a password.
Password Target User	This field is only visible if you choose to run the commands using su or sudo with password above. Enter the password for the specified target user.
SSH Engine	Select the method you want to use to access data with SSH sensors 3095. We strongly recommend that you keep the default engine! For now, you still can use the legacy mode to ensure compatibility with your target systems. Choose between: ▪ **Default (recommended)**: This is the default monitoring method for SSH sensors. It provides best performance and security. ▪ **Compatibility Mode (deprecated)**: Try this legacy method only if the default mode does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions and is deprecated. We will remove this legacy option soon, so please try to get your SSH sensors running with the default SSH engine. ⓘ You can also individually select the SSH engine for each SSH sensor in the sensor settings.

CREDENTIALS FOR VMWARE/XENSERVER

User	Enter a login name for access to VMware and Xen servers. Usually, you will use credentials with administrator privileges.
Password	Enter a password for access to VMware and Xen servers. Usually, you will use credentials with administrator privileges.

CREDENTIALS FOR VMWARE/XENSERVER

Single Sign-On (SSO) passwords for vSphere do not support special characters. Please see the manual sections for VMware sensors for details.

VMware Protocol	Define the protocol used for the connection to VMware and XenServer. Choose between: ▪ **HTTPS (recommended)**: Use an SSL-encrypted connection to VMware and XenServers. ▪ **HTTP**: Use an unencrypted connection to VMware and XenServers.
Session Pool	Define if you want to use session pooling for VMware sensors. Choose between: ▪ **Reuse session for for multiple scans (recommended)**: Select this option to use session pooling. With session pooling, a VMware sensor uses the same session as created in advance to query data and needs not to log in and out for each sensor scan. We recommend that you choose this option because it reduces network load and log entries on the target device, resulting in better performance. ▪ **Create a new session for each scan**: If you select this option and disable session pooling, a VMware sensor has to log in and out for each sensor scan. We recommend that you use the session pooling option above for better performance.

CREDENTIALS FOR SNMP DEVICES

SNMP Version	Select the SNMP version for the device connection. Choose between: ▪ **v1**: Use the simple v1 protocol for SNMP connections. This protocol only offers clear-text data transmission, but it is usually supported by all devices. SNMP v1 does not support 64-bit counters which may result in invalid data when monitoring traffic via SNMP. ▪ **v2c (recommended)**: Use the more advanced v2c protocol for SNMP connections. This is the most common SNMP version. Data is still transferred as clear-text, but it supports 64-bit counters. ▪ **v3**: Use the v3 protocol for SNMP connections. It provides secure authentication and data encryption.

CREDENTIALS FOR SNMP DEVICES

When using SNMP v3 you can only monitor a limited number of sensors per second due to internal limitations. The limit is somewhere between 1 and 50 sensors per second (depending on the SNMP latency of your network). This means that using an interval of 60 seconds limits you to between 60 and 3000 SNMP v3 sensors for each probe. If you experience an increased Interval Delay or Open Requests with the **Probe Health Sensor** 1378, distribute the load over multiple probes 3196. SNMP v1 and v2 do not have this limitation.

Community String	This setting is only visible if you select SNMP version **v1** or **v2c** above. Enter the community string of your devices. This is a kind of "clear-text password" for simple authentication. We recommend that you use the default value.
Authentication Type	This setting is only visible if you select SNMP version **v3** above. Choose between: ▪ **MD5**: Use Message-Digest Algorithm 5 (MD5) for authentication. ▪ **SHA**: Use Secure Hash Algorithm (SHA) for authentication. The type you choose must match the authentication type of your device. If you do not want to use authentication, but you need SNMP v3, for example, because your device requires context, you can leave the field **Password** empty. In this case, SNMP_SEC_LEVEL_NOAUTH is used and authentication deactivated entirely.
User	This setting is only visible if you select SNMP version **v3** above. Enter a username for secure authentication. This value must match the username of your device.
Password	This setting is only visible if you select SNMP version **v3** above. Enter a password for secure authentication. This value must match the password of your device.
Encryption Type	This setting is only visible if you select SNMP version **v3** above. Select an encryption type. Choose between: ▪ **DES**: Use Data Encryption Standard (DES) as encryption algorithm. ▪ **AES**: Use Advanced Encryption Standard (AES) as encryption algorithm. AES 192 and AES 256 are not supported by Net-SNMP because they lack RFC specification.

CREDENTIALS FOR SNMP DEVICES

	The type that you choose must match the encryption type of your device.
Data Encryption Key	This setting is only visible if you select SNMP version **v3** above. Enter an encryption key here. If you provide a key in this field, SNMP data packets are encrypted using the encryption algorithm selected above, which provides increased security. The key that you enter here must match the encryption key of your device. If the key you enter in this field does not match the key configured on the target SNMP device, you will not get an error message about this! Please enter a string or leave the field empty.
Context Name	This setting is only visible if you select SNMP version **v3** above. Enter a context name only if it is required by the configuration of the device. Context is a collection of management information accessible by an SNMP device. Please enter a string.
SNMP Port	Enter the port for the SNMP communication. We recommend that you use the default value.
SNMP Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than the value you enter here, the request is aborted and an error message triggered.

CREDENTIALS FOR DATABASE MANAGEMENT SYSTEMS

The settings you define in this section apply to the following sensor types:

- ADO SQL v2 Sensor 418
- Microsoft SQL v2 Sensor 1135
- MySQL v2 Sensor 1151
- Oracle SQL v2 Sensor 1253
- PostgreSQL Sensor 1363

Port for Databases	Define which ports PRTG will use for connections to the monitored databases. Choose between:

CREDENTIALS FOR DATABASE MANAGEMENT SYSTEMS

- **Set automatically (default port, recommended)**: PRTG automatically determines the type of the monitored database and uses the corresponding default port to connect. See below for a list of default ports.
- **Define one custom port valid for all database sensors**: Choose this option if your database management systems do not use the default ports. Define the port for database connections manually below. If you choose this option, PRTG will use the custom port for all database sensors.

If you choose the automatic port selection, PRTG uses the following default ports:

- Microsoft SQL: 1433
- MySQL: 3306
- Oracle SQL: 1521
- PostgreSQL: 5432

Custom Database Port

Enter the number of the port that PRTG will use for database connections. Please enter an integer value.

All database sensors on this device will use this port to connect.

Authentication Mode

Select the authentication method for the connection to the SQL database. Choose between:

- **Windows authentication with impersonation**: If you select this option, PRTG uses the Windows credentials as defined in the particular device settings 365 for the database connection.
  The user whose credentials are used needs to have permissions to log on to the system on which the PRTG probe with a database sensor runs. This is required for the impersonation.
- **SQL server authentication**: Choose this option if you want to use explicit credentials for database connections.

User

This field is only visible if you select SQL server authentication above. Enter the username for the database connection.

Password

This field is only visible if you select SQL server authentication above. Enter the password for the database connection.

CREDENTIALS FOR DATABASE MANAGEMENT SYSTEMS

Timeout (Sec.)	Enter a timeout in seconds for the request. Please enter an integer value. If the reply takes longer than this value defines, the sensor cancels the request and triggers an error message. The maximum timeout value is 300 seconds (5 minutes).

CREDENTIALS FOR AMAZON CLOUDWATCH

Access Key	Enter your Amazon Web Services (AWS) access key. Please see the corresponding Amazon CloudWatch sensor 391 documentation to learn more about the rights that are required for querying AWS CloudWatch metrics.
Secret Key	Enter your Amazon Web Services (AWS) secret key. Please see the corresponding Amazon CloudWatch sensor 391 documentation to learn more about the rights that are required for querying AWS CloudWatch metrics.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

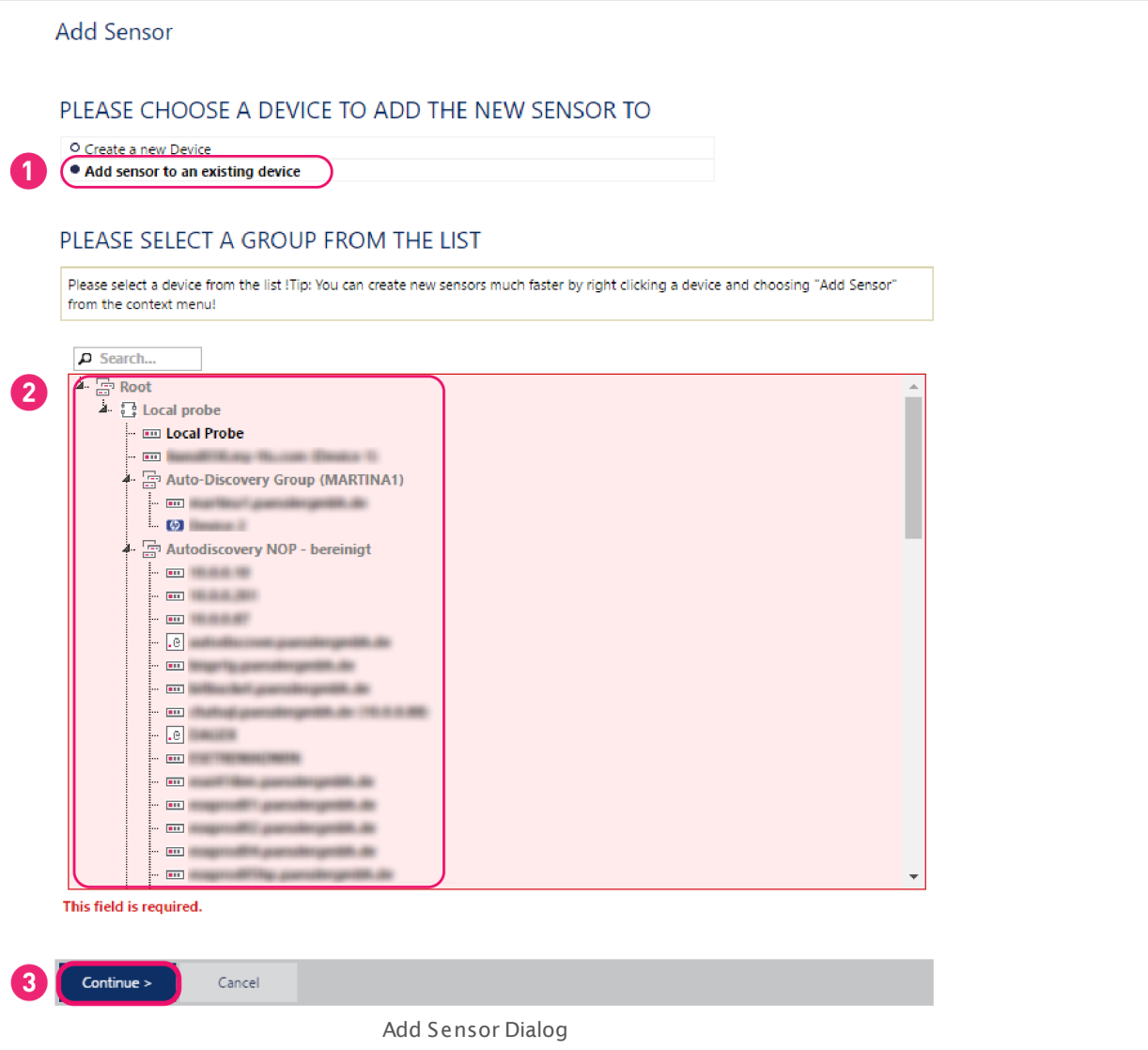
Click the **Continue** button to save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

7.2.3 Add a Sensor

This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

To add a sensor manually, select **Sensors | Add Sensor** from the main menu. Then an assistant will appear, leading you through two steps. For a faster setup, you can select **Add Sensor...** in the context menu of the device that you want to add the new sensor to. This will skip the device selection and take you directly to step 2 289.

Step 1 - Select Device



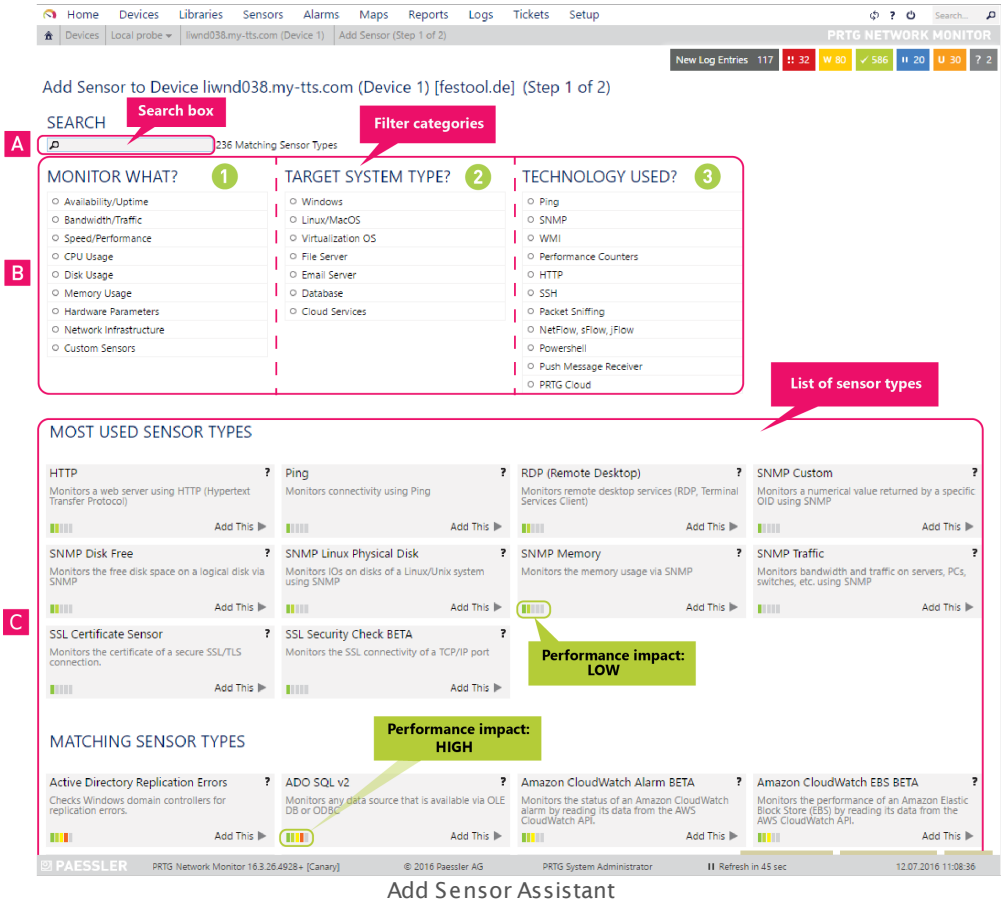
Add Sensor Dialog

Click here to enlarge: https://media-s3.paessler.com/prtg-screenshots/addsensor2_new.png

- Select **Add sensor to an existing device** (default setting).
- Choose the device you want to add the new sensor to.
- Click **Continue**.

The add sensor assistant appears.

Step 2 - Choose Sensor Type



Add Sensor Assistant

Click here to enlarge: https://media-s3.paessler.com/prtg-screenshots/addsensor3.png

The add sensor assistant helps you choose the correct sensor (see screenshot above).

- Narrow down the sensor types:
  - Enter (parts of) the name into the search box. A
  - Choose appropriate criteria to filter the shown sensor types. B
  - Go through the detailed list of sensors matching the selected device. C

- If you cannot find a suitable sensor, search for custom sensors in our PRTG Script World. Just click **Looking For More Sensor Types?**. See section List of Available Sensor Types—Script World Sensors 404 for more information.

- Choose which sensor best monitors the parameters you require.
- Click the sensor box to select this sensor.

The sensor settings dialog opens.

- Enter suitable sensor settings.

PRTG suggests sensor types to create on the selected device. This recommendation is automatically calculated based on the current user's sensor usage and shows the ten most commonly used sensor types (if enough sensor types are already in use).

If you are unsure which sensor type will provide the information you require, then we recommend that you use the filter categories to progressively narrow down your choices.

You can either:

- Select the type of parameter you want to monitor via **Monitor What?**. 1
- Specify the type of target system you want to monitor and see what sensors are available for this type of hardware in **Target System Type?**. 2
- Choose the technology that you want to use for monitoring (for example SNMP or WMI) in **Technology Used?**. 3

Please also consider whether a sensor's performance impact is high or low by checking the bar in the lower left corner of the sensor box. For further information, see this Knowledge Base article: How to Speed Up PRTG (especially section 4 - Sensor Type and Monitoring Considerations)

This bar indicates that this sensor has a high performance impact.

This bar indicates that this sensor has a low performance impact.

- Confirm via **Continue**.

PRTG will now create the sensor. The device tree opens.

For more information about a sensor type, please see the manual section of the respective sensor (directly accessible via the "?"-symbol in the top-right corner). You can also go to the **List of Available Sensor Types** section to find a comprehensive overview of sensor types.

More

Knowledge Base: How can I change the number of entries in most used sensor types?

- https://kb.paessler.com/en/topic/59788

Knowledge Base: How to Speed Up PRTG (especially section 4 - Sensor Type and Monitoring Considerations)

- https://kb.paessler.com/en/topic/2733

7.3 Manage Device Tree

While viewing the device tree (or parts of it), click the **Management** tab to enter a different tree view that shows your devices and sensors in a less colorful way. While in this view, you can move monitoring objects using drag&drop in your browser window. You can also view and edit object settings by selecting the object. Changes take effect immediately. When done, leave the **Management** tab.

To arrange objects in the tree, you have the following options:

Drag&Drop a Sensor

You can either move a sensor within the same device, or clone a sensor to another device.

- Within the same device, drag any sensor and drop it to the place where you want to have it. A shadow will show the future position. When dropping, the sensor will be moved to this position and existing sensors will be lined up after it. This is a very easy way to reposition your sensors.

- Drag any sensor from one device and drop it on another to clone a sensor. This will create the same sensor type, with the same settings, on the new device, while maintaining the original sensor. A shade will show the future position.
  Cloned sensors are put to **Pause** status initially to give you the chance to change any settings before monitoring begins. Please check the settings 188 and resume 214 monitoring.

You cannot clone 'fixed' objects, such as the root group or a probe device.

To clone entire groups or devices, please use the **Clone Object** 2812 functionality accessible via the objects' Context Menu 215.

Drag&Drop a Group or Device

You can change a group's or device's position by using drag&drop.

- Within the same probe or group, drag any group or device and move it up or down in the device tree. A small red arrow will appear, showing the future position. When dropping, the group or device will be moved to this position and existing probes, groups, and devices will be lined up underneath. This is a very easy way to reposition your groups or devices.

- Drag any group or device from one probe or group and drop it on another probe or group. A small red arrow will appear, showing the future position. When dropping, the group or device will be moved to the new probe or group. Existing groups and devices will be lined up underneath. This is a very easy way to change the probe a group or device is part of, or to add groups or devices to other groups.

The **Local Probe** and Remote Probes cannot be moved.

Multi-Edit Object Properties

You can use Multi-Edit for object settings:

- Hold down the Ctrl key and select multiple groups, devices, or sensors (one of a kind).
- In the appearing dialog, select the settings you want to edit, change the according values, and click **Save**. The changes will be applied to all selected objects.

The dialog is the same as described in the **Multi-Edit** 2816 (Edit Settings) section.

Related Topics

For other ways to arrange objects, please see

- **Arrange Objects** 2811
- **Create Device Template** 2818
- **Clone Object** 2812

7.4 Root Group Settings

On the **Root** group's overview page, click the **Settings** tab to change settings.

The Root Group is Special

The **Root** group is the highest instance in the object hierarchy of your PRTG setup and parent to all other objects. Therefore, all objects inherit settings from the **Root** group. If you define important settings on this high level, work will be easier later on. So, before you create your own sensors, it is a good idea to review the **Root** group's settings to ensure they suit your network. There are already reasonable presets made with installation.

If necessary, you can override every setting for every single child object later. To do so, simply disable the respective **Inherit** option of an object.

Root Group Settings

The following settings are available in the **Settings** tab. As you may not need all of these, just regard the settings you really need and ignore the others. All settings you define here can easily be inherited to all other objects in your setup.

This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

BASIC GROUP SETTINGS

Group Name	Enter a meaningful name to identify the group. The name will be shown by default in the devices tree and in all alarms.
Status	Define if monitoring for this group is started or paused. Choose between: ▪ **Started**: Monitor this group. ▪ **Paused**: Pause monitoring for this group. All sensors on all devices in this group will be paused until this setting is changed again.

LOCATION

Location (for Geo Maps)	When you want to use **Geo Maps** 2824, enter a location in the first line. Geographical maps will display objects (devices, groups) then with a flag, showing the current status using a color code similar to the sensor status icons 163 (green - yellow - orange - red). You can enter a full postal address, city and country only, or latitude and longitude. It is possible to enter any text before, between, and after the coordinates, PRTG will parse latitude and longitude automatically, for example: 49.452778 11.077778 or enter 49.452778 any 11.077778 text A minus sign (-) in the first line will hide an object from geo maps. In this case you can enter location information in line two and following. You can define a specific label for each location: enter a string denoting the label in the first line and provide geo coordinates in the second line. This geo marker will show then the object with the label in the PRTG geo map. The preview map will always hava a road map layout regardless of the map layout you set in **User Interface** 2945.

CREDENTIALS FOR WINDOWS SYSTEMS

Domain or Computer Name	Define the authority for Windows access. This is used for Windows Management Instrumentation (WMI) and other Windows sensors. If you want to use a Windows local user account on the target device, enter the computer name here. If you want to use a Windows domain user account (recommended), enter the (Active Directory) domain name here. If not explicitly defined, PRTG will automatically add a prefix in order to use the NT LAN Manager (NTLM) protocol. Do not leave this field empty.
User	Enter the username for Windows access. Usually, you will use credentials with administrator privileges.
Password	Enter the password for Windows access. Usually, you will use credentials with administrator privileges.

CREDENTIALS FOR LINUX/SOLARIS/MAC OS (SSH/WBEM) SYSTEMS

User	Enter a login name for the access via SSH and WBEM. Usually, you will use credentials with administrator privileges.

CREDENTIALS FOR LINUX/SOLARIS/MAC OS (SSH/WBEM) SYSTEMS

Login	Define the authentication method to use for login. Choose between: ▪ **Login via Password**: Provide a password for login. Enter below. ▪ **Login via Private Key**: Provide a private key for authentication. PRTG can only handle keys in OpenSSH format that are not encrypted. You cannot use password protected keys here. In the text field, paste the entire private key, including the "BEGIN" and "END" lines. Please make sure the according public key is provided on the target machine. For details, please see **Monitoring via SSH** 3095.
Password	This field is only visible if you select password login above. Enter a password for the Linux access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
Private Key	This field is only visible if you select private key login above. Paste a private key into the field (OpenSSH format, unencrypted). Usually, you will use credentials with administrator privileges. If you do not insert a private key for the first time, but change the private key, you need to restart your PRTG core server service 2988 in order for the private key change to take effect! For details, please see **Monitoring via SSH** 3095.
For WBEM Use Protocol	Define the protocol to use for WBEM. This setting is only relevant if you use WBEM sensors. Choose between: ▪ **HTTP**: Use an unencrypted connection for WBEM. ▪ **HTTPS**: Use an SSL-encrypted connection for WBEM.
For WBEM Use Port	Define the port to use for WBEM. This setting is only relevant if you use WBEM sensors. Choose between: ▪ **Set automatically (port 5988 or 5989)**: Use one of the standard ports, depending on whether you choose unencrypted or encrypted connection above. ▪ **Set manually**: Use a custom port. Define below.
WBEM Port	This setting is only visible if you enable manual port selection above. Enter the WBEM port number.
SSH Port	Enter the port number to use for SSH connections. By default, PRTG uses this setting automatically for all SSH sensors 390, unless you define a different port number in the sensor settings.

CREDENTIALS FOR LINUX/SOLARIS/MAC OS (SSH/WBEM) SYSTEMS

SSH Rights Elevation	Define the rights that you want to use to execute the command on the target system. Choose between: ▪ **Run the command as the user connecting (default)**: Use the rights of the user who establishes the SSH connection, as defined above. ▪ **Run the command as another user using 'sudo' (with password)**: Use the rights of another user with a password required for sudo to run commands on the target device, for example, as root user. ▪ **Run the command as another user using 'sudo' (without password)**: Use the rights of another user without a password required for sudo to run commands on the target device, for example, as root user. ▪ **Run the command as another user using 'su'**: Use the rights of another user with su to run commands on the target device.
Target User	This field is only visible if you choose sudo or su above. Enter a username to run the specified command as a user other than root. If you leave this field empty, you will run the command as root. Ensure you set the Linux password even if you use a public or private key for authentication. This is not necessary if the user is allowed to execute the command without a password.
Password Target User	This field is only visible if you choose to run the commands using su or sudo with password above. Enter the password for the specified target user.
SSH Engine	Select the method you want to use to access data with SSH sensors 3095. We strongly recommend that you keep the default engine! For now, you still can use the legacy mode to ensure compatibility with your target systems. Choose between: ▪ **Default (recommended)**: This is the default monitoring method for SSH sensors. It provides best performance and security. ▪ **Compatibility Mode (deprecated)**: Try this legacy method only if the default mode does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions and is deprecated. We will remove this legacy option soon, so please try to get your SSH sensors running with the default SSH engine. ⓘ You can also individually select the SSH engine for each SSH sensor in the sensor settings.

CREDENTIALS FOR VMWARE/XENSERVER

User	Enter a login name for access to VMware and Xen servers. Usually, you will use credentials with administrator privileges.
Password	Enter a password for access to VMware and Xen servers. Usually, you will use credentials with administrator privileges. Single Sign-On (SSO) passwords for vSphere do not support special characters. Please see the manual sections for VMware sensors for details.
VMware Protocol	Define the protocol used for the connection to VMware and XenServer. Choose between: ▪ **HTTPS (recommended)**: Use an SSL-encrypted connection to VMware and XenServers. ▪ **HTTP**: Use an unencrypted connection to VMware and XenServers.
Session Pool	Define if you want to use session pooling for VMware sensors. Choose between: ▪ **Reuse session for for multiple scans (recommended)**: Select this option to use session pooling. With session pooling, a VMware sensor uses the same session as created in advance to query data and needs not to log in and out for each sensor scan. We recommend that you choose this option because it reduces network load and log entries on the target device, resulting in better performance. ▪ **Create a new session for each scan**: If you select this option and disable session pooling, a VMware sensor has to log in and out for each sensor scan. We recommend that you use the session pooling option above for better performance.

CREDENTIALS FOR SNMP DEVICES

SNMP Version	Select the SNMP version for the device connection. Choose between: ▪ **v1**: Use the simple v1 protocol for SNMP connections. This protocol only offers clear-text data transmission, but it is usually supported by all devices. SNMP v1 does not support 64-bit counters which may result in invalid data when monitoring traffic via SNMP.

CREDENTIALS FOR SNMP DEVICES

- **v2c (recommended)**: Use the more advanced v2c protocol for SNMP connections. This is the most common SNMP version. Data is still transferred as clear-text, but it supports 64-bit counters.
- **v3**: Use the v3 protocol for SNMP connections. It provides secure authentication and data encryption.

When using SNMP v3 you can only monitor a limited number of sensors per second due to internal limitations. The limit is somewhere between 1 and 50 sensors per second (depending on the SNMP latency of your network). This means that using an interval of 60 seconds limits you to between 60 and 3000 SNMP v3 sensors for each probe. If you experience an increased Interval Delay or Open Requests with the **Probe Health Sensor** 1378, distribute the load over multiple probes 3196. SNMP v1 and v2 do not have this limitation.

Community String

This setting is only visible if you select SNMP version **v1** or **v2c** above. Enter the community string of your devices. This is a kind of "clear-text password" for simple authentication. We recommend that you use the default value.

Authentication Type

This setting is only visible if you select SNMP version **v3** above. Choose between:

- **MD5**: Use Message-Digest Algorithm 5 (MD5) for authentication.
- **SHA**: Use Secure Hash Algorithm (SHA) for authentication.

The type you choose must match the authentication type of your device.

If you do not want to use authentication, but you need SNMP v3, for example, because your device requires context, you can leave the field **Password** empty. In this case, SNMP_SEC_LEVEL_NOAUTH is used and authentication deactivated entirely.

User

This setting is only visible if you select SNMP version **v3** above. Enter a username for secure authentication. This value must match the username of your device.

Password

This setting is only visible if you select SNMP version **v3** above. Enter a password for secure authentication. This value must match the password of your device.

Encryption Type

This setting is only visible if you select SNMP version **v3** above. Select an encryption type. Choose between:

- **DES**: Use Data Encryption Standard (DES) as encryption algorithm.

CREDENTIALS FOR SNMP DEVICES

- **AES**: Use Advanced Encryption Standard (AES) as encryption algorithm.

AES 192 and AES 256 are not supported by Net-SNMP because they lack RFC specification.

The type that you choose must match the encryption type of your device.

Data Encryption Key	This setting is only visible if you select SNMP version **v3** above. Enter an encryption key here. If you provide a key in this field, SNMP data packets are encrypted using the encryption algorithm selected above, which provides increased security. The key that you enter here must match the encryption key of your device. If the key you enter in this field does not match the key configured on the target SNMP device, you will not get an error message about this! Please enter a string or leave the field empty.
Context Name	This setting is only visible if you select SNMP version **v3** above. Enter a context name only if it is required by the configuration of the device. Context is a collection of management information accessible by an SNMP device. Please enter a string.
SNMP Port	Enter the port for the SNMP communication. We recommend that you use the default value.
SNMP Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than the value you enter here, the request is aborted and an error message triggered.

CREDENTIALS FOR DATABASE MANAGEMENT SYSTEMS

The settings you define in this section apply to the following sensor types:

- ADO SQL v2 Sensor 418
- Microsoft SQL v2 Sensor 1135
- MySQL v2 Sensor 1151
- Oracle SQL v2 Sensor 1253
- PostgreSQL Sensor 1363

CREDENTIALS FOR DATABASE MANAGEMENT SYSTEMS

Port for Databases	Define which ports PRTG will use for connections to the monitored databases. Choose between: ▪ **Set automatically (default port, recommended)**: PRTG automatically determines the type of the monitored database and uses the corresponding default port to connect. See below for a list of default ports. ▪ **Define one custom port valid for all database sensors**: Choose this option if your database management systems do not use the default ports. Define the port for database connections manually below. If you choose this option, PRTG will use the custom port for all database sensors. If you choose the automatic port selection, PRTG uses the following default ports: ▪ Microsoft SQL: 1433 ▪ MySQL: 3306 ▪ Oracle SQL: 1521 ▪ PostgreSQL: 5432
Custom Database Port	Enter the number of the port that PRTG will use for database connections. Please enter an integer value. All database sensors on this device will use this port to connect.
Authentication Mode	Select the authentication method for the connection to the SQL database. Choose between: ▪ **Windows authentication with impersonation**: If you select this option, PRTG uses the Windows credentials as defined in the particular device settings for the database connection. The user whose credentials are used needs to have permissions to log on to the system on which the PRTG probe with a database sensor runs. This is required for the impersonation. ▪ **SQL server authentication**: Choose this option if you want to use explicit credentials for database connections.
User	This field is only visible if you select SQL server authentication above. Enter the username for the database connection.
Password	This field is only visible if you select SQL server authentication above. Enter the password for the database connection.

CREDENTIALS FOR DATABASE MANAGEMENT SYSTEMS

Timeout (Sec.)	Enter a timeout in seconds for the request. Please enter an integer value. If the reply takes longer than this value defines, the sensor cancels the request and triggers an error message. The maximum timeout value is 300 seconds (5 minutes).

CREDENTIALS FOR AMAZON CLOUDWATCH

Access Key	Enter your Amazon Web Services (AWS) access key. Please see the corresponding Amazon CloudWatch sensor 391 documentation to learn more about the rights that are required for querying AWS CloudWatch metrics.
Secret Key	Enter your Amazon Web Services (AWS) secret key. Please see the corresponding Amazon CloudWatch sensor 391 documentation to learn more about the rights that are required for querying AWS CloudWatch metrics.

WINDOWS COMPATIBILITY OPTIONS

When experiencing problems while monitoring via Windows sensors, you can set some compatibility options for trouble shooting.

Preferred Data Source	Define the method Windows sensors will use to query data. This setting is valid only for hybrid sensors offering performance counter and Windows Management Instrumentation (WMI) technology. The setting will be ignored for all other sensors! Choose between: ▪ **Performance Counters and fallback to WMI**: Try to query data via performance counters. If this is not possible, establish a connection via WMI. ▪ **Performance Counters only**: Query data via performance counters only. If this is not possible, a sensor will return no data. ▪ **WMI only (recommended)**: Query data via WMI only. If this is not possible, a sensor will return no data. In current PRTG versions, this is our recommendation to achieve best performance and stability.
Timeout Method	Specify the time the sensor will wait for the return of its WMI query before aborting it with an error message. Choose between:

WINDOWS COMPATIBILITY OPTIONS

- **Use 1.5x scanning interval (recommended)**: Use a default of one and a half times the scanning interval set for the sensor (see below in this settings).
- **Set manually**: Enter a timeout value manually.

We recommend that you use the default value. Only if you experience ongoing timeout errors, try increasing the timeout value.

Timeout Value (Sec.)

This field is only visible if the manual timeout method is selected above. Specify the time the sensor will wait for the return of its WMI query before aborting with an error message. Please enter an integer value.

SNMP COMPATIBILITY OPTIONS

When experiencing problems while monitoring via Simple Network Management Protocol (SNMP) sensors, you can set some compatibility options for trouble shooting.

SNMP Delay (ms)

Add a time in milliseconds that will be waited between two SNMP requests. This can help increase device compatibility. Please enter an integer value. We recommend that you use the default value. If you experience SNMP connection failures, please increase it. You can define a delay between 0 and 100, higher delays are not supported and will be discarded.

Failed Requests

Define if an SNMP sensor will try again after a request fails.

- **Retry (recommended)**: Try again if an SNMP request fails. This can help prevent false error messages due to temporary timeout failures.
- **Do not retry**: Do not retry if an SNMP request fails. With this setting enabled an SNMP sensor will be set to error status earlier.

Overflow Values

Define how PRTG will handle overflow values. Some devices do not handle internal buffer overflows correctly. This can cause false peaks.

- **Ignore overflow values**: Ignore overflow values and do not include them in the monitoring data.
- **Handle overflow values as valid results**: Regard all overflow values as regular data and include them in the monitoring data.

SNMP COMPATIBILITY OPTIONS

We recommend that you use the default value.

If you experience problems because of strange peaks in your data graphs, change this option. Peaks might indicate that the monitored device resets counters without an overflow. PRTG interprets such a behavior as overflow that results in data peaks. Choose the option **Ignore overflow values** in this case. For more details, see this Knowledge Base article: What is the Overflow Values setting in the SNMP Compatibility Options?

Zero Values

Define how PRTG will handle zero values. Some devices send incorrect zero values. This can cause false peaks.

- **Ignore zero values for delta sensors (recommended)**: Ignore zero values and do not include them in the monitoring data.
- **Handle zero values as valid results for delta sensors**: Regard all zero values as regular data and include them in the monitoring data.

We recommend that you use the default value. If you experience problems, change this option.

32-bit/64-bit Counters

Define which kind of traffic counters PRTG will search for on a device.

- **Use 64-bit counters if available (recommended)**: The interface scan will use 64-bit traffic counters, if available. This can avoid buffer overflows in the devices.
- **Use 32-bit counters only**: The interface scan will always use 32-bit traffic counters, even if 64-bit counters are available. This can lead to more reliable monitoring for some devices.

We recommend that you use the default value. If you experience problems, change this option.

Request Mode

Define which kind of request method PRTG uses for SNMP sensors.

- **Use multi get (recommended)**: Bundle multiple SNMP requests into one request.
- **Use single get**: Use one request for each SNMP value. This can increase compatibility with older devices.

We recommend that you use the default value. If you experience problems, change this option.

PRTG uses paging for SNMP requests. This means that if a sensor has to query more than 20 OIDs, it will automatically poll the OIDs in packages of 20 OIDs each per request.

SNMP COMPATIBILITY OPTIONS

Port Name Template

Define how the name of SNMP sensors created on a device will be put together. Enter a template using several variables. When adding new sensors, PRTG scans the interface for available counters at certain OIDs. At each OID usually several fields are available with interface descriptions. They are different for every device and OID. PRTG will use the information in these fields to name the sensors. If a field is empty or not available, an empty string is added to the name. As default, **([port]) [ifalias]** is set as port name template, which will create a name such as (001) Ethernet1, for example. You can use any field names available at a certain OID of your device, among which are:

- **[port]**: The port number of the monitored interface.
- **[ifalias]**: The 'alias' name for the monitored interface as specified by a network manager, providing a non-volatile handling.
- **[ifname]**: The textual name of the monitored interface as assigned by the local device.
- **[ifdescr]**: A textual string containing information about the monitored device or interface, for example, manufacturer, product name, version.
- **[ifspeed]**: An estimate of the monitored interface's current bandwidth (KBit/s).
- **[ifsensor]**: The type of the sensor, this is SNMP Traffic or SNMP RMON. This is useful to differentiate between your SNMP Traffic 2132 and SNMP RMON 2073 sensors.

Combine them as you like to obtain suitable sensor names.

For more information about SNMP sensor names, see this Knowledge Base article: How can I change the defaults for names automatically generated for new SNMP sensors?

Port Name Update

Define how PRTG will react if you change port names in your physical device (for example, a switch or router). Choose between:

- **Keep port names (use this if you edit the names in PRTG)**: Do not automatically adjust sensor names. This is the best option if you want to change names in PRTG manually.
- **Automatic sensor name update if name changes in device**: If PRTG detects changes of port names in your physical device, it will try to automatically adjust sensor names accordingly.

For more information about automatic updates of names, see this Knowledge Base article: Automatically update port name and number for SNMP Traffic sensors when the device changes them

SNMP COMPATIBILITY OPTIONS

Port Identification

Define which field will be used for SNMP interface identification. Choose between:

- **Automatic (recommended)**: Tries the ifAlias field first to identify an SNMP interface and then ifDescr.
  ifName will not be tried automatically.
- **Use ifAlias**: For most devices ifAlias is the best field to get unique interface names.
- **Use ifDescr**: Use this option if the port order of your device changes after a reboot, and there is no ifAlias field available. For example, this is the best option for Cisco ASA devices.
  When using this option it is important that your device returns unique interface names in the ifDescr field.
- **Use ifName**: You can also use this option if there is no unique ifAlias available.
  When using this option it is important that your device returns unique interface names in the ifName field.
- **No Port Update**: Use this option to disable automatic port identification.

Start Interface Index

For SNMP Traffic sensors 2132, define at which index PRTG will start to query the interface range during sensor creation. Use 0 for automatic mode. We recommend that you use the default value.

End Interface Index

For SNMP Traffic sensors 2132, define at which index PRTG will stop to query the interface range during sensor creation. Use 0 for automatic mode. We recommend that you use the default value.

PROXY SETTINGS FOR HTTP SENSORS

HTTP Proxy Settings

The proxy settings determine how a sensor connects to a given URL. You can enter data for an HTTP proxy server that sensors will use when connecting via HTTP or HTTPS.

This setting affects monitoring only and determines the behavior of HTTP sensors. To change proxy settings for the core server, please see **System Administration—Core & Probes** 2967.

PROXY SETTINGS FOR HTTP SENSORS

The SSL Certificate Sensor 2289 and the SSL Security Check Sensor 2299 do not support HTTP proxies, but you can configure connections via SOCKS proxies in their sensor settings.

Name	Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.
Port	Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.
User	If the proxy requires authentication, enter the username for the proxy login. Only basic authentication is available! Please enter a string or leave the field empty.
Password	If the proxy requires authentication, enter the password for the proxy login. Only basic authentication is available! Please enter a string or leave the field empty.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.

SCANNING INTERVAL

- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	To terminate a current maintenance window before the defined end date, you can change the time in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency settings are available only in Probe Settings 312, Group Settings 334, Device Settings 360, and Sensor Settings 384.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** ⓘ Custom channel types can be set on sensor level only.

ADVANCED NETWORK ANALYSIS

Unusual Detection	Define if you want to benefit from unusual detection 2956 for sensors. You can configure the behavior of unusual detection (or disable it completely) in the system settings 2956. Choose between: ▪ **Enabled**: Activate unusual detection for this object and, by default, for all objects underneath in the hierarchy 118 of the device tree. Sensors affected by this setting will turn to orange color (unusual sensor status 163) if PRTG detects unusual activity. ▪ **Disabled**: Do not activate unusual detection. PRTG will ignore unusual values for sensors affected by this setting. These sensor will not show an unusual sensor status.
Similar Sensors Detection	Define if you want to activate **Similar Sensors** 180 analysis. You can configure the depth of analysis of similar sensors detection (or disable it completely) in the system settings 2958. Choose between: ▪ **Enabled**: Activate similar sensors detection for this object and, by default, for all objects underneath in the hierarchy 118 of the device tree. PRTG considers all sensors affected by this setting during similarity analysis. ▪ **Disabled**: Do not activate similar sensors detection. PRTG will not consider sensors affected by this setting during similarity analysis.
System Information	Define if you want to retrieve and show **System Information** 193 for your devices. Choose between:

ADVANCED NETWORK ANALYSIS

- **Enabled**: Activate the system information feature for this object and, by default, for all objects underneath in the hierarchy 118 of the device tree.
- **Disabled**: Do not activate system information.

This setting is not available for local probes in PRTG on demand.

Click **Save** to save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Notifications

The status or the data of a sensor can trigger notifications. Using this mechanism, you can configure external alerting tailored to your needs. In an object's detail page, click the **Notifications** tab to change sensor notification triggers. The defined triggers will be inherited down to sensor level. For detailed information, please see **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see **Object Settings** 188 section.

More

Knowledge Base: How does PRTG compute CPU Index, Traffic Index and Response Time Index?

- https://kb.paessler.com/en/topic/313

Knowledge Base: How can I add my own device icons for use in the PRTG web interface?

- https://kb.paessler.com/en/topic/7313

Knowledge Base: How can I change the defaults for names automatically generated for new SNMP sensors?

- https://kb.paessler.com/en/topic/7363

Knowledge Base: Automatically update port name and number for SNMP Traffic sensors when the device changes them

- https://kb.paessler.com/en/topic/25893

Knowledge Base: What is the Overflow Values setting in the SNMP Compatibility Options?

- https://kb.paessler.com/en/topic/43503

7.5 Probe Settings

On a probe's overview page, click the **Settings** tab to change settings.

Add Remote Probe

You can add additional remote probes to your setup to extend your monitoring to networks that are not directly reachable by your PRTG core installation or cluster.

See section Add Remote Probe 3195 for more details.

Probe Settings

The following settings are available in the **Settings** tab of every probe. Because you may not need all of these for every probe, just regard the settings you really need, ignoring the others.

We recommend that you define as many settings as possible in the Root 294 group, so you can inherit them to all other objects further down in the device tree hierarchy 118.

This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

BASIC PROBE SETTINGS

Probe Name	Enter a meaningful name to identify the probe. The name will be shown by default in the devices tree and in all alarms.
Tags	Enter one or more Tags 124. Confirm each tag by hitting the space, comma, or enter key. You can use tags to group objects and use tag-filtered views later on. Tags are not case sensitive.
Status	Choose if monitoring for this probe is started or paused. ▪ **Started**: Monitor this probe. ▪ **Paused**: Pause monitoring for this probe. All sensors on all devices on this probe will be paused until this setting is changed again.
Priority	Select a priority for the probe. This setting determines where the probe will be placed in list views. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

LOCATION

Location (for Geo Maps)	When you want to use **Geo Maps** 2824, enter a location in the first line. Geographical maps will display objects (devices, groups) then with a flag, showing the current status using a color code similar to the sensor status icons 163 (green - yellow - orange - red). You can enter a full postal address, city and country only, or latitude and longitude. It is possible to enter any text before, between, and after the coordinates, PRTG will parse latitude and longitude automatically, for example: 49.452778 11.077778 or enter 49.452778 any 11.077778 text A minus sign (-) in the first line will hide an object from geo maps. In this case you can enter location information in line two and following. You can define a specific label for each location: enter a string denoting the label in the first line and provide geo coordinates in the second line. This geo marker will show then the object with the label in the PRTG geo map. The preview map will always hava a road map layout regardless of the map layout you set in **User Interface** 2945.

CREDENTIALS FOR WINDOWS SYSTEMS

Domain or Computer Name	Define the authority for Windows access. This is used for Windows Management Instrumentation (WMI) and other Windows sensors. If you want to use a Windows local user account on the target device, enter the computer name here. If you want to use a Windows domain user account (recommended), enter the (Active Directory) domain name here. If not explicitly defined, PRTG will automatically add a prefix in order to use the NT LAN Manager (NTLM) protocol. Do not leave this field empty.
User	Enter the username for Windows access. Usually, you will use credentials with administrator privileges.

CREDENTIALS FOR WINDOWS SYSTEMS

Password	Enter the password for Windows access. Usually, you will use credentials with administrator privileges.

CREDENTIALS FOR LINUX/SOLARIS/MAC OS (SSH/WBEM) SYSTEMS

User	Enter a login name for the access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
Login	Define the authentication method to use for login. Choose between: ▪ **Login via Password**: Provide a password for login. Enter below. ▪ **Login via Private Key**: Provide a private key for authentication. PRTG can only handle keys in OpenSSH format that are not encrypted. You cannot use password protected keys here. In the text field, paste the entire private key, including the "BEGIN" and "END" lines. Please make sure the according public key is provided on the target machine. For details, please see **Monitoring via SSH** 3095.
Password	This field is only visible if you select password login above. Enter a password for the Linux access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
Private Key	This field is only visible if you select private key login above. Paste a private key into the field (OpenSSH format, unencrypted). Usually, you will use credentials with administrator privileges. If you do not insert a private key for the first time, but change the private key, you need to restart your PRTG core server service 2988 in order for the private key change to take effect! For details, please see **Monitoring via SSH** 3095.
For WBEM Use Protocol	Define the protocol to use for WBEM. This setting is only relevant if you use WBEM sensors. Choose between: ▪ **HTTP**: Use an unencrypted connection for WBEM. ▪ **HTTPS**: Use an SSL-encrypted connection for WBEM.
For WBEM Use Port	Define the port to use for WBEM. This setting is only relevant if you use WBEM sensors. Choose between: ▪ **Set automatically (port 5988 or 5989)**: Use one of the standard ports, depending on whether you choose unencrypted or encrypted connection above.

CREDENTIALS FOR LINUX/SOLARIS/MAC OS (SSH/WBEM) SYSTEMS

- **Set manually**: Use a custom port. Define below.

WBEM Port

This setting is only visible if you enable manual port selection above. Enter the WBEM port number.

SSH Port

Enter the port number to use for SSH connections.

By default, PRTG uses this setting automatically for all SSH sensors 390, unless you define a different port number in the sensor settings.

SSH Rights Elevation

Define the rights that you want to use to execute the command on the target system. Choose between:

- **Run the command as the user connecting (default)**: Use the rights of the user who establishes the SSH connection, as defined above.
- **Run the command as another user using 'sudo' (with password)**: Use the rights of another user with a password required for sudo to run commands on the target device, for example, as root user.
- **Run the command as another user using 'sudo' (without password)**: Use the rights of another user without a password required for sudo to run commands on the target device, for example, as root user.
- **Run the command as another user using 'su'**: Use the rights of another user with su to run commands on the target device.

Target User

This field is only visible if you choose sudo or su above. Enter a username to run the specified command as a user other than root. If you leave this field empty, you will run the command as root. Ensure you set the Linux password even if you use a public or private key for authentication. This is not necessary if the user is allowed to execute the command without a password.

Password Target User

This field is only visible if you choose to run the commands using su or sudo with password above. Enter the password for the specified target user.

SSH Engine

Select the method you want to use to access data with SSH sensors 3095. We strongly recommend that you keep the default engine! For now, you still can use the legacy mode to ensure compatibility with your target systems. Choose between:

- **Default (recommended)**: This is the default monitoring method for SSH sensors. It provides best performance and security.

CREDENTIALS FOR LINUX/SOLARIS/MAC OS (SSH/WBEM) SYSTEMS

- **Compatibility Mode (deprecated)**: Try this legacy method only if the default mode does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions and is deprecated. We will remove this legacy option soon, so please try to get your SSH sensors running with the default SSH engine.

You can also individually select the SSH engine for each SSH sensor in the sensor settings.

CREDENTIALS FOR VMWARE/XENSERVER

User	Enter a login name for access to VMware and Xen servers. Usually, you will use credentials with administrator privileges.
Password	Enter a password for access to VMware and Xen servers. Usually, you will use credentials with administrator privileges. Single Sign-On (SSO) passwords for vSphere do not support special characters. Please see the manual sections for VMware sensors for details.
VMware Protocol	Define the protocol used for the connection to VMware and XenServer. Choose between: ▪ **HTTPS (recommended)**: Use an SSL-encrypted connection to VMware and XenServers. ▪ **HTTP**: Use an unencrypted connection to VMware and XenServers.
Session Pool	Define if you want to use session pooling for VMware sensors. Choose between: ▪ **Reuse session for for multiple scans (recommended)**: Select this option to use session pooling. With session pooling, a VMware sensor uses the same session as created in advance to query data and needs not to log in and out for each sensor scan. We recommend that you choose this option because it reduces network load and log entries on the target device, resulting in better performance. ▪ **Create a new session for each scan**: If you select this option and disable session pooling, a VMware sensor has to log in and out for each sensor scan. We recommend that you use the session pooling option above for better performance.

CREDENTIALS FOR SNMP DEVICES

SNMP Version	Select the SNMP version for the device connection. Choose between: ▪ **v1**: Use the simple v1 protocol for SNMP connections. This protocol only offers clear-text data transmission, but it is usually supported by all devices. ⓘ SNMP v1 does not support 64-bit counters which may result in invalid data when monitoring traffic via SNMP. ▪ **v2c (recommended)**: Use the more advanced v2c protocol for SNMP connections. This is the most common SNMP version. Data is still transferred as clear-text, but it supports 64-bit counters. ▪ **v3**: Use the v3 protocol for SNMP connections. It provides secure authentication and data encryption. ⓘ When using SNMP v3 you can only monitor a limited number of sensors per second due to internal limitations. The limit is somewhere between 1 and 50 sensors per second (depending on the SNMP latency of your network). This means that using an interval of 60 seconds limits you to between 60 and 3000 SNMP v3 sensors for each probe. If you experience an increased Interval Delay or Open Requests with the **Probe Health Sensor** 1378, distribute the load over multiple probes 3196. SNMP v1 and v2 do not have this limitation.
Community String	This setting is only visible if you select SNMP version **v1** or **v2c** above. Enter the community string of your devices. This is a kind of "clear-text password" for simple authentication. We recommend that you use the default value.
Authentication Type	This setting is only visible if you select SNMP version **v3** above. Choose between: ▪ **MD5**: Use Message-Digest Algorithm 5 (MD5) for authentication. ▪ **SHA**: Use Secure Hash Algorithm (SHA) for authentication. The type you choose must match the authentication type of your device. ⓘ If you do not want to use authentication, but you need SNMP v3, for example, because your device requires context, you can leave the field **Password** empty. In this case, SNMP_SEC_LEVEL_NOAUTH is used and authentication deactivated entirely.
User	This setting is only visible if you select SNMP version **v3** above. Enter a username for secure authentication. This value must match the username of your device.

CREDENTIALS FOR SNMP DEVICES

Password	This setting is only visible if you select SNMP version **v3** above. Enter a password for secure authentication. This value must match the password of your device.
Encryption Type	This setting is only visible if you select SNMP version **v3** above. Select an encryption type. Choose between: ▪ **DES**: Use Data Encryption Standard (DES) as encryption algorithm. ▪ **AES**: Use Advanced Encryption Standard (AES) as encryption algorithm. AES 192 and AES 256 are not supported by Net-SNMP because they lack RFC specification. The type that you choose must match the encryption type of your device.
Data Encryption Key	This setting is only visible if you select SNMP version **v3** above. Enter an encryption key here. If you provide a key in this field, SNMP data packets are encrypted using the encryption algorithm selected above, which provides increased security. The key that you enter here must match the encryption key of your device. If the key you enter in this field does not match the key configured on the target SNMP device, you will not get an error message about this! Please enter a string or leave the field empty.
Context Name	This setting is only visible if you select SNMP version **v3** above. Enter a context name only if it is required by the configuration of the device. Context is a collection of management information accessible by an SNMP device. Please enter a string.
SNMP Port	Enter the port for the SNMP communication. We recommend that you use the default value.
SNMP Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than the value you enter here, the request is aborted and an error message triggered.

CREDENTIALS FOR DATABASE MANAGEMENT SYSTEMS

The settings you define in this section apply to the following sensor types:

- ADO SQL v2 Sensor 418
- Microsoft SQL v2 Sensor 1135
- MySQL v2 Sensor 1151
- Oracle SQL v2 Sensor 1253
- PostgreSQL Sensor 1363

Port for Databases	Define which ports PRTG will use for connections to the monitored databases. Choose between: ▪ **Set automatically (default port, recommended)**: PRTG automatically determines the type of the monitored database and uses the corresponding default port to connect. See below for a list of default ports. ▪ **Define one custom port valid for all database sensors**: Choose this option if your database management systems do not use the default ports. Define the port for database connections manually below. If you choose this option, PRTG will use the custom port for all database sensors. If you choose the automatic port selection, PRTG uses the following default ports: ▪ Microsoft SQL: 1433 ▪ MySQL: 3306 ▪ Oracle SQL: 1521 ▪ PostgreSQL: 5432
Custom Database Port	Enter the number of the port that PRTG will use for database connections. Please enter an integer value. All database sensors on this device will use this port to connect.
Authentication Mode	Select the authentication method for the connection to the SQL database. Choose between: ▪ **Windows authentication with impersonation**: If you select this option, PRTG uses the Windows credentials as defined in the particular device settings 365 for the database connection. The user whose credentials are used needs to have permissions to log on to the system on which the PRTG probe with a database sensor runs. This is required for the impersonation.

CREDENTIALS FOR DATABASE MANAGEMENT SYSTEMS

- **SQL server authentication**: Choose this option if you want to use explicit credentials for database connections.

User	This field is only visible if you select SQL server authentication above. Enter the username for the database connection.
Password	This field is only visible if you select SQL server authentication above. Enter the password for the database connection.
Timeout (Sec.)	Enter a timeout in seconds for the request. Please enter an integer value. If the reply takes longer than this value defines, the sensor cancels the request and triggers an error message. The maximum timeout value is 300 seconds (5 minutes).

CREDENTIALS FOR AMAZON CLOUDWATCH

Access Key	Enter your Amazon Web Services (AWS) access key. Please see the corresponding Amazon CloudWatch sensor 391 documentation to learn more about the rights that are required for querying AWS CloudWatch metrics.
Secret Key	Enter your Amazon Web Services (AWS) secret key. Please see the corresponding Amazon CloudWatch sensor 391 documentation to learn more about the rights that are required for querying AWS CloudWatch metrics.

WINDOWS COMPATIBILITY OPTIONS

When experiencing problems while monitoring via Windows sensors, you can set some compatibility options for trouble shooting.

Preferred Data Source	Define the method Windows sensors will use to query data. This setting is valid only for hybrid sensors offering performance counter and Windows Management Instrumentation (WMI) technology. The setting will be ignored for all other sensors! Choose between: ▪ **Performance Counters and fallback to WMI**: Try to query data via performance counters. If this is not possible, establish a connection via WMI.

WINDOWS COMPATIBILITY OPTIONS

- **Performance Counters only**: Query data via performance counters only. If this is not possible, a sensor will return no data.
- **WMI only (recommended)**: Query data via WMI only. If this is not possible, a sensor will return no data. In current PRTG versions, this is our recommendation to achieve best performance and stability.

Timeout Method

Specify the time the sensor will wait for the return of its WMI query before aborting it with an error message. Choose between:

- **Use 1.5x scanning interval (recommended)**: Use a default of one and a half times the scanning interval set for the sensor (see below in this settings).
- **Set manually**: Enter a timeout value manually.

We recommend that you use the default value. Only if you experience ongoing timeout errors, try increasing the timeout value.

Timeout Value (Sec.)

This field is only visible if the manual timeout method is selected above. Specify the time the sensor will wait for the return of its WMI query before aborting with an error message. Please enter an integer value.

SNMP COMPATIBILITY OPTIONS

When experiencing problems while monitoring via Simple Network Management Protocol (SNMP) sensors, you can set some compatibility options for trouble shooting.

SNMP Delay (ms)

Add a time in milliseconds that will be waited between two SNMP requests. This can help increase device compatibility. Please enter an integer value. We recommend that you use the default value. If you experience SNMP connection failures, please increase it. You can define a delay between 0 and 100, higher delays are not supported and will be discarded.

Failed Requests

Define if an SNMP sensor will try again after a request fails.

- **Retry (recommended)**: Try again if an SNMP request fails. This can help prevent false error messages due to temporary timeout failures.
- **Do not retry**: Do not retry if an SNMP request fails. With this setting enabled an SNMP sensor will be set to error status earlier.

SNMP COMPATIBILITY OPTIONS

Overflow Values	Define how PRTG will handle overflow values. Some devices do not handle internal buffer overflows correctly. This can cause false peaks. ▪ **Ignore overflow values**: Ignore overflow values and do not include them in the monitoring data. ▪ **Handle overflow values as valid results**: Regard all overflow values as regular data and include them in the monitoring data. We recommend that you use the default value. If you experience problems because of strange peaks in your data graphs, change this option. Peaks might indicate that the monitored device resets counters without an overflow. PRTG interprets such a behavior as overflow that results in data peaks. Choose the option **Ignore overflow values** in this case. For more details, see this Knowledge Base article: What is the Overflow Values setting in the SNMP Compatibility Options?
Zero Values	Define how PRTG will handle zero values. Some devices send incorrect zero values. This can cause false peaks. ▪ **Ignore zero values for delta sensors (recommended)**: Ignore zero values and do not include them in the monitoring data. ▪ **Handle zero values as valid results for delta sensors**: Regard all zero values as regular data and include them in the monitoring data. We recommend that you use the default value. If you experience problems, change this option.
32-bit/64-bit Counters	Define which kind of traffic counters PRTG will search for on a device. ▪ **Use 64-bit counters if available (recommended)**: The interface scan will use 64-bit traffic counters, if available. This can avoid buffer overflows in the devices. ▪ **Use 32-bit counters only**: The interface scan will always use 32-bit traffic counters, even if 64-bit counters are available. This can lead to more reliable monitoring for some devices. We recommend that you use the default value. If you experience problems, change this option.
Request Mode	Define which kind of request method PRTG uses for SNMP sensors. ▪ **Use multi get (recommended)**: Bundle multiple SNMP requests into one request. ▪ **Use single get**: Use one request for each SNMP value. This can increase compatibility with older devices.

SNMP COMPATIBILITY OPTIONS

We recommend that you use the default value. If you experience problems, change this option.

PRTG uses paging for SNMP requests. This means that if a sensor has to query more than 20 OIDs, it will automatically poll the OIDs in packages of 20 OIDs each per request.

Port Name Template

Define how the name of SNMP sensors created on a device will be put together. Enter a template using several variables. When adding new sensors, PRTG scans the interface for available counters at certain OIDs. At each OID usually several fields are available with interface descriptions. They are different for every device and OID. PRTG will use the information in these fields to name the sensors. If a field is empty or not available, an empty string is added to the name. As default, **([port]) [ifalias]** is set as port name template, which will create a name such as (001) Ethernet1, for example. You can use any field names available at a certain OID of your device, among which are:

- **[port]**: The port number of the monitored interface.
- **[ifalias]**: The 'alias' name for the monitored interface as specified by a network manager, providing a non-volatile handling.
- **[ifname]**: The textual name of the monitored interface as assigned by the local device.
- **[ifdescr]**: A textual string containing information about the monitored device or interface, for example, manufacturer, product name, version.
- **[ifspeed]**: An estimate of the monitored interface's current bandwidth (KBit/s).
- **[ifsensor]**: The type of the sensor, this is SNMP Traffic or SNMP RMON. This is useful to differentiate between your SNMP Traffic 2132 and SNMP RMON 2073 sensors.

Combine them as you like to obtain suitable sensor names.

For more information about SNMP sensor names, see this Knowledge Base article: How can I change the defaults for names automatically generated for new SNMP sensors?

Port Name Update

Define how PRTG will react if you change port names in your physical device (for example, a switch or router). Choose between:

- **Keep port names (use this if you edit the names in PRTG)**: Do not automatically adjust sensor names. This is the best option if you want to change names in PRTG manually.

SNMP COMPATIBILITY OPTIONS

- **Automatic sensor name update if name changes in device**: If PRTG detects changes of port names in your physical device, it will try to automatically adjust sensor names accordingly.

For more information about automatic updates of names, see this Knowledge Base article: Automatically update port name and number for SNMP Traffic sensors when the device changes them

Port Identification

Define which field will be used for SNMP interface identification. Choose between:

- **Automatic (recommended)**: Tries the ifAlias field first to identify an SNMP interface and then ifDescr.
  ifName will not be tried automatically.
- **Use ifAlias**: For most devices ifAlias is the best field to get unique interface names.
- **Use ifDescr**: Use this option if the port order of your device changes after a reboot, and there is no ifAlias field available. For example, this is the best option for Cisco ASA devices.
  When using this option it is important that your device returns unique interface names in the ifDescr field.
- **Use ifName**: You can also use this option if there is no unique ifAlias available.
  When using this option it is important that your device returns unique interface names in the ifName field.
- **No Port Update**: Use this option to disable automatic port identification.

Start Interface Index

For SNMP Traffic sensors, define at which index PRTG will start to query the interface range during sensor creation. Use 0 for automatic mode. We recommend that you use the default value.

End Interface Index

For SNMP Traffic sensors, define at which index PRTG will stop to query the interface range during sensor creation. Use 0 for automatic mode. We recommend that you use the default value.

PROXY SETTINGS FOR HTTP SENSORS

HTTP Proxy Settings	The proxy settings determine how a sensor connects to a given URL. You can enter data for an HTTP proxy server that sensors will use when connecting via HTTP or HTTPS. This setting affects monitoring only and determines the behavior of HTTP sensors. To change proxy settings for the core server, please see **System Administration—Core & Probes** 2967. The **SSL Certificate Sensor** 2289 and the **SSL Security Check Sensor** 2299 do not support HTTP proxies, but you can configure connections via SOCKS proxies in their sensor settings.
Name	Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.
Port	Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.
User	If the proxy requires authentication, enter the username for the proxy login. Only basic authentication is available! Please enter a string or leave the field empty.
Password	If the proxy requires authentication, enter the password for the proxy login. Only basic authentication is available! Please enter a string or leave the field empty.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

SCANNING INTERVAL

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

CLUSTER USAGE

Scanning Distribution

This box is only visible if you run a PRTG cluster. Sometimes you want to exclude a certain node from monitoring the sensors running on this probe, group, or device, for example, if a device is not reachable from every node configured in your cluster. In the list of cluster nodes, please select the nodes that will not be included in sensor scans. By default, this setting is inherited 122 to all objects underneath.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. To terminate a current maintenance window before the defined end date, you can change the time in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current object if its parent object is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current object if its parent object is in a **Down** status, or if it is paused by another dependency. Additionally, pause the current object if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	You do not trigger a status change by dependency if you manually pause a master object or if you pause it by schedule. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 210 to choose an object on which the current object will be dependent on.
Dependency Delay (Sec.)	This field is only visible if you select another object than the parent as dependency type. Define a time span in seconds for dependency delay. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

ADVANCED NETWORK ANALYSIS

Unusual Detection	Define if you want to benefit from unusual detection 2956 for sensors. You can configure the behavior of unusual detection (or disable it completely) in the system settings 2956. Choose between: ▪ **Enabled**: Activate unusual detection for this object and, by default, for all objects underneath in the hierarchy 118 of the device tree. Sensors affected by this setting will turn to orange color (unusual sensor status 163) if PRTG detects unusual activity. ▪ **Disabled**: Do not activate unusual detection. PRTG will ignore unusual values for sensors affected by this setting. These sensor will not show an unusual sensor status.
Similar Sensors Detection	Define if you want to activate **Similar Sensors** 180 analysis. You can configure the depth of analysis of similar sensors detection (or disable it completely) in the system settings 2958. Choose between: ▪ **Enabled**: Activate similar sensors detection for this object and, by default, for all objects underneath in the hierarchy 118 of the device tree. PRTG considers all sensors affected by this setting during similarity analysis. ▪ **Disabled**: Do not activate similar sensors detection. PRTG will not consider sensors affected by this setting during similarity analysis.
System Information	Define if you want to retrieve and show **System Information** 193 for your devices. Choose between: ▪ **Enabled**: Activate the system information feature for this object and, by default, for all objects underneath in the hierarchy 118 of the device tree. ▪ **Disabled**: Do not activate system information. This setting is not available for local probes in PRTG on demand.

PROBE SETTINGS FOR MONITORING

Define the IP address used for outgoing monitoring requests.

- If there is more than one IP on the current system available, you can specify the IP address that PRTG will use for outgoing monitoring requests of certain sensor types.

PROBE SETTINGS FOR MONITORING

- This setting will be used for sensors using the following connection types: HTTP, DNS, FTP, IMAP, POP3, Port, Remote Desktop, SMTP, and SNMP.
- The setting is valid for all monitoring requests sent from this PRTG probe.
- This setting is useful for devices that expect a certain IP address when queried.
- Default setting is **auto**. PRTG will select an IP address automatically.

This feature does not support all sensor types for technical reasons.

If you change this setting, some sensors might stop working. For example, sensors might show a **Down** status if the selected IP address is blocked on the way to or directly on the monitored device.

Outgoing IPv4	Define the IP address for outgoing requests using the IPv4 protocol. The list shows all IP addresses available on the current system. Choose a specific IP address or select **auto**.
Outgoing IPv6	Define the IP address for outgoing requests using the IPv6 protocol. The list shows all IP addresses available on the current system. Choose a specific IP address or select **auto**. For details about the basic concept of IPv6 in PRTG, please see the **IPv6** 133 section.

Cluster Connectivity	This box is only visible if you run a PRTG cluster. Define if this probe connects to all cluster nodes, including the failover nodes, or only to the primary master node. Choose between: ▪ **Probe sends data only to primary master node**: The probe connects only to the primary master node. You are not able to review monitoring data on failover nodes. Consider to choose this option if you have bandwidth limitations in your network or if the probe cannot access your failover node(s). ▪ **Probe sends data to all cluster nodes**: This is the default option. The probe connects to all nodes in your cluster and sends monitoring data to the failover node(s) in addition to the primary master. The probe is visible on all your nodes as soon as it connects automatically to the correct IP addresses and ports of the failover nodes. If your master node fails, you can still see monitoring data of this probe. PRTG will not notify you if a remote probe is disconnected from a cluster node. Please check explicitly on a cluster node if your remote probes are connected (for example, via the device tree in the PRTG web interface on a cluster node).

SCHEDULED RESTART SETTINGS

This setting is not available for local probes in PRTG on demand.

Restart Options	For best performance, we recommend that you regularly restart the Windows servers on which PRTG is running. To do this automatically for PRTG, you can schedule an automatic restart. Choose between the following options: ▪ **No scheduled reboot or service restart**: Do not perform any scheduled restart of services automatically. We recommend a manual restart every few weeks. You can initiate a restart of your PRTG core server and probes under **System Administration—Administrative Tools** 2987 in the PRTG web interface. ▪ **Scheduled restart of PRTG services**: Restart all PRTG services on the system where this probe runs on. If you choose this option on the local probe, the PRTG core server will restart as well. Define a schedule below. ▪ **Scheduled system reboot (recommended)**: We recommend this setting, although it is not set by default. Enter a schedule below. We recommend that you restart Windows servers once a month for best performance.
Restart Schedule	You can only see this setting if you selected a schedule option above. Choose how often you want to restart PRTG services or the Windows server: ▪ **Once per week**: Select a day of the week and a time below. ▪ **Once per month (recommended)**: Select a day of the month and a time below.
Specify Day	You can only see this setting if you selected a schedule option above. Select a specific day of a week (Monday to Sunday) or month (1st to 30th or Last). If you select **Last**, the restart will always be executed on the last day of the month, regardless of how many days the month has. If you select a date that does not exist in every month (for example, the 30th day in February), PRTG will automatically initiate the restart on the last day of this month.
Specify Hour	You can only see this setting if you selected a schedule option above. Select the time of day when PRTG will perform the restart. You will get a Windows warning message 10 minutes before the restart to inform you if you are a currently logged in user. The actual restart time can differ up to 30 minutes from the settings you enter here.

Click **Save** to save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Notifications

The status or the data of a sensor can trigger notifications. Using this mechanism, you can configure external alerting tailored to your needs. In an object's detail page, click the **Notifications** tab to change sensor notification triggers. The defined triggers will be inherited down to sensor level. For detailed information, please see **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see **Object Settings** 188 section.

More

Knowledge Base: How does PRTG compute CPU Index, Traffic Index and Response Time Index?

- https://kb.paessler.com/en/topic/313

Knowledge Base: How can I add my own device icons for use in the PRTG web interface?

- https://kb.paessler.com/en/topic/7313

Knowledge Base: How can I change the defaults for names automatically generated for new SNMP sensors?

- https://kb.paessler.com/en/topic/7363

Knowledge Base: Automatically update port name and number for SNMP Traffic sensors when the device changes them

- https://kb.paessler.com/en/topic/25893

Knowledge Base: What is the Overflow Values setting in the SNMP Compatibility Options?

- https://kb.paessler.com/en/topic/43503

7.6 Group Settings

On a group's overview page, click the **Settings** tab to change settings.

Add Group

The **Add Group** dialog appears when adding a new group to a parent group. It only shows the setting fields that are imperative for creating the group. Therefore, you will not see all setting fields in this dialog. For example, the **Group Status** option is not available in this step.

You can change all settings in the group's **Settings** tab later.

Group Settings

The following settings are available in the **Settings** tab of every group. As you may not need all of these for every group, just regard the settings you really need, ignoring the others.

ⓘ This documentation does not refer to the setting of the special **Root** group. The settings available there differ from those described here.

We recommend that you define as many settings as possible in the **Root** 294 group, so you can inherit them to all other objects further down in the device tree hierarchy 118.

ⓘ This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

BASIC GROUP SETTINGS

Group Name	Enter a meaningful name to identify the group. The name will be shown by default in the devices tree and in all alarms.
Status	Choose if monitoring for this group is started or paused. .We recommend that you use the default value. You can add additional tags to it, if you like. ▪ **Started**: Monitor this group. ▪ **Paused**: Pause monitoring for this group. All sensors on all devices in this group will be paused until this setting is changed again.
Parent Tags	Shows **Tags** 124 that this group inherits 124 from its parent probe 118. This setting is shown for your information only and cannot be changed here.

BASIC GROUP SETTINGS

Tags	Enter one or more **Tags**. Confirm each tag by hitting the space, comma, or enter key. You can use tags to group objects and use tag-filtered views later on. Tags are not case sensitive.
Priority	Select a priority for the group. This setting determines where the group will be placed in list views. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

GROUP TYPE

Sensor Management	Select which type of auto-discovery you would like to perform for this group. Choose between: ▪ **Manual (no auto-discovery)**: Do not auto-discover any sensors, only add sensors manually. ▪ **Automatic device identification (standard, recommended)**: Use a small set of auto-discovery templates. This will scan your LAN and usually create a set of standard sensors on your device. ▪ **Automatic device identification (detailed, may create many sensors**: Use an extended set of auto-discovery templates. This will scan your LAN and usually create many sensors on your device. ▪ **Automatic sensor creation using specific device templates**: Use specific auto-discovery templates only. Please select templates below. This will scan your LAN and add sensors defined in the template.
Device Template(s)	This option is only visible if you enable using specific device templates above. Choose one or more templates by adding a check mark in front of the respective template name. You can also select and deselect all items by using the check box in the table head. PRTG will use the selected templates for auto-discovery on the current device. Choose from: ▪ **ADSL** ▪ **Amazon Cloudwatch** ▪ **Buffalo TeraStation NAS** ▪ **Cisco ASA VPN** ▪ **Cisco Device (Generic)**

- Dell EqualLogic
- Dell MDI Disk
- DNS Server
- Environment Jacarta
- Environment Poseidon
- FTP Server
- Generic Device (PING only)
- Generic Device (SNMP-enabled)
- Generic Device (SNMP-enabled, Detailed)
- HTTP Web Server
- Hyper V Host Server
- IPMI enabled devices
- Juniper NS Device
- Linux/UNIX Device (SNMP or SSH enabled)
- Mail Server (Generic)
- Mail Server (MS Exchange)
- Microsoft Sharepoint 2010
- NAS LenovoEMC
- NAS QNAP
- NAS Synology
- NetApp
- NTP Server
- Printer (HP)
- Printer Generic
- RDP Server
- RMON compatible device
- Server (Compaq/HP agents)
- Server (Dell)
- Sever Cisco UCS
- Server IBM
- SonicWALL
- SSL Security Check
- Switch (Cisco Catalyst)

	▪ **Switch (Cisco IOS Based)** ▪ **Switch (HP Procurve)** ▪ **UNIX/Linux Device** ▪ **UPS Health (APC)** ▪ **UPS Health (Generic)** ▪ **UPS Health (Leibert)** ▪ **VMware ESX / vCenter Server** ▪ **Webserver** ▪ **Windows (Detailed via WMI)** ▪ **Windows (via Remote Powershell)** ▪ **Windows (via WMI)** ▪ **Windows IIS (via SNMP)** ▪ **XEN Hosts** ▪ **XEN Virtual Machines** Once the auto-discovery is finished, PRTG will create a new ticket [200] and list the device templates that it used to create new sensors. The ticket will not show templates that were not applied.
Discovery Schedule	Define when PRTG will run the auto-discovery. Choose between: ▪ **Once**: Perform auto-discovery only once. PRTG will add new devices and sensors once. If you select this option, you have to start the auto-discovery manually [250], it will not run automatically. ▪ **Hourly**: Perform auto-discovery for new devices and sensors every 60 minutes. Please use this option with caution! Frequently executed auto-discoveries might cause performance issues, especially when large network segments are scanned every hour. ▪ **Daily**: Perform auto-discovery for new devices and sensors every 24 hours. The first auto-discovery will run immediately, all other discoveries will start at the time defined in the **Auto-Discovery Settings** section of the System Administration—Monitoring [2959] settings. ▪ **Weekly**: Perform auto-discovery for new devices and sensors every 7 days. The first auto-discovery will run immediately, all other discoveries will start at the time defined in the **Auto-Discovery Settings** section of the System Administration—Monitoring [2959] settings.
IP Selection Method	Define how you want to define the IP range for auto-discovery. Choose between:

	▪ **Class C base IP with start/end (IPv4)**: Define an IPv4 class C address range. ▪ **List of individual IPs and DNS names (IPv4)**: Enter a list of individual IPv4 addresses or DNS names. ▪ **IP and subnet (IPv4)**: Enter an IPv4 address and subnet mask. ▪ **IP with octet range (IPv4)**: Enter an IPv4 address range for every IP octet individually. With this, you can define very customizable IP ranges. ▪ **List of individual IPs and DNS names (IPv6)**: Enter a list of individual IPv6 addresses or DNS names. ▪ **Use computers from the active directory (maximum 1000 computers)**: Search in the active directory for computers to perform auto-discovery. Define your active directory domain in advance in the system administration. See **System Administration—Core & Probes** 2971. Only subnets with up to 65,536 IP addresses can be discovered! If you define a range with a higher number of addresses, discovery will stop before it is completed.
IPv4 Base	This field is only visible if you select Class C network detection above. Enter a class C network as IP base for the auto-discovery. Enter the first three octets of an IPv4 IP address, for example, **192.168.0**
IPv4 Range Start	This field is only visible if you select Class C network detection above. Enter the IP octet of the class C network specified above from which PRTG will start the auto-discovery. This will complete the IP base above to an IPv4 address. For example, enter **1** to discover from **192.168.0.1**.
IPv4 Range End	This field is only visible if you select Class C network detection above. Enter the IP octet of the class C network specified above at which PRTG will stop the auto-discovery. This will complete the IP base above to an IPv4 address. For example, enter **254** to discover up to **192.168.0.254**.
IPv4/DNS Name List IPv6/DNS Name List	This field is only visible if you select the IP list option above. Enter a list of IP addresses or DNS names which the auto-discovery will scan. Enter each address in a separate line.
IPv4 and Subnet (IPv4)	This field is only visible if you select the IP and subnet option above. Enter an expression in the format **address/subnet**, for example, 192.168.3.0/255.255.255.0. You can also use the short form like 192.168.3.0/24 in this example. PRTG will scan the complete host range (without network and broadcast address) defined by the IP address and the subnet mask.

IP with Octet Range	This field is only visible if you select the octet range option above. Enter an expression in the format **a1.a2.a3.a4**, where a1, a2, a3, and a4 are each a number between 0-255, or a range with two numbers and a hyphen like 1-127. All permutations of all ranges are calculated. For example, 10.0.1-10.1-100 results in 1,000 addresses that PRTG will scan during auto-discovery.
Organizational Unit	This field is only visible if you select active directory above. Enter an organizational unit (OU) to restrict the active directory search to computers that are part of this OU. Just enter the name of the OU without any other term (so without "OU" in front). If you leave this field empty, there will not be any restriction. Make sure that the OU contains a host. If the OU is empty, you will receive an error message. If you have sub-OUs, consider the correct syntax in the format **Y,OU=X**: OUs that are part of another OU have to be listed together with their parent(s). Enter the sub-OU followed by ,OU= and the name of the parent OU. Examples: ▪ Assuming that the organizational unit 'Y' is part of the OU named 'X'. Then the syntax would be Y,OU=X ▪ For three OUs 'X', 'Y' part of 'X', and 'Z' part of 'Y', the syntax would be Z,OU=Y,OU=X The order is important, sub-OUs have to be listed left of their particular parents!
Name Resolution	Define how to monitor newly discovered devices. This affects only new devices. The setting for existing devices will remain unchanged. Depending on your selection the **IP Address/DNS Name** field of an added device shows the DNS name or IP address which PRTG uses to access the target device. Choose between: ▪ **Use DNS names (recommended)**: Monitor newly discovered devices via their DNS names (if available). ▪ **Use IP addresses**: Monitor newly discovered devices via their IP address. We recommend that you use the default value. This setting does not affect how PRTG shows the devices in the device tree.
Device Rescan	Define if you want to add devices that already exist in your PRTG installation also to the currently selected group. Choose between:

- **Skip auto-discovery for known devices/IPs (recommended)**: Do not re-scan known devices or IP addresses, only add devices with new IPs or DNS names when auto-discovering. PRTG will not add devices that are already included elsewhere in your configuration, for example, in other groups.
- **Perform auto-discovery for known devices/IPs**: Re-scan devices with known IP addresses with every auto-discovery. This option will add devices that already exist in other groups also to this group and runs the auto-discovery on the newly added devices.
  The auto-discovery will not run on devices that already exist in this group. If you want to run the auto-discovery for an existing device, you have to start the auto-discovery on this device.

We recommend that you use the default value.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

LOCATION

Location (for Geo Maps)

When you want to use **Geo Maps** 2824, enter a location in the first line. Geographical maps will display objects (devices, groups) then with a flag, showing the current status using a color code similar to the sensor status icons 163 (green - yellow - orange - red). You can enter a full postal address, city and country only, or latitude and longitude. It is possible to enter any text before, between, and after the coordinates, PRTG will parse latitude and longitude automatically, for example: 49.452778 11.077778 or enter 49.452778 any 11.077778 text

A minus sign (-) in the first line will hide an object from geo maps. In this case you can enter location information in line two and following.

You can define a specific label for each location: enter a string denoting the label in the first line and provide geo coordinates in the second line. This geo marker will show then the object with the label in the PRTG geo map.

The preview map will always hava a road map layout regardless of the map layout you set in **User Interface** 2945.

CREDENTIALS FOR WINDOWS SYSTEMS

Domain or Computer Name	Define the authority for Windows access. This is used for Windows Management Instrumentation (WMI) and other Windows sensors. If you want to use a Windows local user account on the target device, enter the computer name here. If you want to use a Windows domain user account (recommended), enter the (Active Directory) domain name here. If not explicitly defined, PRTG will automatically add a prefix in order to use the NT LAN Manager (NTLM) protocol. Do not leave this field empty.
User	Enter the username for Windows access. Usually, you will use credentials with administrator privileges.
Password	Enter the password for Windows access. Usually, you will use credentials with administrator privileges.

CREDENTIALS FOR LINUX/SOLARIS/MAC OS (SSH/WBEM) SYSTEMS

User	Enter a login name for the access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
Login	Define the authentication method to use for login. Choose between: ▪ **Login via Password**: Provide a password for login. Enter below. ▪ **Login via Private Key**: Provide a private key for authentication. PRTG can only handle keys in OpenSSH format that are not encrypted. You cannot use password protected keys here. In the text field, paste the entire private key, including the "BEGIN" and "END" lines. Please make sure the according public key is provided on the target machine. For details, please see Monitoring via SSH 3095.
Password	This field is only visible if you select password login above. Enter a password for the Linux access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
Private Key	This field is only visible if you select private key login above. Paste a private key into the field (OpenSSH format, unencrypted). Usually, you will use credentials with administrator privileges. If you do not insert a private key for the first time, but change the private key, you need to restart your PRTG core server service 2988 in order for the private key change to take effect! For details, please see Monitoring via SSH 3095.

CREDENTIALS FOR LINUX/SOLARIS/MAC OS (SSH/WBEM) SYSTEMS

For WBEM Use Protocol	Define the protocol to use for WBEM. This setting is only relevant if you use WBEM sensors. Choose between: ▪ **HTTP**: Use an unencrypted connection for WBEM. ▪ **HTTPS**: Use an SSL-encrypted connection for WBEM.
For WBEM Use Port	Define the port to use for WBEM. This setting is only relevant if you use WBEM sensors. Choose between: ▪ **Set automatically (port 5988 or 5989)**: Use one of the standard ports, depending on whether you choose unencrypted or encrypted connection above. ▪ **Set manually**: Use a custom port. Define below.
WBEM Port	This setting is only visible if you enable manual port selection above. Enter the WBEM port number.
SSH Port	Enter the port number to use for SSH connections. By default, PRTG uses this setting automatically for all SSH sensors 390, unless you define a different port number in the sensor settings.
SSH Rights Elevation	Define the rights that you want to use to execute the command on the target system. Choose between: ▪ **Run the command as the user connecting (default)**: Use the rights of the user who establishes the SSH connection, as defined above. ▪ **Run the command as another user using 'sudo' (with password)**: Use the rights of another user with a password required for sudo to run commands on the target device, for example, as root user. ▪ **Run the command as another user using 'sudo' (without password)**: Use the rights of another user without a password required for sudo to run commands on the target device, for example, as root user. ▪ **Run the command as another user using 'su'**: Use the rights of another user with su to run commands on the target device.
Target User	This field is only visible if you choose sudo or su above. Enter a username to run the specified command as a user other than root. If you leave this field empty, you will run the command as root. Ensure you set the Linux password even if you use a public or private key for authentication. This is not necessary if the user is allowed to execute the command without a password.

CREDENTIALS FOR LINUX/SOLARIS/MAC OS (SSH/WBEM) SYSTEMS

Password Target User	This field is only visible if you choose to run the commands using su or sudo with password above. Enter the password for the specified target user.
SSH Engine	Select the method you want to use to access data with SSH sensors 3095. We strongly recommend that you keep the default engine! For now, you still can use the legacy mode to ensure compatibility with your target systems. Choose between: ▪ **Default (recommended)**: This is the default monitoring method for SSH sensors. It provides best performance and security. ▪ **Compatibility Mode (deprecated)**: Try this legacy method only if the default mode does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions and is deprecated. We will remove this legacy option soon, so please try to get your SSH sensors running with the default SSH engine. ⓘ You can also individually select the SSH engine for each SSH sensor in the sensor settings.

CREDENTIALS FOR VMWARE/XENSERVER

User	Enter a login name for access to VMware and Xen servers. Usually, you will use credentials with administrator privileges.
Password	Enter a password for access to VMware and Xen servers. Usually, you will use credentials with administrator privileges. ⓘ Single Sign-On (SSO) passwords for vSphere do not support special characters. Please see the manual sections for VMware sensors for details.
VMware Protocol	Define the protocol used for the connection to VMware and XenServer. Choose between: ▪ **HTTPS (recommended)**: Use an SSL-encrypted connection to VMware and XenServers. ▪ **HTTP**: Use an unencrypted connection to VMware and XenServers.
Session Pool	Define if you want to use session pooling for VMware sensors. Choose between:

CREDENTIALS FOR VMWARE/XENSERVER

- **Reuse session for for multiple scans (recommended)**: Select this option to use session pooling. With session pooling, a VMware sensor uses the same session as created in advance to query data and needs not to log in and out for each sensor scan. We recommend that you choose this option because it reduces network load and log entries on the target device, resulting in better performance.
- **Create a new session for each scan**: If you select this option and disable session pooling, a VMware sensor has to log in and out for each sensor scan. We recommend that you use the session pooling option above for better performance.

CREDENTIALS FOR SNMP DEVICES

SNMP Version

Select the SNMP version for the device connection. Choose between:

- **v1**: Use the simple v1 protocol for SNMP connections. This protocol only offers clear-text data transmission, but it is usually supported by all devices.
  SNMP v1 does not support 64-bit counters which may result in invalid data when monitoring traffic via SNMP.
- **v2c (recommended)**: Use the more advanced v2c protocol for SNMP connections. This is the most common SNMP version. Data is still transferred as clear-text, but it supports 64-bit counters.
- **v3**: Use the v3 protocol for SNMP connections. It provides secure authentication and data encryption.

When using SNMP v3 you can only monitor a limited number of sensors per second due to internal limitations. The limit is somewhere between 1 and 50 sensors per second (depending on the SNMP latency of your network). This means that using an interval of 60 seconds limits you to between 60 and 3000 SNMP v3 sensors for each probe. If you experience an increased Interval Delay or Open Requests with the **Probe Health Sensor** 1378, distribute the load over multiple probes 3196. SNMP v1 and v2 do not have this limitation.

Community String

This setting is only visible if you select SNMP version **v1** or **v2c** above. Enter the community string of your devices. This is a kind of "clear-text password" for simple authentication. We recommend that you use the default value.

CREDENTIALS FOR SNMP DEVICES

Authentication Type	This setting is only visible if you select SNMP version **v3** above. Choose between: ▪ **MD5**: Use Message-Digest Algorithm 5 (MD5) for authentication. ▪ **SHA**: Use Secure Hash Algorithm (SHA) for authentication. The type you choose must match the authentication type of your device. ⓘ If you do not want to use authentication, but you need SNMP v3, for example, because your device requires context, you can leave the field **Password** empty. In this case, SNMP_SEC_LEVEL_NOAUTH is used and authentication deactivated entirely.
User	This setting is only visible if you select SNMP version **v3** above. Enter a username for secure authentication. This value must match the username of your device.
Password	This setting is only visible if you select SNMP version **v3** above. Enter a password for secure authentication. This value must match the password of your device.
Encryption Type	This setting is only visible if you select SNMP version **v3** above. Select an encryption type. Choose between: ▪ **DES**: Use Data Encryption Standard (DES) as encryption algorithm. ▪ **AES**: Use Advanced Encryption Standard (AES) as encryption algorithm. ⓘ AES 192 and AES 256 are not supported by Net-SNMP because they lack RFC specification. ⓘ The type that you choose must match the encryption type of your device.
Data Encryption Key	This setting is only visible if you select SNMP version **v3** above. Enter an encryption key here. If you provide a key in this field, SNMP data packets are encrypted using the encryption algorithm selected above, which provides increased security. The key that you enter here must match the encryption key of your device. ⓘ If the key you enter in this field does not match the key configured on the target SNMP device, you will not get an error message about this! Please enter a string or leave the field empty.

CREDENTIALS FOR SNMP DEVICES

Context Name	This setting is only visible if you select SNMP version **v3** above. Enter a context name only if it is required by the configuration of the device. Context is a collection of management information accessible by an SNMP device. Please enter a string.
SNMP Port	Enter the port for the SNMP communication. We recommend that you use the default value.
SNMP Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than the value you enter here, the request is aborted and an error message triggered.

CREDENTIALS FOR DATABASE MANAGEMENT SYSTEMS

The settings you define in this section apply to the following sensor types:

- **ADO SQL v2 Sensor** 418
- **Microsoft SQL v2 Sensor** 1135
- **MySQL v2 Sensor** 1151
- **Oracle SQL v2 Sensor** 1253
- **PostgreSQL Sensor** 1363

Port for Databases

Define which ports PRTG will use for connections to the monitored databases. Choose between:

- **Set automatically (default port, recommended)**: PRTG automatically determines the type of the monitored database and uses the corresponding default port to connect. See below for a list of default ports.
- **Define one custom port valid for all database sensors**: Choose this option if your database management systems do not use the default ports. Define the port for database connections manually below. If you choose this option, PRTG will use the custom port for all database sensors.

If you choose the automatic port selection, PRTG uses the following default ports:

- Microsoft SQL: 1433
- MySQL: 3306
- Oracle SQL: 1521

CREDENTIALS FOR DATABASE MANAGEMENT SYSTEMS

	▪ PostgreSQL: 5432
Custom Database Port	Enter the number of the port that PRTG will use for database connections. Please enter an integer value. All database sensors on this device will use this port to connect.
Authentication Mode	Select the authentication method for the connection to the SQL database. Choose between: ▪ **Windows authentication with impersonation**: If you select this option, PRTG uses the Windows credentials as defined in the particular device settings [365] for the database connection. The user whose credentials are used needs to have permissions to log on to the system on which the PRTG probe with a database sensor runs. This is required for the impersonation. ▪ **SQL server authentication**: Choose this option if you want to use explicit credentials for database connections.
User	This field is only visible if you select SQL server authentication above. Enter the username for the database connection.
Password	This field is only visible if you select SQL server authentication above. Enter the password for the database connection.
Timeout (Sec.)	Enter a timeout in seconds for the request. Please enter an integer value. If the reply takes longer than this value defines, the sensor cancels the request and triggers an error message. The maximum timeout value is 300 seconds (5 minutes).

CREDENTIALS FOR AMAZON CLOUDWATCH

Access Key	Enter your Amazon Web Services (AWS) access key. Please see the corresponding Amazon CloudWatch sensor [391] documentation to learn more about the rights that are required for querying AWS CloudWatch metrics.
Secret Key	Enter your Amazon Web Services (AWS) secret key. Please see the corresponding Amazon CloudWatch sensor [391] documentation to learn more about the rights that are required for querying AWS CloudWatch metrics.

WINDOWS COMPATIBILITY OPTIONS

When experiencing problems while monitoring via Windows sensors, you can set some compatibility options for trouble shooting.

Preferred Data Source	Define the method Windows sensors will use to query data. This setting is valid only for hybrid sensors offering performance counter and Windows Management Instrumentation (WMI) technology. The setting will be ignored for all other sensors! Choose between: ▪ **Performance Counters and fallback to WMI**: Try to query data via performance counters. If this is not possible, establish a connection via WMI. ▪ **Performance Counters only**: Query data via performance counters only. If this is not possible, a sensor will return no data. ▪ **WMI only (recommended)**: Query data via WMI only. If this is not possible, a sensor will return no data. In current PRTG versions, this is our recommendation to achieve best performance and stability.
Timeout Method	Specify the time the sensor will wait for the return of its WMI query before aborting it with an error message. Choose between: ▪ **Use 1.5x scanning interval (recommended)**: Use a default of one and a half times the scanning interval set for the sensor (see below in this settings). ▪ **Set manually**: Enter a timeout value manually. We recommend that you use the default value. Only if you experience ongoing timeout errors, try increasing the timeout value.
Timeout Value (Sec.)	This field is only visible if the manual timeout method is selected above. Specify the time the sensor will wait for the return of its WMI query before aborting with an error message. Please enter an integer value.

SNMP COMPATIBILITY OPTIONS

When experiencing problems while monitoring via Simple Network Management Protocol (SNMP) sensors, you can set some compatibility options for trouble shooting.

SNMP COMPATIBILITY OPTIONS

SNMP Delay (ms)	Add a time in milliseconds that will be waited between two SNMP requests. This can help increase device compatibility. Please enter an integer value. We recommend that you use the default value. If you experience SNMP connection failures, please increase it. You can define a delay between 0 and 100, higher delays are not supported and will be discarded.
Failed Requests	Define if an SNMP sensor will try again after a request fails. ▪ **Retry (recommended)**: Try again if an SNMP request fails. This can help prevent false error messages due to temporary timeout failures. ▪ **Do not retry**: Do not retry if an SNMP request fails. With this setting enabled an SNMP sensor will be set to error status earlier.
Overflow Values	Define how PRTG will handle overflow values. Some devices do not handle internal buffer overflows correctly. This can cause false peaks. ▪ **Ignore overflow values**: Ignore overflow values and do not include them in the monitoring data. ▪ **Handle overflow values as valid results**: Regard all overflow values as regular data and include them in the monitoring data. We recommend that you use the default value. If you experience problems because of strange peaks in your data graphs, change this option. Peaks might indicate that the monitored device resets counters without an overflow. PRTG interprets such a behavior as overflow that results in data peaks. Choose the option **Ignore overflow values** in this case. For more details, see this Knowledge Base article: What is the Overflow Values setting in the SNMP Compatibility Options?
Zero Values	Define how PRTG will handle zero values. Some devices send incorrect zero values. This can cause false peaks. ▪ **Ignore zero values for delta sensors (recommended)**: Ignore zero values and do not include them in the monitoring data. ▪ **Handle zero values as valid results for delta sensors**: Regard all zero values as regular data and include them in the monitoring data. We recommend that you use the default value. If you experience problems, change this option.
32-bit/64-bit Counters	Define which kind of traffic counters PRTG will search for on a device.

SNMP COMPATIBILITY OPTIONS

- **Use 64-bit counters if available (recommended)**: The interface scan will use 64-bit traffic counters, if available. This can avoid buffer overflows in the devices.
- **Use 32-bit counters only**: The interface scan will always use 32-bit traffic counters, even if 64-bit counters are available. This can lead to more reliable monitoring for some devices.

We recommend that you use the default value. If you experience problems, change this option.

Request Mode

Define which kind of request method PRTG uses for SNMP sensors.

- **Use multi get (recommended)**: Bundle multiple SNMP requests into one request.
- **Use single get**: Use one request for each SNMP value. This can increase compatibility with older devices.

We recommend that you use the default value. If you experience problems, change this option.

PRTG uses paging for SNMP requests. This means that if a sensor has to query more than 20 OIDs, it will automatically poll the OIDs in packages of 20 OIDs each per request.

Port Name Template

Define how the name of SNMP sensors created on a device will be put together. Enter a template using several variables. When adding new sensors, PRTG scans the interface for available counters at certain OIDs. At each OID usually several fields are available with interface descriptions. They are different for every device and OID. PRTG will use the information in these fields to name the sensors. If a field is empty or not available, an empty string is added to the name. As default, **([port]) [ifalias]** is set as port name template, which will create a name such as (001) Ethernet1, for example. You can use any field names available at a certain OID of your device, among which are:

- **[port]**: The port number of the monitored interface.
- **[ifalias]**: The 'alias' name for the monitored interface as specified by a network manager, providing a non-volatile handling.
- **[ifname]**: The textual name of the monitored interface as assigned by the local device.
- **[ifdescr]**: A textual string containing information about the monitored device or interface, for example, manufacturer, product name, version.
- **[ifspeed]**: An estimate of the monitored interface's current bandwidth (KBit/s).

SNMP COMPATIBILITY OPTIONS

- **[ifsensor]**: The type of the sensor, this is SNMP Traffic or SNMP RMON. This is useful to differentiate between your SNMP Traffic 2132 and SNMP RMON 2073 sensors.

Combine them as you like to obtain suitable sensor names.

For more information about SNMP sensor names, see this Knowledge Base article: How can I change the defaults for names automatically generated for new SNMP sensors?

Port Name Update

Define how PRTG will react if you change port names in your physical device (for example, a switch or router). Choose between:

- **Keep port names (use this if you edit the names in PRTG)**: Do not automatically adjust sensor names. This is the best option if you want to change names in PRTG manually.
- **Automatic sensor name update if name changes in device**: If PRTG detects changes of port names in your physical device, it will try to automatically adjust sensor names accordingly.

For more information about automatic updates of names, see this Knowledge Base article: Automatically update port name and number for SNMP Traffic sensors when the device changes them

Port Identification

Define which field will be used for SNMP interface identification. Choose between:

- **Automatic (recommended)**: Tries the ifAlias field first to identify an SNMP interface and then ifDescr.
  ifName will not be tried automatically.
- **Use ifAlias**: For most devices ifAlias is the best field to get unique interface names.
- **Use ifDescr**: Use this option if the port order of your device changes after a reboot, and there is no ifAlias field available. For example, this is the best option for Cisco ASA devices.
  When using this option it is important that your device returns unique interface names in the ifDescr field.
- **Use ifName**: You can also use this option if there is no unique ifAlias available.
  When using this option it is important that your device returns unique interface names in the ifName field.
- **No Port Update**: Use this option to disable automatic port identification.

SNMP COMPATIBILITY OPTIONS

Start Interface Index	For SNMP Traffic sensors 2132, define at which index PRTG will start to query the interface range during sensor creation. Use 0 for automatic mode. We recommend that you use the default value.
End Interface Index	For SNMP Traffic sensors 2132, define at which index PRTG will stop to query the interface range during sensor creation. Use 0 for automatic mode. We recommend that you use the default value.

PROXY SETTINGS FOR HTTP SENSORS

HTTP Proxy Settings	The proxy settings determine how a sensor connects to a given URL. You can enter data for an HTTP proxy server that sensors will use when connecting via HTTP or HTTPS. This setting affects monitoring only and determines the behavior of HTTP sensors. To change proxy settings for the core server, please see **System Administration—Core & Probes** 2967. The **SSL Certificate Sensor** 2289 and the **SSL Security Check Sensor** 2299 do not support HTTP proxies, but you can configure connections via SOCKS proxies in their sensor settings.
Name	Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.
Port	Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.
User	If the proxy requires authentication, enter the username for the proxy login. Only basic authentication is available! Please enter a string or leave the field empty.
Password	If the proxy requires authentication, enter the password for the proxy login. Only basic authentication is available! Please enter a string or leave the field empty.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply. If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply. If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

CLUSTER USAGE

Scanning Distribution	This box is only visible if you run a PRTG cluster. Sometimes you want to exclude a certain node from monitoring the sensors running on this probe, group, or device, for example, if a device is not reachable from every node configured in your cluster. In the list of cluster nodes, please select the nodes that will not be included in sensor scans. By default, this setting is inherited [122] to all objects underneath.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings [2916]. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. To terminate a current maintenance window before the defined end date, you can change the time in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current object if its parent object is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current object if its parent object is in a **Down** status, or if it is paused by another dependency. Additionally, pause the current object if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. You do not trigger a status change by dependency if you manually pause a master object or if you pause it by schedule. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies [2822] in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector [210] to choose an object on which the current object will be dependent on.
Dependency Delay (Sec.)	This field is only visible if you select another object than the parent as dependency type. Define a time span in seconds for dependency delay. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

ADVANCED NETWORK ANALYSIS

Unusual Detection	Define if you want to benefit from unusual detection 2956 for sensors. You can configure the behavior of unusual detection (or disable it completely) in the system settings 2956. Choose between: ▪ **Enabled**: Activate unusual detection for this object and, by default, for all objects underneath in the hierarchy 118 of the device tree. Sensors affected by this setting will turn to orange color (unusual sensor status 163) if PRTG detects unusual activity. ▪ **Disabled**: Do not activate unusual detection. PRTG will ignore unusual values for sensors affected by this setting. These sensor will not show an unusual sensor status.
Similar Sensors Detection	Define if you want to activate **Similar Sensors** 180 analysis. You can configure the depth of analysis of similar sensors detection (or disable it completely) in the system settings 2958. Choose between: ▪ **Enabled**: Activate similar sensors detection for this object and, by default, for all objects underneath in the hierarchy 118 of the device tree. PRTG considers all sensors affected by this setting during similarity analysis. ▪ **Disabled**: Do not activate similar sensors detection. PRTG will not consider sensors affected by this setting during similarity analysis.
System Information	Define if you want to retrieve and show **System Information** 193 for your devices. Choose between: ▪ **Enabled**: Activate the system information feature for this object and, by default, for all objects underneath in the hierarchy 118 of the device tree. ▪ **Disabled**: Do not activate system information. This setting is not available for local probes in PRTG on demand.

NUMBER OF SENSORS LIMITATION

Sensor Limit	This setting allows the administrator to set a limit for the maximum number of sensors in this group. Subgroups are also included in this limitation. If the amount of sensors exceeds the limitation, surplus sensors will be paused 214. This is of special interest for a Managed Service Provider (MSP). Choose between:

NUMBER OF SENSORS LIMITATION

	▪ **Allow unlimited number of sensors**: Do not limit the number of sensors for this group. Any number of sensors can be added to this group and its subgroups. ▪ **Limit number of sensors in this group**: Enable a limitation for the number of sensors in this group. Only a defined number of sensors can monitor in this group and its subgroups.
Maximum Number of Sensors	This field is only visible if you enable limitation above. Define how many sensors are allowed in this group and its subgroups. Sensors that exceed this group sensor limit will be paused. Please enter an integer value. ⓘ Sensors in paused status 163 count for this group limit as well (for example, manually paused sensors, sensors paused by dependency or schedule), but not for the number of available sensors in your license. ⓘ Manually paused sensors will override the sensor message "exceeds group sensor limit".

Click **Save** to save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Notifications

The status or the data of a sensor can trigger notifications. Using this mechanism, you can configure external alerting tailored to your needs. In an object's detail page, click the **Notifications** tab to change sensor notification triggers. The defined triggers will be inherited down to sensor level. For detailed information, please see **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see **Object Settings** 188 section.

More

Knowledge Base: How does PRTG compute CPU Index, Traffic Index and Response Time Index?

- https://kb.paessler.com/en/topic/313

Knowledge Base: How can I add my own device icons for use in the PRTG web interface?

- https://kb.paessler.com/en/topic/7313

Knowledge Base: How can I change the defaults for names automatically generated for new SNMP sensors?

- https://kb.paessler.com/en/topic/7363

Knowledge Base: Automatically update port name and number for SNMP Traffic sensors when the device changes them

- https://kb.paessler.com/en/topic/25893

Knowledge Base: What is the Overflow Values setting in the SNMP Compatibility Options?

- https://kb.paessler.com/en/topic/43503

7.7 Device Settings

On the details page of a device, click the **Settings** tab to change settings.

Add Device

The **Add Device** dialog appears when you add a new device to a group. It only shows the setting fields that are imperative for creating the device in PRTG. Because of this, you will not see all setting fields in this dialog. For example, the **Device Status** option is not available in this step.

You can change all settings in the **Settings** tab of the device later.

Device Settings

The following settings are available in the **Settings** tab of every device. Because you do not need all of these for every device, depending on the device type, just define the settings you really need and ignore the others.

We recommend that you define as many settings as possible in the **Root** 294 group, so you can inherit them to all other objects further down in the device tree hierarchy 118.

For device settings, there is also multi-edit available. This enables you to change the properties of many devices at a time. For more details, please see **Multi-Edit Lists** 2814 section.

This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

BASIC DEVICE SETTINGS

Device Name	Enter a meaningful name to identify the device. PRTG shows this name by default in the device tree 151 and in all **Alarms** 190 and **Notifications** 2829.
Status	Define the activity status of the device. Choose between: ▪ **Started**: Monitor this device. ▪ **Paused**: Pause monitoring for this device. All sensors on it are in status 163 **Paused** until you change this setting again.
IP Version	Define which IP protocol PRTG will use to connect to this device. The setting is valid for all sensors created on this device. Choose between:

BASIC DEVICE SETTINGS

- **IPv4 device**: Use IP version 4 for all requests to this device.
- **IPv6 device**: Use IP version 6 for all requests to this device.

IP Address/DNS Name

Enter the IP address (either v4 or v6, depending on your selection above) or DNS name for the device. Most sensors you create on this device will inherit this setting and try connecting to this address for monitoring.

Some sensor types have their own setting for IP address/DNS name to which they connect.

Parent Tags

Shows **Tags** [124] that this device inherits [124] from its parent group and probe [118]. This setting is shown for your information only and cannot be changed here.

Tags

Enter one or more **Tags** [124]. Confirm each tag by with the space, comma, or enter key. Sensors on this device inherit these tags. You can use tags to group sensors and tag-filtered views, for example, in **Libraries** [2845]. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to it, if you like.

Priority

Select a priority [211] for the device. This setting determines the order in which your devices are displayed when you view table lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

ADDITIONAL DEVICE INFORMATION

Device Icon

Choose a device icon from the list. PRTG shows it in the device tree.

For information on how to add your custom icons to PRTG on premises instances, please see this article in the Knowledge Base: How can I add my own device icons for use in the PRTG web interface?

Service URL

Specify a URL you would like to open directly when you select **Device Tools | Go To Service URL** from the context menu [222] of the device. For example, you can configure this option to call the address http://www.example.com/service.html. Enter a valid URL or leave the field empty.

DEVICE TYPE

Sensor Management	Select which type of auto-discovery you would like to perform for this device. Choose between: ▪ **Manual (no auto-discovery)**: Select this if you want to only create sensors manually. ▪ **Automatic device identification (standard, recommended)**: Use a small set of auto-discovery templates. This will scan your LAN and usually create a set of standard sensors on your device. ▪ **Automatic device identification (detailed, may create many sensors)**: Use an extended set of auto-discovery templates. This will scan your LAN and usually create many sensors on your device. ▪ **Automatic sensor creation using specific device template (s)**: Use specific auto-discovery templates only. Please select templates below. This will scan your LAN and add sensors defined in the template.
Discovery Schedule	This option is only visible if you select one of the auto-discovery options above. Define when the auto-discovery will run. Choose between: ▪ **Once**: Perform auto-discovery only once. For existing devices, this will initiate a one-time sensor update for the current device. If you select this option, you have to start the auto-discovery manually 250, it will not run automatically. ▪ **Hourly**: Perform auto-discovery for new sensors every hour. ▪ **Daily**: Perform auto-discovery for new sensors every day. ▪ **Weekly**: Perform auto-discovery for new sensors every week.
Device Template(s)	This option is only visible if using specific device templates (last option) is enabled above. Choose one or more templates by adding a check mark in front of the respective template name. You can also select and deselect all items by using the check box in the table head. These will be used for auto-discovery on the current device. Choose from: ▪ **ADSL** ▪ **Amazon Cloudwatch** ▪ **Buffalo TeraStation NAS** ▪ **Cisco ASA VPN** ▪ **Cisco Device (Generic)** ▪ **Dell EqualLogic**

DEVICE TYPE

- Dell MDI Disk
- DNS Server
- Environment Jacarta
- Environment Poseidon
- FTP Server
- Generic Device (PING only)
- Generic Device (SNMP-enabled)
- Generic Device (SNMP-enabled, Detailed)
- HTTP Web Server
- Hyper V Host Server
- IPMI enabled devices
- Juniper NS Device
- Linux/UNIX Device (SNMP or SSH enabled)
- Mail Server (Generic)
- Mail Server (MS Exchange)
- Microsoft Sharepoint 2010
- NAS LenovoEMC
- NAS QNAP
- NAS Synology
- NetApp
- NTP Server
- Printer (HP)
- Printer Generic
- RDP Server
- RMON compatible device
- Server (Compaq/HP agents)
- Server (Dell)
- Sever Cisco UCS
- Server IBM
- SonicWALL
- SSL Security Check

DEVICE TYPE

- **Switch (Cisco Catalyst)**
- **Switch (Cisco IOS Based)**
- **Switch (HP Procurve)**
- **UNIX/Linux Device**
- **UPS Health (APC)**
- **UPS Health (Generic)**
- **UPS Health (Leibert)**
- **VMware ESX / vCenter Server**
- **Webserver**
- **Windows (Detailed via WMI)**
- **Windows (via Remote Powershell)**
- **Windows (via WMI)**
- **Windows IIS (via SNMP)**
- **XEN Hosts**
- **XEN Virtual Machines**

Once the auto-discovery is finished, PRTG will create a new ticket 200 and list the device templates that were actually used to create new sensors. Templates that were not applied will not be shown in the ticket.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

LOCATION

Location (for Geo Maps)	When you want to use **Geo Maps** 2824, enter a location in the first line. Geographical maps will display objects (devices, groups) then with a flag, showing the current status using a color code similar to the sensor status icons 163 (green - yellow - orange - red). You can enter a full postal address, city and country only, or latitude and longitude. It is possible to enter any text before, between, and after the coordinates, PRTG will parse latitude and longitude automatically, for example: 49.452778 11.077778 or enter 49.452778 any 11.077778 text A minus sign (-) in the first line will hide an object from geo maps. In this case you can enter location information in line two and following. You can define a specific label for each location: enter a string denoting the label in the first line and provide geo coordinates in the second line. This geo marker will show then the object with the label in the PRTG geo map. The preview map will always hava a road map layout regardless of the map layout you set in **User Interface** 2945.

CREDENTIALS FOR WINDOWS SYSTEMS

Domain or Computer Name	Define the authority for Windows access. This is used for Windows Management Instrumentation (WMI) and other Windows sensors. If you want to use a Windows local user account on the target device, enter the computer name here. If you want to use a Windows domain user account (recommended), enter the (Active Directory) domain name here. If not explicitly defined, PRTG will automatically add a prefix in order to use the NT LAN Manager (NTLM) protocol. Do not leave this field empty.
User	Enter the username for Windows access. Usually, you will use credentials with administrator privileges.
Password	Enter the password for Windows access. Usually, you will use credentials with administrator privileges.

CREDENTIALS FOR LINUX/SOLARIS/MAC OS (SSH/WBEM) SYSTEMS

User	Enter a login name for the access via SSH and WBEM. Usually, you will use credentials with administrator privileges.

CREDENTIALS FOR LINUX/SOLARIS/MAC OS (SSH/WBEM) SYSTEMS

Login	Define the authentication method to use for login. Choose between: ▪ **Login via Password**: Provide a password for login. Enter below. ▪ **Login via Private Key**: Provide a private key for authentication. PRTG can only handle keys in OpenSSH format that are not encrypted. You cannot use password protected keys here. In the text field, paste the entire private key, including the "BEGIN" and "END" lines. Please make sure the according public key is provided on the target machine. For details, please see **Monitoring via SSH** 3095.
Password	This field is only visible if you select password login above. Enter a password for the Linux access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
Private Key	This field is only visible if you select private key login above. Paste a private key into the field (OpenSSH format, unencrypted). Usually, you will use credentials with administrator privileges. If you do not insert a private key for the first time, but change the private key, you need to restart your PRTG core server service 2988 in order for the private key change to take effect! For details, please see **Monitoring via SSH** 3095.
For WBEM Use Protocol	Define the protocol to use for WBEM. This setting is only relevant if you use WBEM sensors. Choose between: ▪ **HTTP**: Use an unencrypted connection for WBEM. ▪ **HTTPS**: Use an SSL-encrypted connection for WBEM.
For WBEM Use Port	Define the port to use for WBEM. This setting is only relevant if you use WBEM sensors. Choose between: ▪ **Set automatically (port 5988 or 5989)**: Use one of the standard ports, depending on whether you choose unencrypted or encrypted connection above. ▪ **Set manually**: Use a custom port. Define below.
WBEM Port	This setting is only visible if you enable manual port selection above. Enter the WBEM port number.
SSH Port	Enter the port number to use for SSH connections. By default, PRTG uses this setting automatically for all SSH sensors 390, unless you define a different port number in the sensor settings.

CREDENTIALS FOR LINUX/SOLARIS/MAC OS (SSH/WBEM) SYSTEMS

SSH Rights Elevation	Define the rights that you want to use to execute the command on the target system. Choose between: ▪ **Run the command as the user connecting (default)**: Use the rights of the user who establishes the SSH connection, as defined above. ▪ **Run the command as another user using 'sudo' (with password)**: Use the rights of another user with a password required for sudo to run commands on the target device, for example, as root user. ▪ **Run the command as another user using 'sudo' (without password)**: Use the rights of another user without a password required for sudo to run commands on the target device, for example, as root user. ▪ **Run the command as another user using 'su'**: Use the rights of another user with su to run commands on the target device.
Target User	This field is only visible if you choose sudo or su above. Enter a username to run the specified command as a user other than root. If you leave this field empty, you will run the command as root. Ensure you set the Linux password even if you use a public or private key for authentication. This is not necessary if the user is allowed to execute the command without a password.
Password Target User	This field is only visible if you choose to run the commands using su or sudo with password above. Enter the password for the specified target user.
SSH Engine	Select the method you want to use to access data with SSH sensors 3095. We strongly recommend that you keep the default engine! For now, you still can use the legacy mode to ensure compatibility with your target systems. Choose between: ▪ **Default (recommended)**: This is the default monitoring method for SSH sensors. It provides best performance and security. ▪ **Compatibility Mode (deprecated)**: Try this legacy method only if the default mode does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions and is deprecated. We will remove this legacy option soon, so please try to get your SSH sensors running with the default SSH engine. ⓘ You can also individually select the SSH engine for each SSH sensor in the sensor settings.

CREDENTIALS FOR VMWARE/XENSERVER

User	Enter a login name for access to VMware and Xen servers. Usually, you will use credentials with administrator privileges.
Password	Enter a password for access to VMware and Xen servers. Usually, you will use credentials with administrator privileges. Single Sign-On (SSO) passwords for vSphere do not support special characters. Please see the manual sections for VMware sensors for details.
VMware Protocol	Define the protocol used for the connection to VMware and XenServer. Choose between: ▪ **HTTPS (recommended)**: Use an SSL-encrypted connection to VMware and XenServers. ▪ **HTTP**: Use an unencrypted connection to VMware and XenServers.
Session Pool	Define if you want to use session pooling for VMware sensors. Choose between: ▪ **Reuse session for for multiple scans (recommended)**: Select this option to use session pooling. With session pooling, a VMware sensor uses the same session as created in advance to query data and needs not to log in and out for each sensor scan. We recommend that you choose this option because it reduces network load and log entries on the target device, resulting in better performance. ▪ **Create a new session for each scan**: If you select this option and disable session pooling, a VMware sensor has to log in and out for each sensor scan. We recommend that you use the session pooling option above for better performance.

CREDENTIALS FOR SNMP DEVICES

SNMP Version	Select the SNMP version for the device connection. Choose between: ▪ **v1**: Use the simple v1 protocol for SNMP connections. This protocol only offers clear-text data transmission, but it is usually supported by all devices. SNMP v1 does not support 64-bit counters which may result in invalid data when monitoring traffic via SNMP.

CREDENTIALS FOR SNMP DEVICES

- **v2c (recommended)**: Use the more advanced v2c protocol for SNMP connections. This is the most common SNMP version. Data is still transferred as clear-text, but it supports 64-bit counters.
- **v3**: Use the v3 protocol for SNMP connections. It provides secure authentication and data encryption.

When using SNMP v3 you can only monitor a limited number of sensors per second due to internal limitations. The limit is somewhere between 1 and 50 sensors per second (depending on the SNMP latency of your network). This means that using an interval of 60 seconds limits you to between 60 and 3000 SNMP v3 sensors for each probe. If you experience an increased Interval Delay or Open Requests with the **Probe Health Sensor** 1378, distribute the load over multiple probes 3196. SNMP v1 and v2 do not have this limitation.

Community String

This setting is only visible if you select SNMP version **v1** or **v2c** above. Enter the community string of your devices. This is a kind of "clear-text password" for simple authentication. We recommend that you use the default value.

Authentication Type

This setting is only visible if you select SNMP version **v3** above. Choose between:

- **MD5**: Use Message-Digest Algorithm 5 (MD5) for authentication.
- **SHA**: Use Secure Hash Algorithm (SHA) for authentication.

The type you choose must match the authentication type of your device.

If you do not want to use authentication, but you need SNMP v3, for example, because your device requires context, you can leave the field **Password** empty. In this case, SNMP_SEC_LEVEL_NOAUTH is used and authentication deactivated entirely.

User

This setting is only visible if you select SNMP version **v3** above. Enter a username for secure authentication. This value must match the username of your device.

Password

This setting is only visible if you select SNMP version **v3** above. Enter a password for secure authentication. This value must match the password of your device.

Encryption Type

This setting is only visible if you select SNMP version **v3** above. Select an encryption type. Choose between:

- **DES**: Use Data Encryption Standard (DES) as encryption algorithm.

CREDENTIALS FOR SNMP DEVICES

- **AES**: Use Advanced Encryption Standard (AES) as encryption algorithm.

AES 192 and AES 256 are not supported by Net-SNMP because they lack RFC specification.

The type that you choose must match the encryption type of your device.

Data Encryption Key	This setting is only visible if you select SNMP version **v3** above. Enter an encryption key here. If you provide a key in this field, SNMP data packets are encrypted using the encryption algorithm selected above, which provides increased security. The key that you enter here must match the encryption key of your device. If the key you enter in this field does not match the key configured on the target SNMP device, you will not get an error message about this! Please enter a string or leave the field empty.
Context Name	This setting is only visible if you select SNMP version **v3** above. Enter a context name only if it is required by the configuration of the device. Context is a collection of management information accessible by an SNMP device. Please enter a string.
SNMP Port	Enter the port for the SNMP communication. We recommend that you use the default value.
SNMP Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than the value you enter here, the request is aborted and an error message triggered.

CREDENTIALS FOR DATABASE MANAGEMENT SYSTEMS

The settings you define in this section apply to the following sensor types:

- ADO SQL v2 Sensor 418
- Microsoft SQL v2 Sensor 1135
- MySQL v2 Sensor 1151
- Oracle SQL v2 Sensor 1253
- PostgreSQL Sensor 1363

CREDENTIALS FOR DATABASE MANAGEMENT SYSTEMS

Port for Databases	Define which ports PRTG will use for connections to the monitored databases. Choose between: ▪ **Set automatically (default port, recommended)**: PRTG automatically determines the type of the monitored database and uses the corresponding default port to connect. See below for a list of default ports. ▪ **Define one custom port valid for all database sensors**: Choose this option if your database management systems do not use the default ports. Define the port for database connections manually below. If you choose this option, PRTG will use the custom port for all database sensors. If you choose the automatic port selection, PRTG uses the following default ports: ▪ Microsoft SQL: 1433 ▪ MySQL: 3306 ▪ Oracle SQL: 1521 ▪ PostgreSQL: 5432
Custom Database Port	Enter the number of the port that PRTG will use for database connections. Please enter an integer value. All database sensors on this device will use this port to connect.
Authentication Mode	Select the authentication method for the connection to the SQL database. Choose between: ▪ **Windows authentication with impersonation**: If you select this option, PRTG uses the Windows credentials as defined in the particular device settings for the database connection. The user whose credentials are used needs to have permissions to log on to the system on which the PRTG probe with a database sensor runs. This is required for the impersonation. ▪ **SQL server authentication**: Choose this option if you want to use explicit credentials for database connections.
User	This field is only visible if you select SQL server authentication above. Enter the username for the database connection.
Password	This field is only visible if you select SQL server authentication above. Enter the password for the database connection.

CREDENTIALS FOR DATABASE MANAGEMENT SYSTEMS

Timeout (Sec.)	Enter a timeout in seconds for the request. Please enter an integer value. If the reply takes longer than this value defines, the sensor cancels the request and triggers an error message. The maximum timeout value is 300 seconds (5 minutes).

CREDENTIALS FOR AMAZON CLOUDWATCH

Access Key	Enter your Amazon Web Services (AWS) access key. Please see the corresponding Amazon CloudWatch sensor 391 documentation to learn more about the rights that are required for querying AWS CloudWatch metrics.
Secret Key	Enter your Amazon Web Services (AWS) secret key. Please see the corresponding Amazon CloudWatch sensor 391 documentation to learn more about the rights that are required for querying AWS CloudWatch metrics.

WINDOWS COMPATIBILITY OPTIONS

When experiencing problems while monitoring via Windows sensors, you can set some compatibility options for trouble shooting.

Preferred Data Source	Define the method Windows sensors will use to query data. This setting is valid only for hybrid sensors offering performance counter and Windows Management Instrumentation (WMI) technology. The setting will be ignored for all other sensors! Choose between: ▪ **Performance Counters and fallback to WMI**: Try to query data via performance counters. If this is not possible, establish a connection via WMI. ▪ **Performance Counters only**: Query data via performance counters only. If this is not possible, a sensor will return no data. ▪ **WMI only (recommended)**: Query data via WMI only. If this is not possible, a sensor will return no data. In current PRTG versions, this is our recommendation to achieve best performance and stability.
Timeout Method	Specify the time the sensor will wait for the return of its WMI query before aborting it with an error message. Choose between:

WINDOWS COMPATIBILITY OPTIONS

- **Use 1.5x scanning interval (recommended)**: Use a default of one and a half times the scanning interval set for the sensor (see below in this settings).
- **Set manually**: Enter a timeout value manually.

We recommend that you use the default value. Only if you experience ongoing timeout errors, try increasing the timeout value.

Timeout Value (Sec.)

This field is only visible if the manual timeout method is selected above. Specify the time the sensor will wait for the return of its WMI query before aborting with an error message. Please enter an integer value.

SNMP COMPATIBILITY OPTIONS

When experiencing problems while monitoring via Simple Network Management Protocol (SNMP) sensors, you can set some compatibility options for trouble shooting.

SNMP Delay (ms)

Add a time in milliseconds that will be waited between two SNMP requests. This can help increase device compatibility. Please enter an integer value. We recommend that you use the default value. If you experience SNMP connection failures, please increase it. You can define a delay between 0 and 100, higher delays are not supported and will be discarded.

Failed Requests

Define if an SNMP sensor will try again after a request fails.

- **Retry (recommended)**: Try again if an SNMP request fails. This can help prevent false error messages due to temporary timeout failures.
- **Do not retry**: Do not retry if an SNMP request fails. With this setting enabled an SNMP sensor will be set to error status earlier.

Overflow Values

Define how PRTG will handle overflow values. Some devices do not handle internal buffer overflows correctly. This can cause false peaks.

- **Ignore overflow values**: Ignore overflow values and do not include them in the monitoring data.
- **Handle overflow values as valid results**: Regard all overflow values as regular data and include them in the monitoring data.

SNMP COMPATIBILITY OPTIONS

We recommend that you use the default value.

If you experience problems because of strange peaks in your data graphs, change this option. Peaks might indicate that the monitored device resets counters without an overflow. PRTG interprets such a behavior as overflow that results in data peaks. Choose the option **Ignore overflow values** in this case. For more details, see this Knowledge Base article: What is the Overflow Values setting in the SNMP Compatibility Options?

Zero Values

Define how PRTG will handle zero values. Some devices send incorrect zero values. This can cause false peaks.

- **Ignore zero values for delta sensors (recommended)**: Ignore zero values and do not include them in the monitoring data.
- **Handle zero values as valid results for delta sensors**: Regard all zero values as regular data and include them in the monitoring data.

We recommend that you use the default value. If you experience problems, change this option.

32-bit/64-bit Counters

Define which kind of traffic counters PRTG will search for on a device.

- **Use 64-bit counters if available (recommended)**: The interface scan will use 64-bit traffic counters, if available. This can avoid buffer overflows in the devices.
- **Use 32-bit counters only**: The interface scan will always use 32-bit traffic counters, even if 64-bit counters are available. This can lead to more reliable monitoring for some devices.

We recommend that you use the default value. If you experience problems, change this option.

Request Mode

Define which kind of request method PRTG uses for SNMP sensors.

- **Use multi get (recommended)**: Bundle multiple SNMP requests into one request.
- **Use single get**: Use one request for each SNMP value. This can increase compatibility with older devices.

We recommend that you use the default value. If you experience problems, change this option.

PRTG uses paging for SNMP requests. This means that if a sensor has to query more than 20 OIDs, it will automatically poll the OIDs in packages of 20 OIDs each per request.

SNMP COMPATIBILITY OPTIONS

Port Name Template

Define how the name of SNMP sensors created on a device will be put together. Enter a template using several variables. When adding new sensors, PRTG scans the interface for available counters at certain OIDs. At each OID usually several fields are available with interface descriptions. They are different for every device and OID. PRTG will use the information in these fields to name the sensors. If a field is empty or not available, an empty string is added to the name. As default, **([port]) [ifalias]** is set as port name template, which will create a name such as (001) Ethernet1, for example. You can use any field names available at a certain OID of your device, among which are:

- **[port]**: The port number of the monitored interface.
- **[ifalias]**: The 'alias' name for the monitored interface as specified by a network manager, providing a non-volatile handling.
- **[ifname]**: The textual name of the monitored interface as assigned by the local device.
- **[ifdescr]**: A textual string containing information about the monitored device or interface, for example, manufacturer, product name, version.
- **[ifspeed]**: An estimate of the monitored interface's current bandwidth (KBit/s).
- **[ifsensor]**: The type of the sensor, this is SNMP Traffic or SNMP RMON. This is useful to differentiate between your SNMP Traffic 2132 and SNMP RMON 2073 sensors.

Combine them as you like to obtain suitable sensor names.

For more information about SNMP sensor names, see this Knowledge Base article: How can I change the defaults for names automatically generated for new SNMP sensors?

Port Name Update

Define how PRTG will react if you change port names in your physical device (for example, a switch or router). Choose between:

- **Keep port names (use this if you edit the names in PRTG)**: Do not automatically adjust sensor names. This is the best option if you want to change names in PRTG manually.
- **Automatic sensor name update if name changes in device**: If PRTG detects changes of port names in your physical device, it will try to automatically adjust sensor names accordingly.

For more information about automatic updates of names, see this Knowledge Base article: Automatically update port name and number for SNMP Traffic sensors when the device changes them

SNMP COMPATIBILITY OPTIONS

Port Identification

Define which field will be used for SNMP interface identification. Choose between:

- **Automatic (recommended)**: Tries the ifAlias field first to identify an SNMP interface and then ifDescr.
  ifName will not be tried automatically.
- **Use ifAlias**: For most devices ifAlias is the best field to get unique interface names.
- **Use ifDescr**: Use this option if the port order of your device changes after a reboot, and there is no ifAlias field available. For example, this is the best option for Cisco ASA devices.
  When using this option it is important that your device returns unique interface names in the ifDescr field.
- **Use ifName**: You can also use this option if there is no unique ifAlias available.
  When using this option it is important that your device returns unique interface names in the ifName field.
- **No Port Update**: Use this option to disable automatic port identification.

Start Interface Index

For SNMP Traffic sensors 2132, define at which index PRTG will start to query the interface range during sensor creation. Use 0 for automatic mode. We recommend that you use the default value.

End Interface Index

For SNMP Traffic sensors 2132, define at which index PRTG will stop to query the interface range during sensor creation. Use 0 for automatic mode. We recommend that you use the default value.

PROXY SETTINGS FOR HTTP SENSORS

HTTP Proxy Settings

The proxy settings determine how a sensor connects to a given URL. You can enter data for an HTTP proxy server that sensors will use when connecting via HTTP or HTTPS.

This setting affects monitoring only and determines the behavior of HTTP sensors. To change proxy settings for the core server, please see **System Administration—Core & Probes** 2967.

PROXY SETTINGS FOR HTTP SENSORS

The SSL Certificate Sensor 2289 and the SSL Security Check Sensor 2299 do not support HTTP proxies, but you can configure connections via SOCKS proxies in their sensor settings.

Name	Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.
Port	Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.
User	If the proxy requires authentication, enter the username for the proxy login. Only basic authentication is available! Please enter a string or leave the field empty.
Password	If the proxy requires authentication, enter the password for the proxy login. Only basic authentication is available! Please enter a string or leave the field empty.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.

SCANNING INTERVAL

- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

CLUSTER USAGE

Scanning Distribution: This box is only visible if you run a PRTG cluster. Sometimes you want to exclude a certain node from monitoring the sensors running on this probe, group, or device, for example, if a device is not reachable from every node configured in your cluster. In the list of cluster nodes, please select the nodes that will not be included in sensor scans. By default, this setting is inherited 122 to all objects underneath.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. To terminate a current maintenance window before the defined end date, you can change the time in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current object if its parent object is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current object if its parent object is in a **Down** status, or if it is paused by another dependency. Additionally, pause the current object if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. You do not trigger a status change by dependency if you manually pause a master object or if you pause it by schedule.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 210 to choose an object on which the current object will be dependent on.
Dependency Delay (Sec.)	This field is only visible if you select another object than the parent as dependency type. Define a time span in seconds for dependency delay. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

ADVANCED NETWORK ANALYSIS

Unusual Detection	Define if you want to benefit from unusual detection 2956 for sensors. You can configure the behavior of unusual detection (or disable it completely) in the system settings 2956. Choose between: ▪ **Enabled**: Activate unusual detection for this object and, by default, for all objects underneath in the hierarchy 118 of the device tree. Sensors affected by this setting will turn to orange color (unusual sensor status 163) if PRTG detects unusual activity. ▪ **Disabled**: Do not activate unusual detection. PRTG will ignore unusual values for sensors affected by this setting. These sensor will not show an unusual sensor status.
Similar Sensors Detection	Define if you want to activate **Similar Sensors** 180 analysis. You can configure the depth of analysis of similar sensors detection (or disable it completely) in the system settings 2958. Choose between: ▪ **Enabled**: Activate similar sensors detection for this object and, by default, for all objects underneath in the hierarchy 118 of the device tree. PRTG considers all sensors affected by this setting during similarity analysis. ▪ **Disabled**: Do not activate similar sensors detection. PRTG will not consider sensors affected by this setting during similarity analysis.
System Information	Define if you want to retrieve and show **System Information** 193 for your devices. Choose between: ▪ **Enabled**: Activate the system information feature for this object and, by default, for all objects underneath in the hierarchy 118 of the device tree. ▪ **Disabled**: Do not activate system information. This setting is not available for local probes in PRTG on demand.

Click **Save** to save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Notifications

The status or the data of a sensor can trigger notifications. Using this mechanism, you can configure external alerting tailored to your needs. In an object's detail page, click the **Notifications** tab to change sensor notification triggers. The defined triggers will be inherited down to sensor level. For detailed information, please see **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see **Object Settings** 188 section.

More

Knowledge Base: How does PRTG compute CPU Index, Traffic Index and Response Time Index?

- https://kb.paessler.com/en/topic/313

Knowledge Base: How can I add my own device icons for use in the PRTG web interface?

- https://kb.paessler.com/en/topic/7313

Knowledge Base: How can I change the defaults for names automatically generated for new SNMP sensors?

- https://kb.paessler.com/en/topic/7363

Knowledge Base: Automatically update port name and number for SNMP Traffic sensors when the device changes them

- https://kb.paessler.com/en/topic/25893

Knowledge Base: What is the Overflow Values setting in the SNMP Compatibility Options?

- https://kb.paessler.com/en/topic/43503

7.8 Sensor Settings

There are more than 200 different sensor types available. In the **Add Sensor** dialog, all sensors are categorized into groups to help you quickly find what you need. Once you are familiar with the interface, you will probably enter the first letters of a sensor type's name into the **Search** field in the upper-left corner and get to a sensor even faster.

Available Sensor Types

There is a dedicated manual section for every sensor type with details about the available settings. For more information, please see the **List of Available Sensors** 385.

For sensor settings, there is also multi-edit available. This enables you to change properties of many sensors at a time. For more details, please see the **Multi-Edit Lists** 2814 section.

In order to detect unexpected correlations between your network components, PRTG provides a **Similar Sensors** 180 analysis.

Sensor Settings Overview

For information about sensor settings, please see the following sections:

- **Sensor Settings—** 384 **List of Available Sensor Types** 385
- **Additional Sensor Types (Custom Sensors)** 2778
- **Sensor Channels Settings** 2782
- **Sensor Notifications Settings** 2791

7.8.1 List of Available Sensor Types

This chapter lists all available sensors, arranged both by different categories and in alphabetical order.

In the **Add a Sensor** 288 assistant, PRTG offers you various options to easily filter for fitting sensor types.

- Common Sensors 385
- Bandwidth Monitoring Sensors 386
- Web Servers (HTTP) Sensors 386
- SNMP Sensors 387
- Windows WMI/Performance Counters Sensors 389
- Linux/Unix/OS X Sensors 390
- Virtual Servers Sensors 391
- Mail Servers Sensors 391
- Database Servers Sensors 392
- Storage and File Servers Sensors 392
- Various Servers Sensors 394
- VoIP and QoS Sensors 394
- Hardware Parameters Sensors 394
- Cloud Services Sensors 396
- Custom Sensors 396
- PRTG Internal Sensors 397
- All Sensors in Alphabetical Order 397
- Script World Sensors 404
- More 406

Common Sensors

- Cloud HTTP Sensor 571
- Cloud Ping Sensor 580
- HTTP Sensor 848
- Ping Sensor 1319
- Port Sensor 1346
- Port Range Sensor 1355
- SNMP Traffic Sensor 2132
- SSL Certificate Sensor 2289

- SSL Security Check Sensor 2299
- Windows Network Card Sensor 2441

Bandwidth Monitoring Sensors

- IPFIX Sensor 1063
- IPFIX (Custom) Sensor 1075
- jFlow V5 Sensor 1095
- jFlow V5 (Custom) Sensor 1107
- NetFlow V5 Sensor 1207
- NetFlow V5 (Custom) Sensor 1219
- NetFlow V9 Sensor 1230
- NetFlow V9 (Custom) Sensor 1242
- Packet Sniffer Sensor 1278
- Packet Sniffer (Custom) Sensor 1289
- sFlow Sensor 1457
- sFlow (Custom) Sensor 1469
- SNMP Cisco ADSL Sensor 1548
- SNMP Cisco ASA VPN Traffic Sensor 1566
- SNMP Library Sensor 1912
- SNMP NetApp Network Interface Sensor 2014
- SNMP RMON Sensor 2073
- SNMP Traffic Sensor 2132
- Windows Network Card Sensor 2441

Web Servers (HTTP) Sensors

- Cloud HTTP Sensor 571
- Common SaaS Sensor 594
- HTTP Sensor 848
- HTTP Advanced Sensor 858
- HTTP Apache ModStatus PerfStats Sensor 874
- HTTP Apache ModStatus Totals Sensor 884
- HTTP Content Sensor 894
- HTTP Data Advanced Sensor 906
- HTTP Full Web Page Sensor 918
- HTTP Push Count Sensor 929

- HTTP Push Data Sensor 939
- HTTP Push Data Advanced Sensor 951
- HTTP Transaction Sensor 962
- HTTP XML/REST Value Sensor 976
- SSL Certificate Sensor 2289
- SSL Security Check Sensor 2299
- Windows IIS Application Sensor 2421

SNMP Sensors

- SNMP APC Hardware Sensor 1530
- SNMP Buffalo TS System Health Sensor 1539
- SNMP Cisco ADSL Sensor 1548
- SNMP Cisco ASA VPN Connections Sensor 1556
- SNMP Cisco ASA VPN Traffic Sensor 1566
- SNMP Cisco ASA VPN Users Sensor 1577
- SNMP Cisco CBQoS Sensor 1587
- SNMP Cisco System Health Sensor 1596
- SNMP Cisco UCS Blade Sensor 1605
- SNMP Cisco UCS Chassis Sensor 1614
- SNMP Cisco UCS Sensor 1623
- SNMP Cisco UCS System Health Sensor 1632
- SNMP CPU Load Sensor 1641
- SNMP Custom Sensor 1649
- SNMP Custom Advanced Sensor 1658
- SNMP Custom String Sensor 1668
- SNMP Custom String Lookup Sensor 1679
- SNMP Custom Table Sensor 1689
- SNMP Dell EqualLogic Logical Disk Sensor 1701
- SNMP Dell EqualLogic Member Health Sensor 1710
- SNMP Dell EqualLogic Physical Disk Sensor 1720
- SNMP Dell Hardware Sensor 1729
- SNMP Dell PowerEdge Physical Disk Sensor 1738
- SNMP Dell PowerEdge System Health Sensor 1747
- SNMP Disk Free Sensor 1757

- SNMP Hardware Status Sensor 1766
- SNMP HP BladeSystem Server Blade Sensor 1775
- SNMP HP BladeSystem System Health Sensor 1783
- SNMP HP LaserJet Hardware Sensor 1791
- SNMP HP ProLiant Logical Disk Sensor 1800
- SNMP HP ProLiant Memory Controller Sensor 1809
- SNMP HP ProLiant Network Interface Sensor 1818
- SNMP HP ProLiant Physical Disk Sensor 1827
- SNMP HP ProLiant System Health Sensor 1836
- SNMP IBM System X Logical Disk Sensor 1845
- SNMP IBM System X Physical Disk Sensor 1854
- SNMP IBM System X Physical Memory Sensor 1863
- SNMP IBM System X System Health Sensor 1872
- SNMP interSeptor Pro Environment Sensor 1881
- SNMP Juniper System Health Sensor 1889
- SNMP LenovoEMC Physical Disk Sensor 1897
- SNMP LenovoEMC System Health Sensor 1905
- SNMP Library Sensor 1912
- SNMP Linux Disk Free Sensor 1924
- SNMP Linux Load Average Sensor 1936
- SNMP Linux Meminfo Sensor 1944
- SNMP Linux Physical Disk Sensor 1952
- SNMP Memory Sensor 1961
- SNMP NetApp Disk Free Sensor 1970
- SNMP NetApp Enclosure Sensor 1979
- SNMP NetApp I/O Sensor 1988
- SNMP NetApp License Sensor 1997
- SNMP NetApp Logical Unit Sensor 2005
- SNMP NetApp Network Interface Sensor 2014
- SNMP NetApp System Health Sensor 2022
- SNMP Poseidon Environment Sensor 2031
- SNMP Printer Sensor 2039
- SNMP QNAP Logical Disk Sensor 2047
- SNMP QNAP Physical Disk Sensor 2056

- SNMP QNAP System Health Sensor 2065
- SNMP RMON Sensor 2073
- SNMP SonicWALL System Health Sensor 2083
- SNMP SonicWALL VPN Traffic Sensor 2091
- SNMP Synology Logical Disk Sensor 2100
- SNMP Synology Physical Disk Sensor 2108
- SNMP Synology System Health Sensor 2116
- SNMP System Uptime Sensor 2124
- SNMP Traffic Sensor 2132
- SNMP Trap Receiver Sensor 2143
- SNMP Windows Service Sensor 2155

Windows WMI/Performance Counters Sensors

- Active Directory Replication Errors Sensor 407
- Event Log (Windows API) Sensor 677
- PerfCounter Custom Sensor 1299
- PerfCounter IIS Application Pool Sensor 1309
- Windows IIS 6.0 SMTP Received Sensor 2403
- Windows IIS 6.0 SMTP Sent Sensor 2412
- Windows IIS Application Pool Sensor 1309
- Windows CPU Load Sensor 2393
- Windows MSMQ Queue Length Sensor 2430
- Windows Network Card Sensor 2441
- Windows Pagefile Sensor 2452
- Windows Physical Disk I/O Sensor 2461
- Windows Print Queue Sensor 2472
- Windows Process Sensor 2483
- Windows System Uptime Sensor 2493
- Windows Updates Status (Powershell) Sensor 2502
- WMI Custom Sensor 2512
- WMI Custom String Sensor 2522
- WMI Event Log Sensor 2533
- WMI Exchange Server Sensor 2544
- WMI Exchange Transport Queue Sensor 2554

- WMI File Sensor 2564
- WMI Free Disk Space (Multi Disk) Sensor 2573
- WMI HDD Health Sensor 2585
- WMI Logical Disk I/O Sensor 2596
- WMI Memory Sensor 2606
- WMI Microsoft SQL Server 2005 Sensor 2615
- WMI Microsoft SQL Server 2008 Sensor 2628
- WMI Microsoft SQL Server 2012 Sensor 2640
- WMI Microsoft SQL Server 2014 Sensor 2652
- WMI Microsoft SQL Server 2016 Sensor 2664
- WMI Remote Ping Sensor 2676
- WMI Security Center Sensor 2685
- WMI Service Sensor 2695
- WMI Share Sensor 2705
- WMI SharePoint Process Sensor 2715
- WMI Terminal Services (Windows 2008+) Sensor 2724
- WMI Terminal Services (Windows XP/Vista/2003) Sensor 2732
- WMI UTC Time Sensor 2740
- WMI Vital System Data (V2) Sensor 2748
- WMI Volume Sensor 2758
- WSUS Statistics Sensor 2767

Linux/Unix/OS X Sensors

- Python Script Advanced Sensor 1385
- SNMP Linux Disk Free Sensor 1924
- SNMP Linux Load Average Sensor 1936
- SNMP Linux Meminfo Sensor 1944
- SNMP Linux Physical Disk Sensor 1952
- SSH Disk Free Sensor 2170
- SSH INodes Free Sensor 2183
- SSH Load Average Sensor 2193
- SSH Meminfo Sensor 2203
- SSH Remote Ping Sensor 2213
- SSH Script Sensor 2266

- SSH Script Advanced Sensor 2278
- SSH SAN Enclosure Sensor 2223
- SSH SAN Logical Disk Sensor 2233
- SSH SAN Physical Disk Sensor 2244
- SSH SAN System Health Sensor 2255

Virtual Servers Sensors

- Citrix XenServer Host Sensor 550
- Citrix XenServer Virtual Machine Sensor 561
- Docker Container Status Sensor 646
- Enterprise Virtual Array Sensor 666
- Hyper-V Cluster Shared Volume Disk Free Sensor 991
- Hyper-V Host Server Sensor 1001
- Hyper-V Virtual Machine Sensor 1009
- Hyper-V Virtual Network Adapter Sensor 1020
- Hyper-V Virtual Storage Device Sensor 1031
- VMware Datastore (SOAP) Sensor 2344
- VMware Host Hardware (WBEM) Sensor 2354
- VMware Host Hardware Status (SOAP) Sensor 2362
- VMware Host Performance (SOAP) Sensor 2372
- VMware Virtual Machine (SOAP) Sensor 2382

Mail Servers Sensors

- Exchange Backup (Powershell) Sensor 687
- Exchange Database (Powershell) Sensor 697
- Exchange Database DAG (Powershell) Sensor 707
- Exchange Mail Queue (Powershell) Sensor 717
- Exchange Mailbox (Powershell) Sensor 727
- Exchange Public Folder (Powershell) Sensor 737
- IMAP Sensor 1040
- IP on DNS Blacklist Sensor 1054
- POP3 Sensor 1337
- SMTP Sensor 1499
- SMTP&IMAP Round Trip Sensor 1508
- SMTP&POP3 Round Trip Sensor 1519

- SSL Security Check Sensor 2299
- WMI Exchange Server Sensor 2544
- WMI Exchange Transport Queue Sensor 2554
- Windows IIS 6.0 SMTP Received Sensor 2403
- Windows IIS 6.0 SMTP Sent Sensor 2412

Database Servers Sensors

- ADO SQL v2 Sensor 418
- Microsoft SQL v2 Sensor 1135
- MySQL v2 Sensor 1151
- Oracle SQL v2 Sensor 1253
- Oracle Tablespace Sensor 1268
- PostgreSQL Sensor 1363
- WMI Microsoft SQL Server 2005 Sensor 2615
- WMI Microsoft SQL Server 2008 Sensor 2628
- WMI Microsoft SQL Server 2012 Sensor 2640
- WMI Microsoft SQL Server 2014 Sensor 2652
- WMI Microsoft SQL Server 2016 Sensor 2664

Storage and File Servers Sensors

- Dell PowerVault MDi Logical Disk Sensor 609
- Dell PowerVault MDi Physical Disk Sensor 618
- Enterprise Virtual Array Sensor 666
- File Sensor 770
- File Content Sensor 779
- Folder Sensor 789
- FTP Sensor 800
- FTP Server File Count Sensor 808
- Hyper-V Cluster Shared Volume Disk Free Sensor 991
- Hyper-V Virtual Storage Device Sensor 1031
- NetApp cDOT Aggregate (SOAP) Sensor 1166
- NetApp cDOT I/O (SOAP) Sensor 1176
- NetApp cDOT Physical Disk (SOAP) 1187
- NetApp cDOT System Health (SOAP) Sensor 1197
- SFTP Secure File Transfer Protocol Sensor 1481

- Share Disk Free Sensor 1430
- SNMP Buffalo TS System Health Sensor 1539
- SNMP Cisco UCS Physical Disk Sensor 1623
- SNMP Dell EqualLogic Logical Disk Sensor 1701
- SNMP Dell EqualLogic Member Health Sensor 1710
- SNMP Dell EqualLogic Physical Disk Sensor 1720
- SNMP Dell PowerEdge Physical Disk Sensor 1738
- SNMP HP ProLiant Logical Disk Sensor 1800
- SNMP HP ProLiant Physical Disk Sensor 1827
- SNMP IBM System X Logical Disk Sensor 1845
- SNMP IBM System X Physical Disk Sensor 1854
- SNMP Linux Disk Free Sensor 1924
- SNMP Linux Physical Disk Sensor 1952
- SNMP LenovoEMC Physical Disk Sensor 1897
- SNMP LenovoEMC System Health Sensor 1905
- SNMP NetApp Disk Free Sensor 1970
- SNMP NetApp Enclosure Sensor 1979
- SNMP NetApp I/O Sensor 1988
- SNMP NetApp License Sensor 1997
- SNMP NetApp Logical Unit Sensor 2005
- SNMP NetApp Network Interface Sensor 2014
- SNMP NetApp System Health Sensor 2022
- SNMP QNAP Logical Disk Sensor 2047
- SNMP QNAP Physical Disk Sensor 2056
- SNMP QNAP System Health Sensor 2065
- SNMP Synology Logical Disk Sensor 2100
- SNMP Synology Physical Disk Sensor 2108
- SNMP Synology System Health Sensor 2116
- SSH SAN Enclosure Sensor 2223
- SSH SAN Logical Disk Sensor 2233
- SSH SAN Physical Disk Sensor 2244
- SSH SAN System Health Sensor 2255
- TFTP Sensor 2327
- VMware Datastore (SOAP) Sensor 2344

- Windows Physical Disk I/O Sensor 2461
- WMI File Sensor 2564
- WMI Free Disk Space (Multi Disk) Sensor 2573
- WMI Logical Disk I/O Sensor 2596
- WMI Volume Sensor 2758

Various Servers Sensors

- DHCP Sensor 628
- DNS Sensor 638
- IPMI System Health Sensor 1085
- LDAP Sensor 1118
- Ping Sensor 1319
- Ping Jitter Sensor 1328
- Port Sensor 1346
- Port Range Sensor 1355
- RADIUS v2 Sensor 1413
- RDP (Remote Desktop) Sensor 1422
- SNMP Trap Receiver Sensor 2143
- SNTP Sensor 2163
- Syslog Receiver Sensor 2309
- SSL Security Check Sensor 2299
- Traceroute Hop Count Sensor 2335

VoIP and QoS Sensors

- Cisco IP SLA Sensor 540
- SIP Options Ping Sensor 1490
- QoS (Quality of Service) One Way Sensor 1395
- QoS (Quality of Service) Round Trip Sensor 1403
- SNMP Cisco CBQoS Sensor 1587

Hardware Parameter Sensors

- Dell PowerVault MDi Logical Disk Sensor 609
- Dell PowerVault MDi Physical Disk Sensor 618
- Enterprise Virtual Array Sensor 666
- NetApp cDOT Aggregate (SOAP) Sensor 1166

- NetApp cDOT I/O (SOAP) Sensor 1176
- NetApp cDOT Physical Disk (SOAP) Sensor 1187
- NetApp cDOT System Health (SOAP) Sensor 1197
- SNMP APC Hardware Sensor 1530
- SNMP Buffalo TS System Health Sensor 1539
- SNMP Cisco System Health Sensor 1596
- SNMP Cisco UCS Blade Sensor 1605
- SNMP Cisco UCS Chassis Sensor 1614
- SNMP Cisco UCS Physical Disk Sensor 1623
- SNMP Cisco UCS System Health Sensor 1632
- SNMP CPU Load Sensor 1641
- SNMP Dell EqualLogic Logical Disk Sensor 1701
- SNMP Dell EqualLogic Member Health Sensor 1710
- SNMP Dell EqualLogic Physical Disk Sensor 1720
- SNMP Dell Hardware Sensor 1729
- SNMP Dell PowerEdge Physical Disk Sensor 1738
- SNMP Dell PowerEdge System Health Sensor 1747
- SNMP Disk Free Sensor 1757
- SNMP Hardware Status Sensor 1766
- SNMP HP BladeSystem Blade Sensor 1775
- SNMP HP BladeSystem Enclosure System Health Sensor 1783
- SNMP HP LaserJet Hardware Sensor 1791
- SNMP HP ProLiant Memory Controller Sensor 1809
- SNMP HP ProLiant Network Interface Sensor 1818
- SNMP HP ProLiant Physical Disk Sensor 1827
- SNMP HP ProLiant System Health Sensor 1836
- SNMP IBM System X Physical Disk Sensor 1854
- SNMP IBM System X Physical Memory Sensor 1863
- SNMP IBM System X System Health Sensor 1872
- SNMP Juniper NS System Health Sensor 1889
- SNMP LenovoEMC Physical Disk Sensor 1897
- SNMP LenovoEMC System Health Sensor 1905
- SNMP Library Sensor 1912
- SNMP Memory Sensor 1961

- SNMP NetApp I/O Sensor 1988
- SNMP NetApp Enclosure Sensor 1979
- SNMP NetApp Logical Unit Sensor 2005
- SNMP NetApp Network Interface Sensor 2014
- SNMP NetApp System Health Sensor 2022
- SNMP QNAP Physical Disk Sensor 2056
- SNMP QNAP System Health Sensor 2065
- SNMP SonicWALL System Health Sensor 2083
- SNMP SonicWALL VPN Traffic Sensor 2091
- SNMP Synology Physical Disk Sensor 2108
- SNMP Synology System Health Sensor 2116
- SSH SAN Enclosure Sensor 2223
- SSH SAN Logical Disk Sensor 2233
- SSH SAN Physical Disk Sensor 2244
- SSH SAN System Health Sensor 2255
- WMI HDD Health Sensor 2585

Cloud Services Sensors

- Amazon CloudWatch Alarm Sensor 433
- Amazon CloudWatch EBS Sensor 443
- Amazon CloudWatch EC2 Sensor 455
- Amazon CloudWatch ElastiCache Sensor 467
- Amazon CloudWatch ELB Sensor 479
- Amazon CloudWatch RDS Sensor 491
- Amazon CloudWatch SNS Sensor 504
- Amazon CloudWatch SQS Sensor 516
- Common SaaS Sensor 594
- Dropbox Sensor 656
- GitLab Build Status Sensor 818
- Google Analytics Sensor 827
- Google Drive Sensor 839
- Microsoft OneDrive Sensor 1125

Custom Sensors

- EXE/Script Sensor 747

- EXE/Script Advanced Sensor 759
- IPFIX (Custom) Sensor 1075
- jFlow V5 (Custom) Sensor 1107
- NetFlow V5 (Custom) Sensor 1219
- NetFlow V9 (Custom) Sensor 1242
- Packet Sniffer (Custom) Sensor 1289
- Python Script Advanced Sensor 1385
- Sensor Factory Sensor 1438
- sFlow (Custom) Sensor 1469
- SNMP Custom Sensor 1649
- SNMP Custom Advanced Sensor 1658
- SNMP Custom Lookup Sensor 1679
- SNMP Custom String Sensor 1668
- SNMP Custom Table Sensor 1689
- SSH Script Sensor 2266
- WMI Custom Sensor 2512
- WMI Custom String Sensor 2522

PRTG Internal Sensors

- ClusterState Sensor 589
- Core Health Sensor 602
- Probe Health Sensor 1378
- System Health Sensor 2321

All Sensors in Alphabetical Order

The version numbers show when the respective sensor type was originally introduced to PRTG.

- Active Directory Replication Errors Sensor 407 (v8.3.0)
- ADO SQL v2 Sensor 418 (v16.x.24)
- Amazon CloudWatch Alarm Sensor 433 (v16.x.22)
- Amazon CloudWatch EBS Sensor 443 (v15.x.19)
- Amazon CloudWatch EC2 Sensor 455 (v15.x.19)
- Amazon CloudWatch ElastiCache Sensor 467 (v15.x.19)
- Amazon CloudWatch ELB Sensor 479 (v15.x.19)
- Amazon CloudWatch RDS Sensor 491 (v15.x.19)

- Amazon CloudWatch SNS Sensor 504 (v15.x.19)
- Amazon CloudWatch SQS Sensor 516 (v15.x.19)
- Business Process Sensor 528 (v15.x.20)
- Cisco IP SLA Sensor 540 (v7)
- Citrix XenServer Host Sensor 550 (v12.x.1)
- Citrix XenServer Virtual Machine Sensor 561 (v8.1.0)
- Cloud HTTP Sensor 571 (v14.x.14)
- Cloud Ping Sensor 580 (v14.x.14)
- ClusterState Sensor 589 (v9.1.0)
- Common SaaS Sensor 594 (v15.x.19)
- Core Health Sensor 602 (v9.1.0)
- Dell PowerVault MDi Logical Disk Sensor 609 (v12.x.1)
- Dell PowerVault MDi Physical Disk Sensor 618 (v14.x.13)
- DHCP Sensor 628 (v8.2.0)
- DNS Sensor 638 (v7)
- Docker Container Status Sensor 646 (v16.x.22)
- Dropbox Sensor 656 (v15.x.19)
- Enterprise Virtual Array Sensor 666 (v13.x.6)
- Event Log (Windows API) Sensor 677 (v7)
- Exchange Backup (Powershell) Sensor 687 (v13.x.5)
- Exchange Database (Powershell) Sensor 697 (v13.x.5)
- Exchange Database DAG (Powershell) Sensor 707 (v15.x.18)
- Exchange Mail Queue (Powershell) Sensor 717 (v13.x.5)
- Exchange Mailbox (Powershell) Sensor 727 (v13.x.5)
- Exchange Public Folder (Powershell) Sensor 737 (v13.x.5)
- EXE/Script Sensor 747 (v7)
- EXE/Script Advanced Sensor 759 (v7)
- File Sensor 770 (v7)
- File Content Sensor 779 (v7)
- Folder Sensor 789 (v7)
- FTP Sensor 800 (v7)
- FTP Server File Count Sensor 808 (v8.3.0)
- GitLab Build Status Sensor 818 (v16.3.26)
- Google Analytics Sensor 827 (v15.x19)

- Google Drive Sensor 839 (v15.x.19)
- HTTP Sensor 848 (v7)
- HTTP Advanced Sensor 858 (v7)
- HTTP Apache ModStatus PerfStats Sensor 874 (v12.x.3)
- HTTP Apache ModStatus Totals Sensor 884 (v12.x.3)
- HTTP Content Sensor 894 (v7)
- HTTP Data Advanced Sensor 906 (v15.x.16)
- HTTP Full Web Page Sensor 918 (v7)
- HTTP Push Count Sensor 929 (v13.4.8)
- HTTP Push Data Sensor 939 (v14.1.9)
- HTTP Push Data Advanced Sensor 951 (14.1.10)
- HTTP Transaction Sensor 962 (v7)
- HTTP XML/REST Value Sensor 976 (v8.3.0)
- Hyper-V Cluster Shared Volume Disk Free Sensor 991 (v12.3.4)
- Hyper-V Host Server Sensor 1001 (v7)
- Hyper-V Virtual Machine Sensor 1009 (v7)
- Hyper-V Virtual Network Adapter Sensor 1020 (v9.1.0)
- Hyper-V Virtual Storage Device Sensor 1031 (v12.4.4)
- IMAP Sensor 1040 (v7)
- IP on DNS Blacklist Sensor 1054 (v8.3.0)
- IPFIX Sensor 1063 (v13.x.7)
- IPFIX (Custom) Sensor 1075 (v13.x.7)
- IPMI System Health Sensor 1085 (v14.x.11)
- jFlow V5 Sensor 1095 (v8.2.0)
- jFlow V5 (Custom) Sensor 1107 (v8.2.0)
- LDAP Sensor 1118 (v8.1.0)
- Microsoft OneDrive Sensor 1125 (v15.x.19)
- Microsoft SQL v2 Sensor 1135 (v14.x.12)doku
- MySQL v2 Sensor 1151 (v14.x.12)
- NetApp cDOT Aggregate (SOAP) Sensor 1166 (v15.4.21)
- NetApp cDOT I/O (SOAP) Sensor 1176 (v15.4.21)
- NetApp cDOT Physical Disk (SOAP) Sensor 1187 (v15.4.21)
- NetApp cDOT System Health (SOAP) Sensor 1197 (v15.4.21)
- NetFlow V5 Sensor 1207 (v7)

- NetFlow V5 (Custom) Sensor 1219 (v7)
- NetFlow V9 Sensor 1230 (v7)
- NetFlow V9 (Custom) Sensor 1242 (v7)
- Oracle SQL v2 Sensor 1253 (v14.x.13)
- Oracle Tablespace Sensor 1268 (v15.x.18)
- Packet Sniffer Sensor 1278 (v7)
- Packet Sniffer (Custom) Sensor 1289 (v7)
- PerfCounter Custom Sensor 1299 (v12.x.3)
- PerfCounter IIS Application Pool Sensor 1309 (v12.x.6)
- Ping Sensor 1319 (v7)
- Ping Jitter Sensor 1328 (v8.3.0)
- POP3 Sensor 1337 (v7)
- Port Sensor 1346 (v7)
- Port Range Sensor 1355 (v12.x.4)
- PostgreSQL Sensor 1363 (v14.x.12)
- Probe Health Sensor 1378 (v9.1.0)
- Python Script Advanced Sensor 1385 (v15.x.19)
- QoS (Quality of Service) One Way Sensor 1395 (v7)
- QoS (Quality of Service) Round Trip Sensor 1403 (v9.1.0)
- RADIUS v2 Sensor 1413 (v14.x.13)
- RDP (Remote Desktop) Sensor 1422 (v7)
- Sensor Factory Sensor 1438 (v7)
- sFlow Sensor 1457 (v7)
- sFlow (Custom) Sensor 1469 (v7)
- SFTP Secure File Transfer Protocol Sensor 1481 (v12.x.6)
- Share Disk Free Sensor 1430 (v7)
- SIP Options Ping Sensor 1490 (v12.x.1)
- SMTP Sensor 1499 (v7)
- SMTP&IMAP Round Trip Sensor 1508 (v7)
- SMTP&POP3 Round Trip Sensor 1519 (v7)
- SNMP APC Hardware Sensor 1530 (v9.1.0)
- SNMP Buffalo TS System Health Sensor 1539 (v17.1.29)
- SNMP Cisco ADSL Sensor 1548 (v12.x.1)
- SNMP Cisco ASA VPN Connections Sensor 1556 (v12.x.1)

- SNMP Cisco ASA VPN Traffic Sensor 1566 (v12.x.1)
- SNMP Cisco ASA VPN Users Sensor 1577 (v12.x.5)
- SNMP Cisco CBQoS Sensor 1587 (v13.x.5)
- SNMP Cisco System Health Sensor 1596 (v12.x.4)
- SNMP Cisco UCS Blade Sensor 1605 (v14.x.14)
- SNMP Cisco UCS Chassis Sensor 1614 (v13.x.8)
- SNMP Cisco UCS Physical Disk Sensor 1623 (v14.1.10)
- SNMP Cisco UCS System Health Sensor 1632 (v13.x.8)
- SNMP CPU Load Sensor 1641 (v12.x.4)
- SNMP Custom Sensor 1649 (v7)
- SNMP Custom Advanced Sensor 1658 (v15.x.18)
- SNMP Custom String Sensor 1668 (v9.1.0)
- SNMP Custom String Lookup Sensor 1679 (v14.x.14)
- SNMP Custom Table Sensor 1689 (v15x.18)
- SNMP Dell EqualLogic Logical Disk Sensor 1701 (v16.x.24)
- SNMP Dell EqualLogic Member Health Sensor 1710 (v16.x.24)
- SNMP Dell EqualLogic Physical Disk Sensor 1720 (v16.x.24)
- SNMP Dell Hardware Sensor 1729 (v7)
- SNMP Dell PowerEdge Physical Disk Sensor 1738 (v12.x.4)
- SNMP Dell PowerEdge System Health Sensor 1747 (v12.x.4)
- SNMP Disk Free Sensor 1757 (v12.x.4)
- SNMP Hardware Status Sensor 1766 (v13.x.5)
- SNMP HP BladeSystem Blade Sensor 1775 (v15.x.18)
- SNMP HP BladeSystem Enclosure System Health Sensor 1783 (v15.x.18)
- SNMP HP LaserJet Hardware Sensor 1791 (v9.1.0)
- SNMP HP ProLiant Logical Disk Sensor 1800 (v12.x.6)
- SNMP HP ProLiant Memory Controller Sensor 1809 (v12.x.6)
- SNMP HP ProLiant Network Interface Sensor 1818 (v12.x.4)
- SNMP HP ProLiant Physical Disk Sensor 1827 (v12.x.6)
- SNMP HP ProLiant System Health Sensor 1836 (v12.x.4)
- SNMP IBM System X Logical Disk Sensor 1845 (v13.x.4)
- SNMP IBM System X Physical Disk Sensor 1854 (v13.x.4)
- SNMP IBM System X Physical Memory Sensor 1863 (v13.x.4)
- SNMP IBM System X System Health Sensor 1872 (v13.x.4)

- SNMP interSeptor Pro Environment Sensor 1881 (v14.1.10)
- SNMP Juniper NS System Health Sensor 1889 (v15.2.16)
- SNMP LenovoEMC Physical Disk Sensor 1897 (v13.x.8)
- SNMP LenovoEMC System Health Sensor 1905 (v13.x.8)
- SNMP Library Sensor 1912 (v7)
- SNMP Linux Disk Free Sensor 1924 (v8.1.0)
- SNMP Linux Load Average Sensor 1936 (v8.1.0)
- SNMP Linux Meminfo Sensor 1944 (v8.1.0)
- SNMP Linux Physical Disk Sensor 1952 (v13.x.5)
- SNMP Memory Sensor 1961 (v12.x.4)
- SNMP NetApp Disk Free Sensor 1970 (v12.x.3)
- SNMP NetApp Enclosure Sensor 1979 (v12.x.4)
- SNMP NetApp I/O Sensor 1988 (v12.x.3)
- SNMP NetApp License Sensor 1997 (v12.x.4)
- SNMP NetApp Logical Unit Sensor 2005 (v13.x.7)
- SNMP NetApp Network Interface Sensor 2014 (v12.x.3)
- SNMP NetApp System Health Sensor 2022 (v12.x.3)
- SNMP Poseidon Environment Sensor 2031 (v13.x.5)
- SNMP Printer Sensor 2039 (v14.x.11)
- SNMP QNAP Logical Disk Sensor 2047 (v13.x.4)
- SNMP QNAP Physical Disk Sensor 2056 (v13.x.4)
- SNMP QNAP System Health Sensor 2065 (v13.x.4)
- SNMP RMON Sensor 2073 (v12.x.1)
- SNMP SonicWALL System Health Sensor 2083 (v13.x.5)
- SNMP SonicWALL VPN Traffic Sensor 2091 (v13.x.6)
- SNMP Synology Logical Disk Sensor 2100 (v13.x.4)
- SNMP Synology Physical Disk Sensor 2108 (v13.x.4)
- SNMP Synology System Health Sensor 2116 (v13.x.4)
- SNMP System Uptime Sensor 2124 (v7)
- SNMP Traffic Sensor 2132 (v7)
- SNMP Trap Receiver Sensor 2143 (v7)
- SNMP Windows Service Sensor 2155 (v13.x.8)
- SNTP Sensor 2163 (v8.1.0)
- SSH Disk Free Sensor 2170 (v8.1.0)

- SSH INodes Free Sensor 2183 (v8.1.1)
- SSH Load Average Sensor 2193 (v8.1.0)
- SSH Meminfo Sensor 2203 (v8.1.0)
- SSH Remote Ping Sensor 2213 (v12.x.1)
- SSH SAN Enclosure Sensor 2223 (v14.x.12)
- SSH SAN Logical Disk Sensor 2233 (v14.1.9)
- SSH SAN Physical Disk Sensor 2244 (v14.1.9)
- SSH SAN System Health Sensor 2255 (v14.1.9)
- SSH Script Sensor 2266 (v12.x.1)
- SSH Script Advanced Sensor 2278 (v12.x.6)
- SSL Certificate Sensor 2289 (v15.x.19)
- SSL Security Check Sensor 2299 (v14.x.12)
- Syslog Receiver Sensor 2309 (v7)
- System Health Sensor 2321 (v9.1.0)
- TFTP Sensor 2327 (v8.1.0)
- Traceroute Hop Count Sensor 2335 (v8.3.0)
- VMware Datastore (SOAP) Sensor 2344 (v15.x.19)
- VMware Host Hardware (WBEM) Sensor 2354 (v8.1.0)
- VMware Host Hardware Status (SOAP) Sensor 2362 (v12.x.1)
- VMware Host Performance (SOAP) Sensor 2372 (v12.x.1)
- VMware Virtual Machine (SOAP) Sensor 2382 (v7)
- Windows CPU Load Sensor 2393 (v7)
- Windows IIS 6.0 SMTP Received Sensor 2403 (v8.1.0)
- Windows IIS 6.0 SMTP Sent Sensor 2412 (v8.1.0)
- Windows IIS Application Sensor 2421 (v12.x.1)
- Windows MSMQ Queue Length Sensor 2430 (v8.3.0)
- Windows Network Card Sensor 2441 (v7)
- Windows Pagefile Sensor 2452 (v12.x.4)
- Windows Physical Disk I/O Sensor 2461 (v16.x.24)
- Windows Print Queue Sensor 2472 (v8.3.0)
- Windows Process Sensor 2483 (v7)
- Windows System Uptime Sensor 2493 (v8.1.0)
- Windows Updates Status (Powershell) Sensor 2502 (v13.x.6)
- WMI Custom Sensor 2512 (v7)

- WMI Custom String Sensor 2522 (v12.x.4)
- WMI Event Log Sensor 2533 (v7)
- WMI Exchange Server Sensor 2544 (v9)
- WMI Exchange Transport Queue Sensor 2554 (v12.x.1)
- WMI File Sensor 2564 (v7)
- WMI Free Disk Space (Multi Disk) Sensor 2573 (v7)
- WMI HDD Health Sensor 2585 (v12.x.1)
- WMI Logical Disk I/O Sensor 2596 (v16.x.24)
- WMI Memory Sensor 2606 (v7)
- WMI Microsoft SQL Server 2005 Sensor 2615 (v8.1.0)
- WMI Microsoft SQL Server 2008 Sensor 2628 (v8.1.0)
- WMI Microsoft SQL Server 2012 Sensor 2640 (v12.x.6)
- WMI Microsoft SQL Server 2014 Sensor 2652 (v14.x.13)
- WMI Microsoft SQL Server 2016 Sensor 2664 (v16.x.26)
- WMI Remote Ping Sensor 2676 (v12.x.1)
- WMI Security Center Sensor 2685 (v9)
- WMI Service Sensor 2695 (v7)
- WMI Share Sensor 2705 (v8.1.0)
- WMI SharePoint Process Sensor 2715 (v12.x.1)
- WMI Terminal Services (Windows 2008+) Sensor 2724 (v8.1.0)
- WMI Terminal Services (Windows XP/Vista/2003) Sensor 2732 (v8.1.0)
- WMI UTC Time Sensor 2740 (v9.2.0)
- WMI Vital System Data (V2) Sensor 2748 (v7)
- WMI Volume Sensor 2758 (v7)
- WSUS Statistics Sensor 2767 (v9.1.0)

Script World Sensors

In addition to the built-in sensors, you can create your own sensors. Just write a script or a program and use it with a custom sensor 406. There are already many free, useful scripts, plugins, and add-ons for PRTG in the **PRTG Script World**.You can directly open the Script World from the Add Sensor 288 dialog in the PRTG web interface.

- Active Fileshare Sessions
- Active Lync Users, Inbound/Outbound Calls
- Active Windows Users
- AD Group Membership

- Advanced Exchange Server Metrics
- AllNet UPS
- Altaro Hyper-V Backup Monitoring
- Amazon AWS Costs
- APC Battery Replacement
- Atlantis ILIO
- Citrix Environments
- DICOM and HL7
- Dynamic Windows Processes
- Exim Queue Length
- Find Groups and Devices with Auto-Discovery Enabled
- Google Search Appliance
- Historic Windows Events
- HP ProCurve Switch Version and Model
- HTTP Return Codes
- Linux Services
- Locked AD Users
- Microsoft Active Cluster Nodes
- Monitoring Automatic Services
- Monitor BGP Peer Status
- Monitor Users Logged in to PRTG
- Monitor Website Login
- Monitoring Linux Distributions Incompatible with the SSH Disk Free Sensor
- Monitoring the IP Addresses of Hops
- MySQL Replication
- MySQL Table Fragmentation
- RabbitMQ Queues & Exchanges
- SAP Database Monitoring
- SCVMM - Hyper-V and Virtual Machines
- TXT DNS Records Monitoring
- Veeam Backup and Replication
- Windows Registry Value

Please go to https://www.paessler.com/script-world and follow the instructions there to use these sensors.

More

Not find what you were looking for? Have a look at the Additional Sensor Types (Custom Sensors) 2778 section.

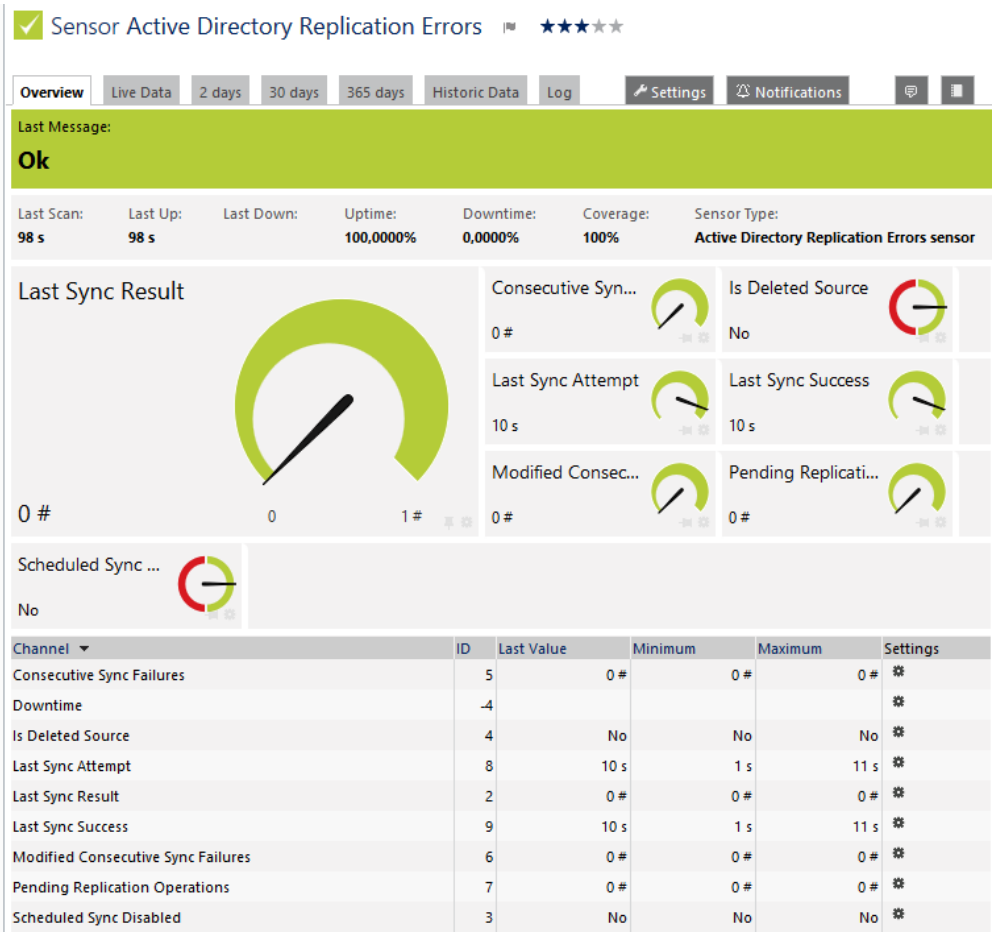
7.8.2 Active Directory Replication Errors Sensor

The Active Directory Replication Errors sensor checks a Windows Domain Controller (DC) for replication errors.

It can show the following:

- Number of consecutive sync failures
- If the source is deleted
- If the scheduled sync is disabled
- Time of the last sync attempt
- Result of the last sync
- Time of the last sync success
- Number of modified consecutive sync failures
- Number of pending replication operations

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Active Directory Replictaion Errors Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/active_directory_replication_errors.png

Remarks

- The device you add the sensor to must be a Domain Controller (DC).
- Requires 409 valid Windows domain credentials in the settings of the parent device 365.
- Requires 409 the probe system to be part of the domain whose Active Directory you monitor.
- Requires 409 .NET 4.0 or higher on the probe system. If the sensor shows the error PE087, please additionally install .NET 3.5 on the probe system.
- We recommend Windows 2012 R2 on the probe system for best performance of this sensor.
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.
- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Requirement: .NET Framework

This sensor type requires the Microsoft .NET Framework to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the remote probe 3196. If the framework is missing, you cannot create this sensor.

Required .NET version (with latest updates): .NET 4.0 (Client Profile is sufficient), .NET 4.5, or .NET 4.6.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/60543

Requirement: Member of Windows Domain

This sensor only works if the computer running the PRTG probe is part of the domain whose Active Directory you want to monitor. The probe runs either on the local system (on every node, if on a cluster probe), or on another system as remote probe 3196. If this requirement is not met, the sensor will not work. You have to add the sensor to a device that represents your Domain Controller (DC) in PRTG.

Requirement: Windows Credentials

Requires credentials for Windows systems to be defined for the device you want to use the sensor on. In the parent device's 365 **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

If you use local credentials, please make sure that the same Windows user accounts (with the same username and password) exist on both the system running the PRTG probe and the target computer. Otherwise the sensor cannot connect correctly.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the replications you want to monitor. PRTG creates one sensor for each replication neighbor you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SENSOR SETTINGS

Replication Neighbor	Select the replication neighbor whose replication you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SETTINGS

Replication Neighbor	Shows the replication neighbor whose replication this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

DEBUG OPTIONS

Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section **Data Storage** 3226. You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel.

SENSOR DISPLAY

	▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. ⓘ This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.

SCANNING INTERVAL

- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: Which .NET version does PRTG require?

- https://kb.paessler.com/en/topic/60543

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

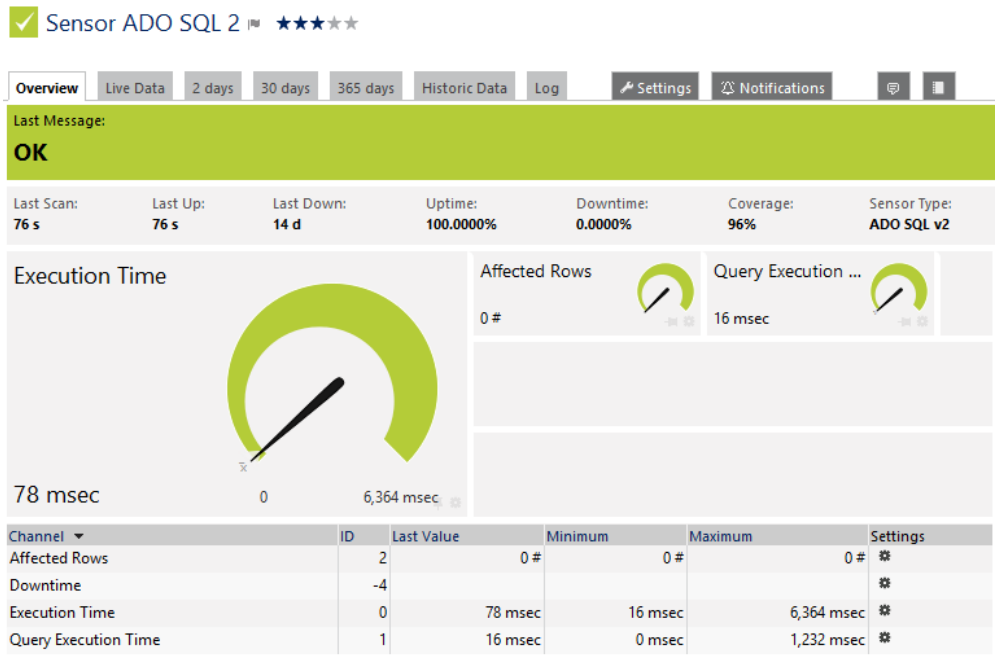
For more general information about settings, please see the **Object Settings** 188 section.

7.8.3 ADO SQL v2 Sensor

The ADO SQL v2 sensor monitors a database using an ActiveX Data Objects (ADO) connection and executes a Structured Query Language (SQL) query. It can monitor any data source that is available via OLE DB (Object Linking and Embedding, Database) or ODBC (Open Database Connectivity).

It can show the following:

- Execution time of the whole request (including connection buildup, query execution, transaction handling, disconnection)
- Execution time of the given query
- Number of rows that were addressed by the query (including select statements if you process data tables)
- It can also process the data table and show defined values in individual channels.



ADO SQL v2 Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/ado-sql-v2.png

Remarks

- Requires 1136 .NET 4.0 on the probe system.
- Define credentials, custom port (if required), and timeout in settings section **Credentials for Database Management Systems** 370 of the parent device, or in the settings of a group or probe above.
- PRTG Manual: **Monitoring Databases** 3120 (includes an example 3121 for channel value selection)

- Knowledge Base: How to setup the SQL v2 sensors in PRTG? Is there a guide?
- Knowledge Base: How can I monitor strings from an SQL database and show a sensor status depending on it?
- Knowledge Base: How can I monitor error tables in SQL databases?
- Your SQL query must be stored in a file on the system of the probe the sensor is created on. If you use it on a remote probe, store the file on the system running the remote probe. In a cluster setup, copy the file to every cluster node.
- Save the SQL script with the query into the **\Custom Sensors\sql\adosql** subfolder of your PRTG installation. See manual section **Data Storage** 3226 for more information about how to find this path.
- If you use an ODBC connection, you have to define the ODBC connection in the Windows ODBC Connection Manager first. If it is a 64-bit Windows, you need to define the ODBC connection as an ODBC 32-bit connection.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Requirement: .NET Framework

This sensor type requires the Microsoft .NET Framework to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the remote probe 3196. If the framework is missing, you cannot create this sensor.

Required .NET version (with latest updates): .NET 4.0 (Client Profile is sufficient), .NET 4.5, or .NET 4.6.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/60543

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DATABASE SPECIFIC

Connection String	Enter the string that the sensor will use to connect to the database. For example, a connection string can look like this: Provider=SQLOLEDB.1;Data Source=10.0.0.200\SQLEXPRESS;User ID=user;Password=userpass;Initial Catalog=Northwind For more information on how to build connection strings, please see **More** 432 section below. For ODBC connections, you need to enter MSDASQL as provider, for example Provider=MSDASQL;DSN=_my_odbc_sqlserver. You can use the placeholders %dbloginuser and %dbloginpassword here. PRTG will replace them with the **Credentials for Database Management Systems** 370 of the parent device.

DATA

SQL Query File	Select an SQL script file that includes a valid SQL statement to execute on the server. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew. The script will be executed with every scanning interval. The list contains SQL scripts from the database management system specific **\Custom Sensors\sql** subfolder of your PRTG installation. Store your script there. If used on a remote probe, the file must be stored on the system running the remote probe. If used on a cluster probe, you must store the file on all servers running a cluster node! For more information on how to find this path, please see **Data Storage** 3226 section. By default, there is the demo script **Demo Serveruptime.sql** available that you can use to monitor the uptime of the target server. For example, a correct expression in the file could be: SELECT AVG (UnitPrice) FROM Products. If you want to use transactions, separate the individual steps with semicolons ";". Please be aware that with each request, the full result set will be transferred, so use filters and limits in your query. You can use the following placeholders in your query file to have them replaced by an input parameter: ▪ Microsoft SQL, MySQL, PostgreSQL: **@prtg** ▪ Oracle SQL: **:prtg** ▪ ADO SQL: **?** (question mark) This is useful if you have various SQL sensors with queries that differ in only one parameter.
Use Input Parameter	Define if you want to pass a parameter to your SQL query file. This will replace the placeholder %prtg (Microsoft SQL, MySQL, PostgreSQL), or :prtg (Oracle SQL), or ? (ADO SQL) in the SQL query. Choose between: ▪ **Don't use input parameter (default)**: Execute the SQL query file without using placeholders. ▪ **Use input parameter**: Execute an SQL query file that contains a placeholder. Provide the parameter you want to use in the query below.
Input Parameter	This field is only visible if you choose **Use input parameter** above. Enter the parameter you want to pass to the SQL query file. This parameter replaces the placeholder %prtg or :prtg or ? in the SQL query.

DATA

	You can also use PRTG placeholders for custom sensors (command line parameters) as input parameter, for example, %sensorid or %deviceid. For details, see **Application Programming Interface (API) Definition** 3174. Provide strings as they are and do not surround them with quotation marks. PRTG will correctly insert string parameters into the query automatically.
Use Transaction	Define if you want to use transactions and if they will affect the database content. Choose between: ▪ **Don't use transaction (default)**: No transactions will be executed. ▪ **Use transaction and always rollback**: Choose this option to ensure that no data in the database will be changed by the query. In the SQL query file, separate the single steps of the transaction with semicolons. ▪ **Use transaction and commit on success**: Choose this option to perform changes on the database with the query. The changes will only apply if all execution steps succeed without any errors. In the SQL query file, separate the single steps of the transaction with semicolons.
Data Processing	Define if you want to process data from the database. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew. Choose between: ▪ **Just execute the query**: If you select this option, the sensor will only show information about the number of affected rows and the execution time of the query. Affected rows are rows that were changed somehow with the query (for example, created, deleted, edited). ▪ **Count table rows**: Choose this option if you perform a SELECT statement and want to monitor how many rows of the data table this statement returns. ▪ **Process data table**: Select this option to read and analyze the queried data table. If you select this option, the sensor will count rows with SELECT statements as well.
Handle DBNull in Channel Values as	This setting is only visible if you select **Process data table** above. Define the sensor behavior if DBNull is returned by the query. Choose between: ▪ **Error**: The sensor will show a **Down** status if DBNull is reported. ▪ **Number 0**: The sensor will recognize the result DBNull as a valid value and interpret it as the number 0.

DATA

Select Channel Value by	This setting is only visible if you select **Process data table** above. Define how the desired cell in the database table will be selected. This is necessary to configure the cells that will be used in the sensor channels. Choose between: ▪ **Column number**: The channel value will be determined by using the value in row 0 of the column whose number you specify below. ▪ **Column name**: The channel value will be determined by using the value in row 0 of the column whose name you specify below. ▪ **Row number**: The channel value will be determined by using the value in column 0 of the row whose number you specify below. ▪ **Key value pair**: The channel value will be determined by searching in column 0 for the key you specify below and returning the value in column 1 of the same row where the key value was found. The option you choose here also defines the method to optionally determine a value for the sensor message. For details, see setting **Use Data Table Value in Sensor Message** below. Please see manual section **Monitoring Databases** 3120 for an example 3121 for channel value selection.
Sensor Channel #x	This setting is only visible if you select **Process data table** above. You can define up to 10 different channels for the data processing of this sensor. You have to define at least one data channel if you process the data table, so you will see all available settings for Channel #1 without enabling it manually. For all other possible channels, choose between: ▪ **Disable**: This channel will not be added to the sensor. ▪ **Enable**: This channel will be added to the sensor. Define the settings as described above. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Sensor Channel #x Name	This setting is only visible if you select **Process data table** above. Enter a unique name for the channel. Please enter a string. Channels will be generated dynamically with this name as identifier. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

DATA

Sensor Channel #x Column Number	This setting is only visible if you select **Column number** above. Provide the number of the column which will be used to determine the channel value in row 0. Please enter an integer value.
Sensor Channel #x Column Name	This setting is only visible if you select **Column number** above. Provide the name of the column which will be used to determine the channel value in row 0. Please enter a string.
Sensor Channel #x Row Number	This setting is only visible if you select **Row number** above. Provide the number of the row which will be used to determine the channel value in column 0. Please enter an integer value.
Sensor Channel #x Key	This setting is only visible if you select **Key value pair** above. Provide the key to search for in column 0 of the data table. The value in column 1 of the same row where the key value was found will be used to determine the channel value. Please enter a string.
Sensor Channel #x Mode	This setting is only visible if you select **Process data table** above. Define how to display the determined value in the channel. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew. Choose between: ▪ **Absolute (recommended)**: Shows the value as the sensor retrieves it from the data table. ▪ **Difference**: The sensor calculates and shows the difference between the last and the current value returned from the data table.
Sensor Channel #x Unit	This setting is only visible if you select **Process data table** above. Define the unit of the channel value. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew. Choose between: ▪ BytesBandwidth ▪ BytesMemory ▪ BytesDisk ▪ Temperature ▪ Percent ▪ TimeResponse ▪ TimeSeconds ▪ TimeHours

DATA

- Count
- CPU
- BytesFile
- SpeedDisk
- SpeedNet
- Custom
- Value Lookup

For more information about the available units, please refer to the PRTG Application Programming Interface (API) Definition 3174 for custom sensors.

To use lookups 3183 with this channel, choose **Value Lookup** and select your lookup file below. Do not use **Custom** for using lookups with this sensor!

Sensor Channel #x Custom Unit

This setting is only visible if you select **Custom** above. Define a unit for the channel value. Please enter a string.

Sensor Channel #x Value Lookup

This settings is only visible if you select **Value Lookup** above. Select a lookup 3183 file that you want to use with this channel.

Use Data Table Value in Sensor Message

This setting is only visible if you select **Process data table** above. Define if the sensor message will show a value from the data table. Choose between:

- **Disable**: Do not use a custom sensor message.
- **Enable**: Define a custom sensor message with a defined value of the data table. Define the value selection below.

The method to determine a value for the sensor message is defined in setting **Select Channel Value by** above.

Sensor Message Column Number

This setting is only visible if you select **Column number** and **Use Data Table Value in Sensor Message** above. Enter the number of a column. The sensor message will show the value in row 0 of this column. Please enter an integer value.

Columns and rows start with index 0.

Sensor Message Column Name

This setting is only visible if you select **Column name** and **Use Data Table Value in Sensor Message** above. Enter the name of a column. The sensor message will show the value in row 0 of this column. Please enter a string.

DATA

	Columns and rows start with index 0.
Sensor Message Row Number	This setting is only visible if you select **Row number** and **Use Data Table Value in Sensor Message** above. Enter the number of a row. The sensor message will show value in column 0 of this row. Please enter an integer value. Columns and rows start with index 0.
Sensor Message Key	This setting is only visible if you select **Key value pair** and **Use Data Table Value in Sensor Message** above. Enter a key to search for in column 0 of the data table. The sensor message will show the value in column 1 of the row where the key has been found. Please enter a string. Columns and rows start with index 0.
Sensor Message	This setting is only visible if you select **Use Data Table Value in Sensor Message** above. Define the sensor message. Please enter a string. Use the placeholder {0} at the position where the value will be added. Example: **The message is {0}**
If Sensor Message Changes	Define what this sensor will do when the sensor value changes. You can choose between: ▪ **Ignore changes (default)**: The sensor takes no action on change. ▪ **Trigger 'change' notification**: The sensor sends an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification 2791 whenever the sensor value changes.
Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result.

DATA

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section Data Storage 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: How to setup the SQL v2 sensors in PRTG? Is there a guide?

- https://kb.paessler.com/en/topic/70618

Knowledge Base: How can I monitor strings from an SQL database and show a sensor status depending on it?

- https://kb.paessler.com/en/topic/63259

Knowledge Base: How do I monitor the size of a Microsoft SQL server database?

- https://kb.paessler.com/en/topic/18183

Knowledge Base: How can I monitor error tables in SQL databases?

- https://kb.paessler.com/en/topic/70774

Knowledge Base: Which .NET version does PRTG require?

- https://kb.paessler.com/en/topic/60543

PRTG Manual:

- **Monitoring Databases** 3120

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

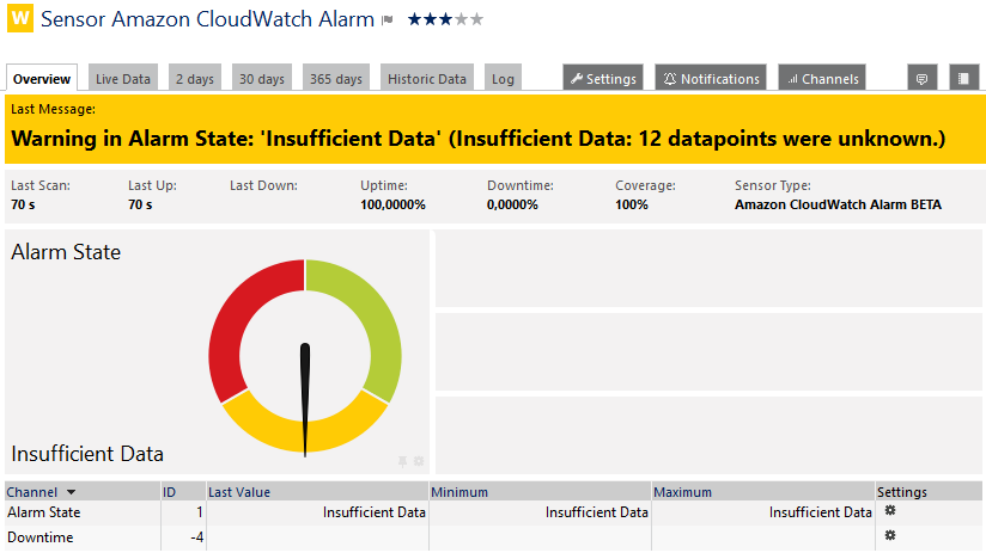
Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.4 Amazon CloudWatch Alarm Sensor

The Amazon CloudWatch Alarm sensor monitors the status of an Amazon CloudWatch alarm. It reads the data via the AWS CloudWatch Application Programming Interface (API).

- This sensor can show the status of a configured alarm for a CloudWatch service.



Amazon CloudWatch Alarm Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/amazon_cloudwatch_alarm.png

Remarks

- The data you see in the sensor message is not necessarily the current data. It merely shows the reason for the current status [163] and why the sensor changed to it. This means for the **Up** status, for example, that this data is as old as the amount of time that has passed since the last alarm disappeared.
- Requires [434] access rights for CloudWatch queries. For details, please see the Knowledge Base: How do I define access rights for Amazon CloudWatch queries?
- Requires [434] .NET 4.0 or higher on the probe system.
- Define **Credentials for Amazon CloudWatch** [372] in settings that are higher in the **Object Hierarchy** [118], for example, in the parent device settings [360].
- Names of configured alarms that you want to monitor must not contain double spaces.
- Amazon will charge you (a small amount) for each "Amazon CloudWatch API Request" query the sensor sends to the Amazon servers. For details, please see the Knowledge Base: How much does Amazon charge for using the CloudWatch API?
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** [3183].

- Currently, this sensor type is in beta status. The methods of operating can change at any time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.

BETA

Requirement: Access Rights for Amazon CloudWatch Queries

The AWS Identity and Access Management (IAM) account that you use with the Amazon CloudWatch sensor needs specific rights to query any metrics. For details, see the Knowledge Base article https://kb.paessler.com/en/topic/38083

Requirement: .NET Framework

This sensor type requires the Microsoft .NET Framework to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the remote probe 3196. If the framework is missing, you cannot create this sensor.

Required .NET version (with latest updates): .NET 4.0 (Client Profile is sufficient), .NET 4.5, or .NET 4.6.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/60543

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

PRTG looks for configured alarms on CloudWatch. This can take up to several minutes.

Select which alarm(s) you want to monitor. PRTG creates one sensor for each alarm you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

AMAZON CLOUDWATCH SPECIFIC

Services	Select the alarms you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

AMAZON CLOUDWATCH SPECIFIC

To better find what you want to monitor, especially in large tables, use the search function in the upper-right corner.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

AMAZON CLOUDWATCH SPECIFIC

Region	Shows the region in which the monitored AWS instance runs. It is one of the following regions: ▪ US East (Northern Virginia) ▪ US West (Oregon) ▪ US West (Northern California) ▪ Canada (Central) ▪ EU (Ireland) ▪ EU (Frankfurt) ▪ Asia Pacific (Singapore) ▪ Asia Pacific (Tokyo) ▪ Asia Pacific (Sydney) ▪ Asia Pacific (Seoul) ▪ Asia Pacific (Mumbai) ▪ South America (Sao Paulo) Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Description	Shows the description of the AWS service instance that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
ID	Shows the ID of the AWS instance that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Result Handling	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result.

AMAZON CLOUDWATCH SPECIFIC

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section **Data Storage** 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.
- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: How do I define access rights for Amazon CloudWatch queries?

- https://kb.paessler.com/en/topic/38083

Knowledge Base: How much does Amazon charge for using the CloudWatch API?

- https://kb.paessler.com/en/topic/37543

Knowledge Base: Which .NET version does PRTG require?

- https://kb.paessler.com/en/topic/60543

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

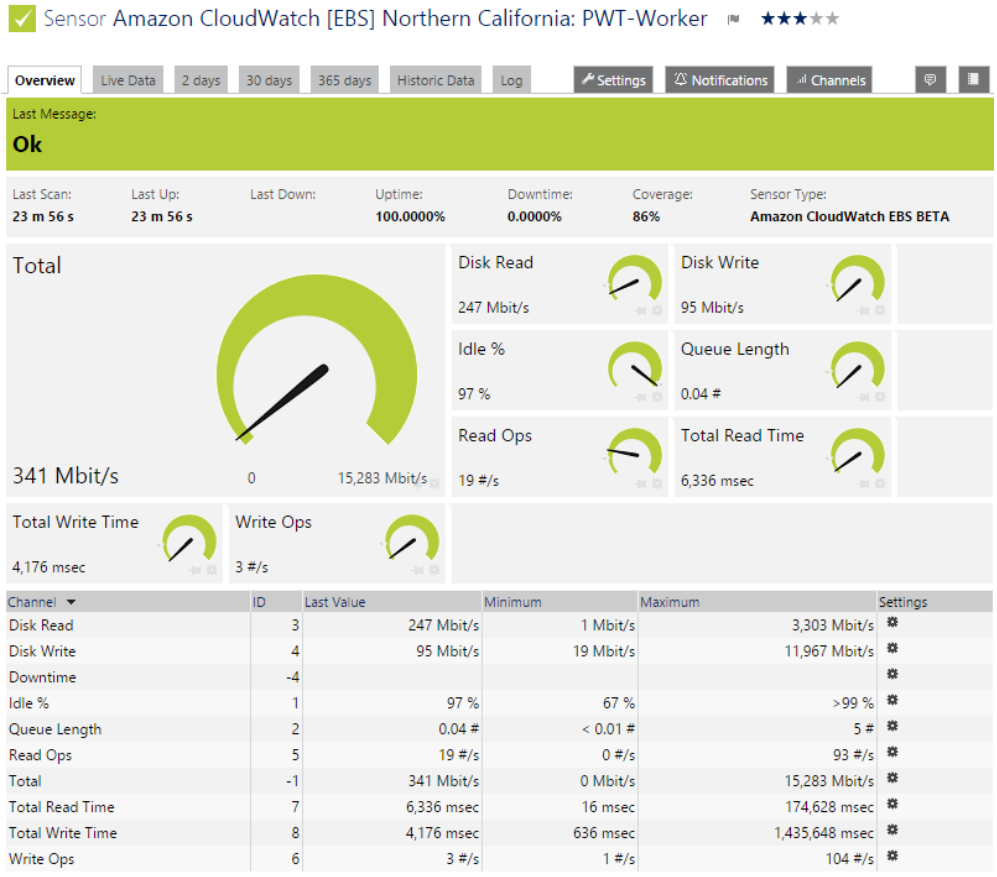
7.8.5 Amazon CloudWatch EBS Sensor

The Amazon CloudWatch EBS sensor monitors the performance of the Amazon Cloud service Elastic Block Store (EBS).

The sensor can show the following:

- Total volume of I/O operations
- Total disk read and write time
- Disk read and write speed
- Number of disk read and write operations per second
- Idle time with no submitted operations
- Number of read and write operations waiting to be completed

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Amazon CloudWatch EBS Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/amazon_cloudwatch_ebs_sensor.png

Remarks

- Requires access rights for CloudWatch queries. For details, please see the Knowledge Base: How do I define access rights for Amazon CloudWatch queries?
- Requires .NET 4.0 or higher on the probe system.
- Define **Credentials for Amazon CloudWatch** 372 in settings that are higher in the **Object Hierarchy** 118, for example, in the parent device settings 360.
- The minimum scanning interval for this sensor is **15 minutes**.
- Configure notification triggers 2791 with a latency of **0 seconds** to receive all notifications for this sensor ([...] for at least 0 seconds).
- This sensor will only show those channels for which it receives data from Amazon. You can check the availability of data in your CloudWatch Console on the AWS website. To know which channels are possible for the various services of this Amazon CloudWatch sensor, see the manual section **Supported Metrics**. If the sensor does not receive data from Amazon for more than 6 hours, it will go into error status.
- To know which dimensions you can monitor, see the manual section **Supported Dimensions**.
- Amazon will charge you (a small amount) for each "Amazon CloudWatch API Request" query the sensor sends to the Amazon servers. Depending on the service, each Amazon CloudWatch sensor sends about 10 to 30 requests with each scanning interval. Last time we checked the Amazon price list, they charged max. US$ 0.014 per 1,000 requests (depending on your region).
  For details, please see the Knowledge Base: How much does Amazon charge for using the CloudWatch API?
- BETA Currently, this sensor type is in beta status. The methods of operating can change at any time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.

Requirement: Access Rights for Amazon CloudWatch Queries

The AWS Identity and Access Management (IAM) account that you use with the Amazon CloudWatch sensor needs specific rights to query any metrics. For details, see section **More** 453.

Requirement: .NET Framework

This sensor type requires the Microsoft .NET Framework to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the remote probe 3196. If the framework is missing, you cannot create this sensor.

Required .NET version (with latest updates): .NET 4.0 (Client Profile is sufficient), .NET 4.5, or .NET 4.6.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/60543

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

PRTG looks for available instances.

This can take up to several minutes.

Select which service instance(s) you want to monitor. PRTG creates one sensor for each instance you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

AMAZON CLOUDWATCH SPECIFIC

Services	Select the Volume you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items. To better find what you want to monitor, especially in large tables, use the search function in the upper-right corner.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets

BASIC SENSOR SETTINGS

	200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

AMAZON CLOUDWATCH SPECIFIC

Region	Shows the region in which the monitored AWS instance runs. It is one of the following regions: ▪ US East (Northern Virginia) ▪ US West (Oregon) ▪ US West (Northern California) ▪ Canada (Central) ▪ EU (Ireland) ▪ EU (Frankfurt) ▪ Asia Pacific (Singapore) ▪ Asia Pacific (Tokyo) ▪ Asia Pacific (Sydney) ▪ Asia Pacific (Seoul) ▪ Asia Pacific (Mumbai) ▪ South America (Sao Paulo)

AMAZON CLOUDWATCH SPECIFIC

	Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Description	Shows the description of the AWS service instance that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
ID	Shows the ID of the AWS instance that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Result Handling	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section **Data Storage** 3226. You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor.

SENSOR DISPLAY

- **Show channels independently (default)**: Show an own graph for each channel.
- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

This sensor type has a fixed minimum scanning interval for performance reasons. You cannot run the sensor in shorter intervals than this minimum interval. Consequently, shorter scanning intervals as defined in **System Administration—Monitoring** 2955 are not available for this sensor.

For Amazon CloudWatch sensors, the minimum scanning interval is **15 minutes**.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

Supported Metrics

AMAZON CLOUDWATCH METRICS

Elastic Block Store (EBS)	▪ VolumeTotalReadTime (Sum) ▪ VolumeTotalWriteTime (Sum) ▪ VolumeReadBytes (Sum) ▪ VolumeWriteOps (Sum) ▪ VolumeReadOps (Sum) ▪ VolumeWriteBytes (Sum) ▪ VolumeConsumedReadWriteOps (Sum) ▪ VolumeQueueLength (Average) ▪ VolumeIdleTime (Sum)

Supported Dimensions

AMAZON CLOUDWATCH DIMENSIONS

Elastic Block Store (EBS)	▪ Volume

More

Knowledge Base: How do I define access rights for Amazon CloudWatch queries?

- https://kb.paessler.com/en/topic/38083

Knowledge Base: How much does Amazon charge for using the CloudWatch API?

- https://kb.paessler.com/en/topic/37543

Knowledge Base: Which .NET version does PRTG require?

- https://kb.paessler.com/en/topic/60543

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

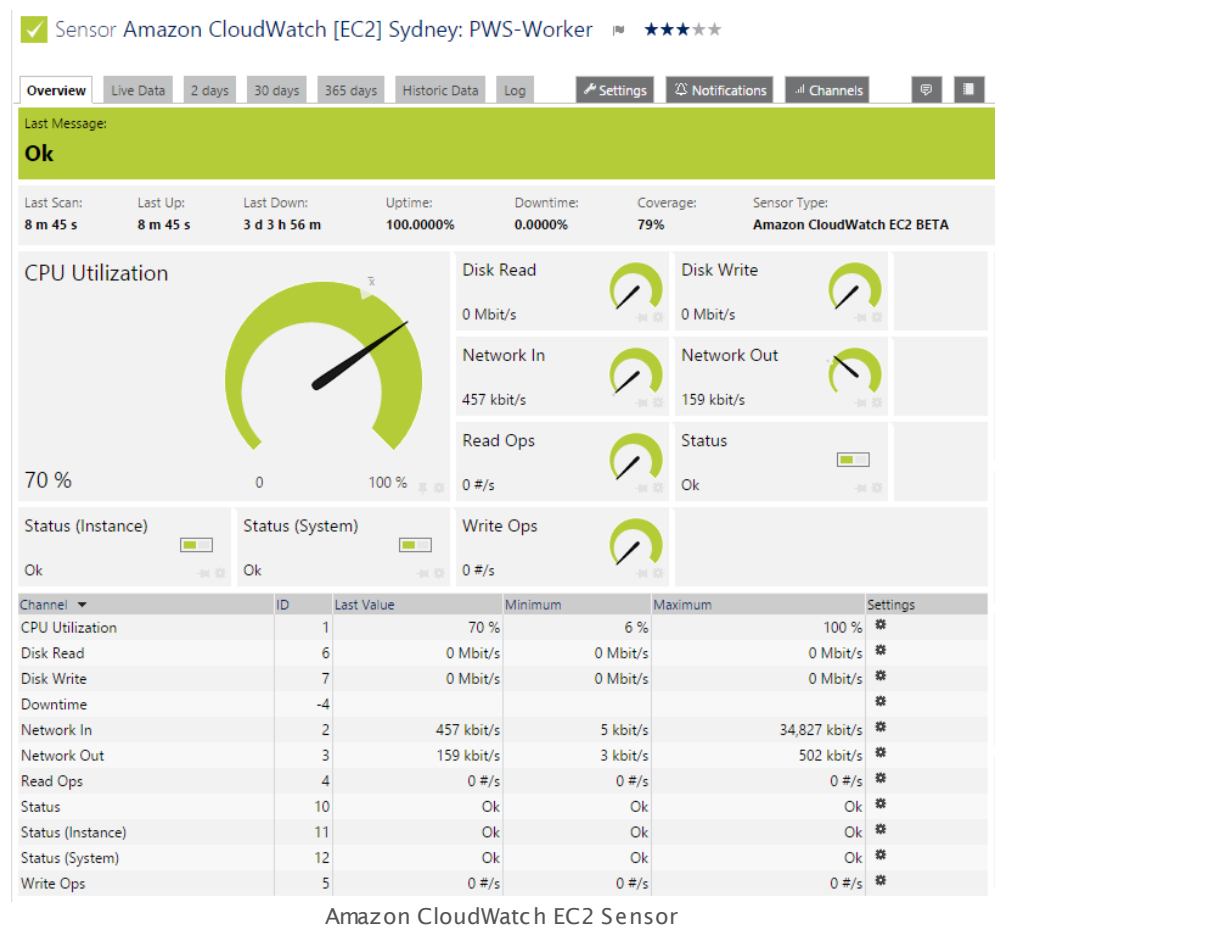
7.8.6 Amazon CloudWatch EC2 Sensor

The Amazon CloudWatch EC2 sensor monitors the performance of the Amazon Cloud service Elastic Cloud Computing (EC2).

The sensor can show the following:

- CPU utilization
- Network load in and out
- Disk I/O:
  - Read and write speed
  - Number of disk read and write operations per second
- CPU credit usage and balance
- EC2 status checks

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Channel	ID	Last Value	Minimum	Maximum	Settings
CPU Utilization	1	70 %	6 %	100 %	
Disk Read	6	0 Mbit/s	0 Mbit/s	0 Mbit/s	
Disk Write	7	0 Mbit/s	0 Mbit/s	0 Mbit/s	
Downtime	-4				
Network In	2	457 kbit/s	5 kbit/s	34,827 kbit/s	
Network Out	3	159 kbit/s	3 kbit/s	502 kbit/s	
Read Ops	4	0 #/s	0 #/s	0 #/s	
Status	10	Ok	Ok	Ok	
Status (Instance)	11	Ok	Ok	Ok	
Status (System)	12	Ok	Ok	Ok	
Write Ops	5	0 #/s	0 #/s	0 #/s	

Amazon CloudWatch EC2 Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/amazon_cloudwatch_ec2_sensor.png

Remarks

- Requires access rights for CloudWatch queries. For details, please see the Knowledge Base: How do I define access rights for Amazon CloudWatch queries?
- Requires .NET 4.0 or higher on the probe system.
- Define **Credentials for Amazon CloudWatch** 372 in settings that are higher in the **Object Hierarchy** 118, for example, in the parent device settings 360.
- The minimum scanning interval for this sensor is **15 minutes**.
- Configure notification triggers 2791 with a latency of **0 seconds** to receive all notifications for this sensor ([...] for at least 0 seconds).
- This sensor will only show those channels for which it receives data from Amazon. You can check the availability of data in your CloudWatch Console on the AWS website. To know which channels are possible for the various services of this Amazon CloudWatch sensor, see the manual section **Supported Metrics**. If the sensor does not receive data from Amazon for more than 6 hours, it will go into error status.
- To know which dimensions you can monitor, see the manual section **Supported Dimensions**.
- Amazon will charge you (a small amount) for each "Amazon CloudWatch API Request" query the sensor sends to the Amazon servers. Depending on the service, each Amazon CloudWatch sensor sends about 10 to 30 requests with each scanning interval. Last time we checked the Amazon price list, they charged max. US$ 0.014 per 1,000 requests (depending on your region).
  For details, please see the Knowledge Base: How much does Amazon charge for using the CloudWatch API?
- BETA Currently, this sensor type is in beta status. The methods of operating can change at any time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.

Requirement: Access Rights for Amazon CloudWatch Queries

The AWS Identity and Access Management (IAM) account that you use with the Amazon CloudWatch sensor needs specific rights to query any metrics. For details, see section **More** 465.

Requirement: .NET Framework

This sensor type requires the Microsoft .NET Framework to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the remote probe 3196. If the framework is missing, you cannot create this sensor.

Required .NET version (with latest updates): .NET 4.0 (Client Profile is sufficient), .NET 4.5, or .NET 4.6.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/60543

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

PRTG looks for available instances.

This can take up to several minutes.

Select which service instance(s) you want to monitor. PRTG creates one sensor for each instance you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

AMAZON CLOUDWATCH SPECIFIC

Services	Select the Instances or Auto Scaling Groups you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items. To better find what you want to monitor, especially in large tables, use the search function in the upper-right corner.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

AMAZON CLOUDWATCH SPECIFIC

Region	Shows the region in which the monitored AWS instance runs. It is one of the following regions: ▪ US East (Northern Virginia) ▪ US West (Oregon) ▪ US West (Northern California) ▪ Canada (Central) ▪ EU (Ireland) ▪ EU (Frankfurt) ▪ Asia Pacific (Singapore) ▪ Asia Pacific (Tokyo) ▪ Asia Pacific (Sydney) ▪ Asia Pacific (Seoul)

AMAZON CLOUDWATCH SPECIFIC

- Asia Pacific (Mumbai)
- South America (Sao Paulo)

Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Description

Shows the description of the AWS service instance that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

ID

Shows the ID of the AWS instance that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Result Handling

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result**: Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section Data Storage 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

Detailed Monitoring

Choose whether you would like to import more or less detailed monitoring data from the AWS API. Choose between

- **Enabled:** You get 1 dataset per minute.
- **Disabled (default):** You get 1 dataset per 5 minutes.

To use detailed monitoring in PRTG, you must also activate it for your monitored instance in the AWS web console.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

This sensor type has a fixed minimum scanning interval for performance reasons. You cannot run the sensor in shorter intervals than this minimum interval. Consequently, shorter scanning intervals as defined in **System Administration—Monitoring** 2955 are not available for this sensor.

For Amazon CloudWatch sensors, the minimum scanning interval is **15 minutes**.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

Supported Metrics

AMAZON CLOUDWATCH METRICS

Elastic Compute Cloud (EC2)	▪ CPUUtilization (Average) ▪ NetworkIn (Sum) ▪ NetworkOut (Sum) ▪ DiskReadBytes (Sum) ▪ DiskReadOps (Sum) ▪ DiskWriteBytes (Sum) ▪ DiskWriteOps (Sum) ▪ CPUCreditUsage (Average) ▪ CPUCreditBalance (Average) ▪ StatusCheckFailed (Maximum) ▪ StatusCheckFailed_Instance (Maximum) ▪ StatusCheckFailed_System (Maximum)

Supported Dimensions

AMAZON CLOUDWATCH DIMENSIONS

Elastic Compute Cloud (EC2)	▪ Instance ▪ Auto Scaling Group

More

Knowledge Base: How do I define access rights for Amazon CloudWatch queries?

- https://kb.paessler.com/en/topic/38083

Knowledge Base: How much does Amazon charge for using the CloudWatch API?

- https://kb.paessler.com/en/topic/37543

Knowledge Base: Which .NET version does PRTG require?

- https://kb.paessler.com/en/topic/60543

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.7 Amazon CloudWatch ElastiCache Sensor

The Amazon CloudWatch ElastiCache sensor monitors the performance of the Amazon Cloud service ElastiCache.

The sensor can show the following:

- CPU utilization
- Memory
- Cache I/O
- Network I/O
- Cache Statistics

See **Supported Metrics** 477 for a list of data that this sensor can potentially show in dedicated channels.

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

Channel	ID	Last Value	Minimum	Maximum	Settings
CPU Utilization	10	4 %	1 %	5 %	
Current Connections	11	5,614 #	3,902 #	5,614 #	
Current Items	12	23,161 #	7,240 #	23,161 #	
Downtime	-4				
Evictions	17	0 #	0 #	0 #	
Freeable Memory	18	1,501 MByte	1,489 MByte	1,559 MByte	
Network In	23	266 kbit/s	5 kbit/s	462 kbit/s	
Network Out	24	250 kbit/s	18 kbit/s	449 kbit/s	
New Connections	25	3 #	0 #	46 #	
Reclaimed	27	197 #	0 #	9,606 #	
Swap Usage	28	0 MByte	0 MByte	0 MByte	

Amazon CloudWatch ElastiCache Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/amazon_cloudwatch_elasticache_sensor.png

Remarks

- Requires access rights for CloudWatch queries. For details, please see the Knowledge Base: How do I define access rights for Amazon CloudWatch queries?
- Requires .NET 4.0 or higher on the probe system.
- Define **Credentials for Amazon CloudWatch** 372 in settings that are higher in the **Object Hierarchy** 118, for example, in the parent device settings 360.
- The minimum scanning interval for this sensor is **15 minutes**.
- Configure notification triggers 2791 with a latency of **0 seconds** to receive all notifications for this sensor ([...] for at least 0 seconds).
- This sensor will only show those channels for which it receives data from Amazon. You can check the availability of data in your CloudWatch Console on the AWS website. To know which channels are possible for the various services of this Amazon CloudWatch sensor, see the manual section **Supported Metrics**. If the sensor does not receive data from Amazon for more than 6 hours, it will go into error status.
- To know which dimensions you can monitor, see the manual section **Supported Dimensions**.
- Amazon will charge you (a small amount) for each "Amazon CloudWatch API Request" query the sensor sends to the Amazon servers. Depending on the service, each Amazon CloudWatch sensor sends about 10 to 30 requests with each scanning interval. Last time we checked the Amazon price list, they charged max. US$ 0.014 per 1,000 requests (depending on your region).
  For details, please see the Knowledge Base: How much does Amazon charge for using the CloudWatch API?
- Currently, this sensor type is in beta status. The methods of operating can change at any time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.

BETA

Requirement: Access Rights for Amazon CloudWatch Queries

The AWS Identity and Access Management (IAM) account that you use with the Amazon CloudWatch sensor needs specific rights to query any metrics. For details, see section **More** 478.

Requirement: .NET Framework

This sensor type requires the Microsoft .NET Framework to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the remote probe 3196. If the framework is missing, you cannot create this sensor.

Required .NET version (with latest updates): .NET 4.0 (Client Profile is sufficient), .NET 4.5, or .NET 4.6.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/60543

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

PRTG looks for available instances.

This can take up to several minutes.

Select which service instance(s) you want to monitor. PRTG creates one sensor for each instance you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

AMAZON CLOUDWATCH SPECIFIC

Services	Select the Cache Clusters or Cache Cluster Nodes you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items. To better find what you want to monitor, especially in large tables, use the search function in the upper-right corner.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

AMAZON CLOUDWATCH SPECIFIC

Region	Shows the region in which the monitored AWS instance runs. It is one of the following regions: ▪ US East (Northern Virginia) ▪ US West (Oregon) ▪ US West (Northern California) ▪ Canada (Central) ▪ EU (Ireland) ▪ EU (Frankfurt) ▪ Asia Pacific (Singapore) ▪ Asia Pacific (Tokyo) ▪ Asia Pacific (Sydney) ▪ Asia Pacific (Seoul)

AMAZON CLOUDWATCH SPECIFIC

- Asia Pacific (Mumbai)
- South America (Sao Paulo)

Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Description

Shows the description of the AWS service instance that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

ID

Shows the ID of the AWS instance that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Result Handling

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result**: Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.

  For more information on how to find the folder used for storage, see section **Data Storage** 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

SENSOR DISPLAY

Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

This sensor type has a fixed minimum scanning interval for performance reasons. You cannot run the sensor in shorter intervals than this minimum interval. Consequently, shorter scanning intervals as defined in **System Administration—Monitoring** 2955 are not available for this sensor.

For Amazon CloudWatch sensors, the minimum scanning interval is **15 minutes**.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

Supported Metrics

AMAZON CLOUDWATCH METRICS

ElastiCache	▪ CPUUtilization (Average) ▪ CurrConnections (Average) ▪ CurrItems (Average) ▪ NewItems (Sum) ▪ NewConnections (Sum) ▪ FreeableMemory (Average) ▪ UnusedMemory (Average) ▪ SwapUsage (Average) ▪ BytesUsedForCacheItems (Average) ▪ BytesReadIntoMemcached (Sum) ▪ BytesWrittenOutFromMemcached (Sum) ▪ NetworkBytesIn (Sum) ▪ NetworkBytesOut (Sum) ▪ Evictions (Sum) ▪ Reclaimed (Sum) ▪ CasBadval (Sum) ▪ CasHits (Sum) ▪ CasMisses (Sum) ▪ CmdFlush (Sum) ▪ Cmdget (Sum) ▪ Cmdset (Sum) ▪ DecrMisses (Sum) ▪ DecrHits (Sum) ▪ DeleteHits (Sum) ▪ DeleteMisses (Sum) ▪ GetHits (Sum) ▪ GetMisses (Sum) ▪ IncrHits (Sum) ▪ IncrMisses (Sum)

Supported Dimensions

AMAZON CLOUDWATCH DIMENSIONS	
ElastiCache	▪ Cache Cluster ▪ Cache Cluster Node

More

Knowledge Base: How do I define access rights for Amazon CloudWatch queries?

- https://kb.paessler.com/en/topic/38083

Knowledge Base: How much does Amazon charge for using the CloudWatch API?

- https://kb.paessler.com/en/topic/37543

Knowledge Base: Which .NET version does PRTG require?

- https://kb.paessler.com/en/topic/60543

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.8 Amazon CloudWatch ELB Sensor

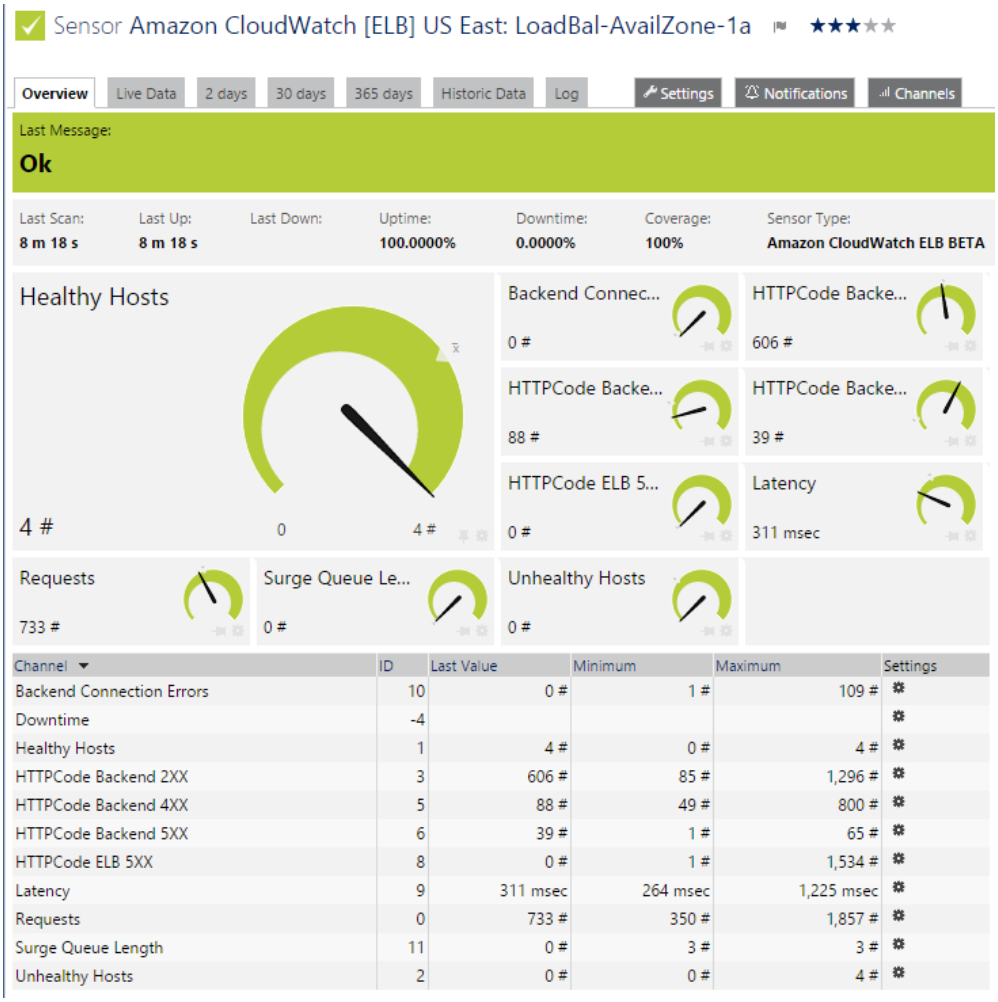
The Amazon CloudWatch ELB sensor monitors the performance of the Amazon Cloud service Elastic Load Balancing (ELB).

The sensor can show the following:

- Host Count
- HTTP Result Count (2xx, 3xx, 4xx, 5xx)
- Latency
- Queue

See **Supported Metrics** 489 for a list of data that this sensor can potentially show in dedicated channels.

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Channel	ID	Last Value	Minimum	Maximum	Settings
Backend Connection Errors	10	0 #	1 #	109 #	
Downtime	-4				
Healthy Hosts	1	4 #	0 #	4 #	
HTTPCode Backend 2XX	3	606 #	85 #	1,296 #	
HTTPCode Backend 4XX	5	88 #	49 #	800 #	
HTTPCode Backend 5XX	6	39 #	1 #	65 #	
HTTPCode ELB 5XX	8	0 #	1 #	1,534 #	
Latency	9	311 msec	264 msec	1,225 msec	
Requests	0	733 #	350 #	1,857 #	
Surge Queue Length	11	0 #	3 #	3 #	
Unhealthy Hosts	2	0 #	0 #	4 #	

Amazon CloudWatch ELB Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/amazon_cloudwatch_elb_sensor.png

Remarks

- Requires access rights for CloudWatch queries. For details, please see the Knowledge Base: How do I define access rights for Amazon CloudWatch queries?
- Requires .NET 4.0 or higher on the probe system.
- Define **Credentials for Amazon CloudWatch** 372 in settings that are higher in the **Object Hierarchy** 118, for example, in the parent device settings 360.
- The minimum scanning interval for this sensor is **15 minutes**.
- Configure notification triggers 2791 with a latency of **0 seconds** to receive all notifications for this sensor ([...] for at least 0 seconds).
- This sensor will only show those channels for which it receives data from Amazon. You can check the availability of data in your CloudWatch Console on the AWS website. To know which channels are possible for the various services of this Amazon CloudWatch sensor, see the manual section **Supported Metrics**. If the sensor does not receive data from Amazon for more than 6 hours, it will go into error status.
- To know which dimensions you can monitor, see the manual section **Supported Dimensions**.
- Amazon will charge you (a small amount) for each "Amazon CloudWatch API Request" query the sensor sends to the Amazon servers. Depending on the service, each Amazon CloudWatch sensor sends about 10 to 30 requests with each scanning interval. Last time we checked the Amazon price list, they charged max. US$ 0.014 per 1,000 requests (depending on your region).
  For details, please see the Knowledge Base: How much does Amazon charge for using the CloudWatch API?
- BETA Currently, this sensor type is in beta status. The methods of operating can change at any time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.

Requirement: Access Rights for Amazon CloudWatch Queries

The AWS Identity and Access Management (IAM) account that you use with the Amazon CloudWatch sensor needs specific rights to query any metrics. For details, see section **More** 489.

Requirement: .NET Framework

This sensor type requires the Microsoft .NET Framework to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the remote probe 3196. If the framework is missing, you cannot create this sensor.

Required .NET version (with latest updates): .NET 4.0 (Client Profile is sufficient), .NET 4.5, or .NET 4.6.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/60543

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

PRTG looks for available instances.

This can take up to several minutes.

Select which service instance(s) you want to monitor. PRTG creates one sensor for each instance you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

AMAZON CLOUDWATCH SPECIFIC

Services	Select the Load Balancers or Availability Zones you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items. To better find what you want to monitor, especially in large tables, use the search function in the upper-right corner.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

AMAZON CLOUDWATCH SPECIFIC

Region	Shows the region in which the monitored AWS instance runs. It is one of the following regions: ▪ US East (Northern Virginia) ▪ US West (Oregon) ▪ US West (Northern California) ▪ Canada (Central) ▪ EU (Ireland) ▪ EU (Frankfurt) ▪ Asia Pacific (Singapore) ▪ Asia Pacific (Tokyo) ▪ Asia Pacific (Sydney) ▪ Asia Pacific (Seoul)

AMAZON CLOUDWATCH SPECIFIC

- Asia Pacific (Mumbai)
- South America (Sao Paulo)

Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Description

Shows the description of the AWS service instance that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

ID

Shows the ID of the AWS instance that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Result Handling

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result**: Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.

  For more information on how to find the folder used for storage, see section **Data Storage** 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

SENSOR DISPLAY

Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

This sensor type has a fixed minimum scanning interval for performance reasons. You cannot run the sensor in shorter intervals than this minimum interval. Consequently, shorter scanning intervals as defined in **System Administration—Monitoring** 2955 are not available for this sensor.

For Amazon CloudWatch sensors, the minimum scanning interval is **15 minutes**.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

Supported Metrics

AMAZON CLOUDWATCH METRICS

Elastic Load Balancing (ELB)	▪ RequestCount (Sum) ▪ SpilloverCount (Sum) ▪ HealthyHostCount (Minimum) ▪ UnHealthyHostCount (Maximum) ▪ BackendConnectionErrors (Sum) ▪ HTTPCode_Backend_2XX (Sum) ▪ HTTPCode_Backend_3XX (Sum) ▪ HTTPCode_Backend_4XX (Sum) ▪ HTTPCode_Backend_5XX (Sum) ▪ HTTPCode_ELB_4XX (Sum) ▪ HTTPCode_ELB_5XX (Sum) ▪ Latency (Average) ▪ SurgeQueueLength (Average)

Supported Dimensions

AMAZON CLOUDWATCH DIMENSIONS

Elastic Load Balancing (ELB)	▪ Load Balancer ▪ Availability Zone

More

Knowledge Base: How do I define access rights for Amazon CloudWatch queries?

▪ https://kb.paessler.com/en/topic/38083

Knowledge Base: How much does Amazon charge for using the CloudWatch API?

▪ https://kb.paessler.com/en/topic/37543

Knowledge Base: Which .NET version does PRTG require?

▪ https://kb.paessler.com/en/topic/60543

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.9 Amazon CloudWatch RDS Sensor

The Amazon CloudWatch RDS sensor monitors the performance of the Amazon Cloud service Relational Database Service (RDS).

The sensor can show the following:

- CPU Utilization
- CPU Credit Usage and CPU Credit Balance
- Memory Usage
- Database I/O
- Network I/O
- Storage information

See **Supported Metrics** 502 for a list of data that this sensor can potentially show in dedicated channels.

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

Channel	ID	Last Value	Minimum	Maximum	Settings
CPU Utilization	1	37 %	30 %	45 %	
Database Connections	2	0 #	0 #	0 #	
DB Read	9	5 KByte	1 KByte	615 KByte	
DB Write	10	61 KByte	53 KByte	116 KByte	
Disk Queue Depth	13	0 #	0 #	0 #	
Downtime	-4				
Free Storage Space	4	101,650 MByte	101,645 MByte	101,665 MByte	
Freeable Memory	3	310 MByte	306 MByte	476 MByte	
Network In	14	4 kbit/s	3 kbit/s	4 kbit/s	
Network Out	15	27 kbit/s	23 kbit/s	28 kbit/s	
Read Latency	7	0 msec	0 msec	2 msec	
Read OPS	5	1 #/s	1 #/s	35 #/s	
Write Latency	8	2 msec	1 msec	5 msec	
Write OPS	6	9 #/s	6 #/s	21 #/s	

Amazon CloudWatch RDS Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/amazon_cloudwatch_rds_sensor.png

Remarks

- Requires access rights for CloudWatch queries. For details, please see the Knowledge Base: How do I define access rights for Amazon CloudWatch queries?
- Requires .NET 4.0 or higher on the probe system.
- Define **Credentials for Amazon CloudWatch** 372 in settings that are higher in the **Object Hierarchy** 118, for example, in the parent device settings 360.
- The minimum scanning interval for this sensor is **15 minutes**.
- Configure notification triggers 2791 with a latency of **0 seconds** to receive all notifications for this sensor ([...] for at least 0 seconds).

- This sensor will only show those channels for which it receives data from Amazon. You can check the availability of data in your CloudWatch Console on the AWS website. To know which channels are possible for the various services of this Amazon CloudWatch sensor, see the manual section **Supported Metrics**. If the sensor does not receive data from Amazon for more than 6 hours, it will go into error status.
- To know which dimensions you can monitor, see the manual section **Supported Dimensions**.
- Amazon will charge you (a small amount) for each "Amazon CloudWatch API Request" query the sensor sends to the Amazon servers. Depending on the service, each Amazon CloudWatch sensor sends about 10 to 30 requests with each scanning interval. Last time we checked the Amazon price list, they charged max. US$ 0.014 per 1,000 requests (depending on your region).
  For details, please see the Knowledge Base: How much does Amazon charge for using the CloudWatch API?
- Currently, this sensor type is in beta status. The methods of operating can change at any time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.

BETA

Requirement: Access Rights for Amazon CloudWatch Queries

The AWS Identity and Access Management (IAM) account that you use with the Amazon CloudWatch sensor needs specific rights to query any metrics. For details, see section **More** 502.

Requirement: .NET Framework

This sensor type requires the Microsoft .NET Framework to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the remote probe 3196. If the framework is missing, you cannot create this sensor.

Required .NET version (with latest updates): .NET 4.0 (Client Profile is sufficient), .NET 4.5, or .NET 4.6.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/60543

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

PRTG looks for available instances.

This can take up to several minutes.

Select which service instance(s) you want to monitor. PRTG creates one sensor for each instance you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

AMAZON CLOUDWATCH SPECIFIC

Services	Select the Engines or Database Instances you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items. To better find what you want to monitor, especially in large tables, use the search function in the upper right corner.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

BASIC SENSOR SETTINGS

	You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

AMAZON CLOUDWATCH SPECIFIC

Region	Shows the region in which the monitored AWS instance runs. It is one of the following regions: ▪ US East (Northern Virginia) ▪ US West (Oregon) ▪ US West (Northern California) ▪ Canada (Central) ▪ EU (Ireland) ▪ EU (Frankfurt) ▪ Asia Pacific (Singapore) ▪ Asia Pacific (Tokyo) ▪ Asia Pacific (Sydney) ▪ Asia Pacific (Seoul) ▪ Asia Pacific (Mumbai) ▪ South America (Sao Paulo) Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Description	Shows the description of the AWS service instance that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

AMAZON CLOUDWATCH SPECIFIC

ID	Shows the ID of the AWS instance that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Result Handling	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section **Data Storage** 3226. You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

SENSOR DISPLAY

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.

SCANNING INTERVAL

- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

This sensor type has a fixed minimum scanning interval for performance reasons. You cannot run the sensor in shorter intervals than this minimum interval. Consequently, shorter scanning intervals as defined in **System Administration—Monitoring** 2955 are not available for this sensor.

For Amazon CloudWatch sensors, the minimum scanning interval is **15 minutes**.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

Supported Metrics

AMAZON CLOUDWATCH METRICS

Relational Database Service (RDS)	▪ CPUUtilization (Average) ▪ CPUCreditUsage (Average) ▪ CPUCreditBalance (Average) ▪ DatabaseConnections (Sum) ▪ FreeableMemory (Sum) ▪ FreeStorageSpace (Average) ▪ SwapUsage (Sum) ▪ BinLogDiskUsage (Sum) ▪ DiskQueueDepth (Sum) ▪ ReplicLag (Average) ▪ ReadIOPS (Sum) ▪ WriteIOPS (Sum) ▪ ReadLatency (Average) ▪ WriteLatency (Average) ▪ ReadThroughput (Sum) ▪ WriteThroughput (Sum) ▪ NetworkReceiveThroughput (Sum) ▪ NetworkTransmitThroughput (Sum)

Supported Dimensions

AMAZON CLOUDWATCH DIMENSIONS

Relational Database Service (RDS)	▪ Engine ▪ DB Instance

More

Knowledge Base: How do I define access rights for Amazon CloudWatch queries?

- https://kb.paessler.com/en/topic/38083

Knowledge Base: How much does Amazon charge for using the CloudWatch API?

- https://kb.paessler.com/en/topic/37543

Knowledge Base: Which .NET version does PRTG require?

- https://kb.paessler.com/en/topic/60543

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.10 Amazon CloudWatch SNS Sensor

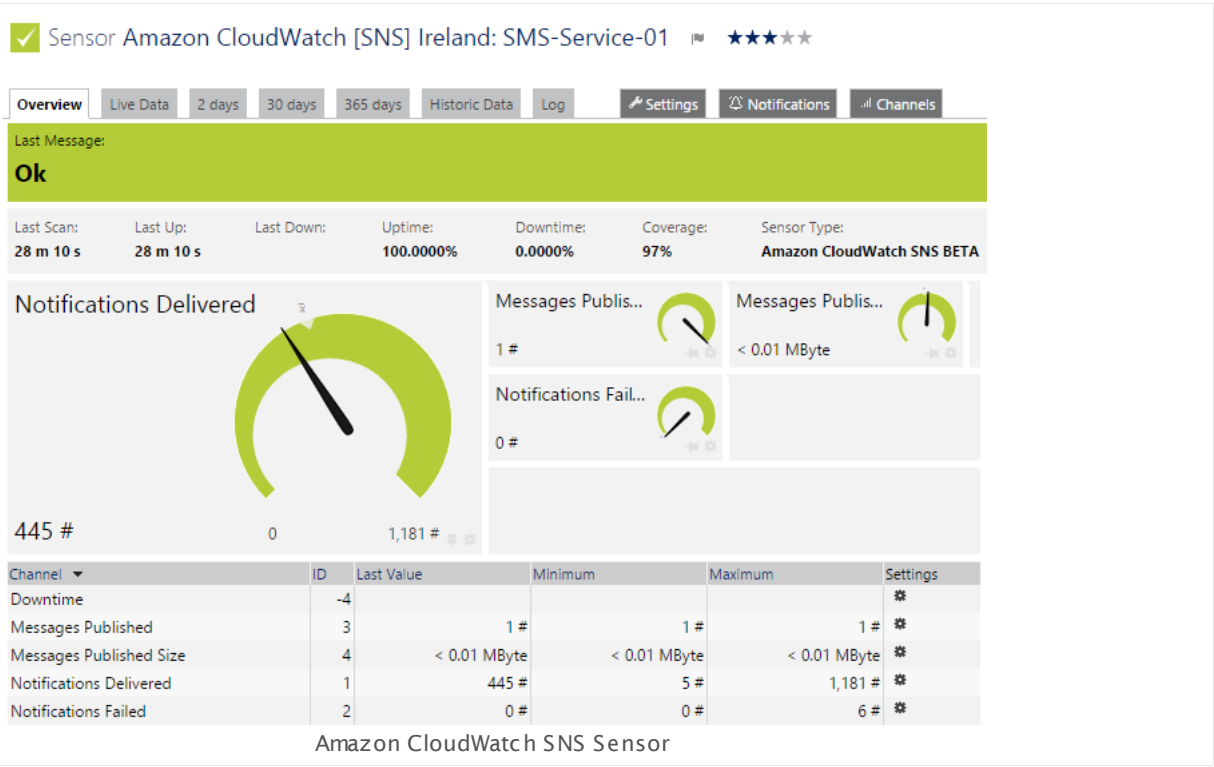
The Amazon CloudWatch SNS sensor monitors the performance of the Amazon Cloud service Simple Notification Service (SNS).

The sensor can show the following:

- Message Counting
- Error Counting

See **Supported Metrics** 514 for a list of data that this sensor can potentially show in dedicated channels.

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Amazon CloudWatch SNS Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/amazon_cloudwatch_sns_sensor.png

Remarks

- Requires access rights for CloudWatch queries. For details, please see the Knowledge Base: How do I define access rights for Amazon CloudWatch queries?
- Requires .NET 4.0 or higher on the probe system.
- Define **Credentials for Amazon CloudWatch** 372 in settings that are higher in the **Object Hierarchy** 118, for example, in the parent device settings 360.
- The minimum scanning interval for this sensor is **15 minutes**.

- Configure notification triggers [2791] with a latency of **0 seconds** to receive all notifications for this sensor ([...] for at least 0 seconds).
- This sensor will only show those channels for which it receives data from Amazon. You can check the availability of data in your CloudWatch Console on the AWS website. To know which channels are possible for the various services of this Amazon CloudWatch sensor, see the manual section **Supported Metrics**. If the sensor does not receive data from Amazon for more than 6 hours, it will go into error status.
- To know which dimensions you can monitor, see the manual section **Supported Dimensions**.
- Amazon will charge you (a small amount) for each "Amazon CloudWatch API Request" query the sensor sends to the Amazon servers. Depending on the service, each Amazon CloudWatch sensor sends about 10 to 30 requests with each scanning interval. Last time we checked the Amazon price list, they charged max. US$ 0.014 per 1,000 requests (depending on your region).
  For details, please see the Knowledge Base: How much does Amazon charge for using the CloudWatch API?
- Currently, this sensor type is in beta status. The methods of operating can change at any time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.

BETA

Requirement: Access Rights for Amazon CloudWatch Queries

The AWS Identity and Access Management (IAM) account that you use with the Amazon CloudWatch sensor needs specific rights to query any metrics. For details, see section **More** [514].

Requirement: .NET Framework

This sensor type requires the Microsoft .NET Framework to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the remote probe [3196]. If the framework is missing, you cannot create this sensor.

Required .NET version (with latest updates): .NET 4.0 (Client Profile is sufficient), .NET 4.5, or .NET 4.6.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/60543

Add Sensor

The **Add Sensor** dialog appears when you manually [288] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

PRTG looks for available instances.

This can take up to several minutes.

Select which service instance(s) you want to monitor. PRTG creates one sensor for each instance you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

AMAZON CLOUDWATCH SPECIFIC

Services	Select the Applications, Platforms or Topics you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items. To better find what you want to monitor, especially in large tables, use the search function in the upper-right corner.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	Enter one or more **Tags**, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

AMAZON CLOUDWATCH SPECIFIC

Region	Shows the region in which the monitored AWS instance runs. It is one of the following regions: ▪ US East (Northern Virginia) ▪ US West (Oregon) ▪ US West (Northern California) ▪ Canada (Central) ▪ EU (Ireland) ▪ EU (Frankfurt) ▪ Asia Pacific (Singapore) ▪ Asia Pacific (Tokyo) ▪ Asia Pacific (Sydney) ▪ Asia Pacific (Seoul) ▪ Asia Pacific (Mumbai) ▪ South America (Sao Paulo) Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

AMAZON CLOUDWATCH SPECIFIC

Description	Shows the description of the AWS service instance that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
ID	Shows the ID of the AWS instance that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Result Handling	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section **Data Storage** 3226. You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.

SCANNING INTERVAL

- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

This sensor type has a fixed minimum scanning interval for performance reasons. You cannot run the sensor in shorter intervals than this minimum interval. Consequently, shorter scanning intervals as defined in **System Administration—Monitoring** 2955 are not available for this sensor.

For Amazon CloudWatch sensors, the minimum scanning interval is **15 minutes**.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

Supported Metrics

AMAZON CLOUDWATCH METRICS

Simple Notification Service (SNS)	▪ NumberOfNotificationsDelivered (Sum) ▪ NumberOfNotificationsFailed (Sum) ▪ NumberOfMessagesPublished (Average) ▪ PublishSize (Average)

Supported Dimensions

AMAZON CLOUDWATCH DIMENSIONS

Simple Notification Service (SNS)	▪ Application ▪ Platform ▪ Application and Platform ▪ Topic

More

Knowledge Base: How do I define access rights for Amazon CloudWatch queries?

- https://kb.paessler.com/en/topic/38083

Knowledge Base: How much does Amazon charge for using the CloudWatch API?

- https://kb.paessler.com/en/topic/37543

Knowledge Base: Which .NET version does PRTG require?

- https://kb.paessler.com/en/topic/60543

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.11 Amazon CloudWatch SQS Sensor

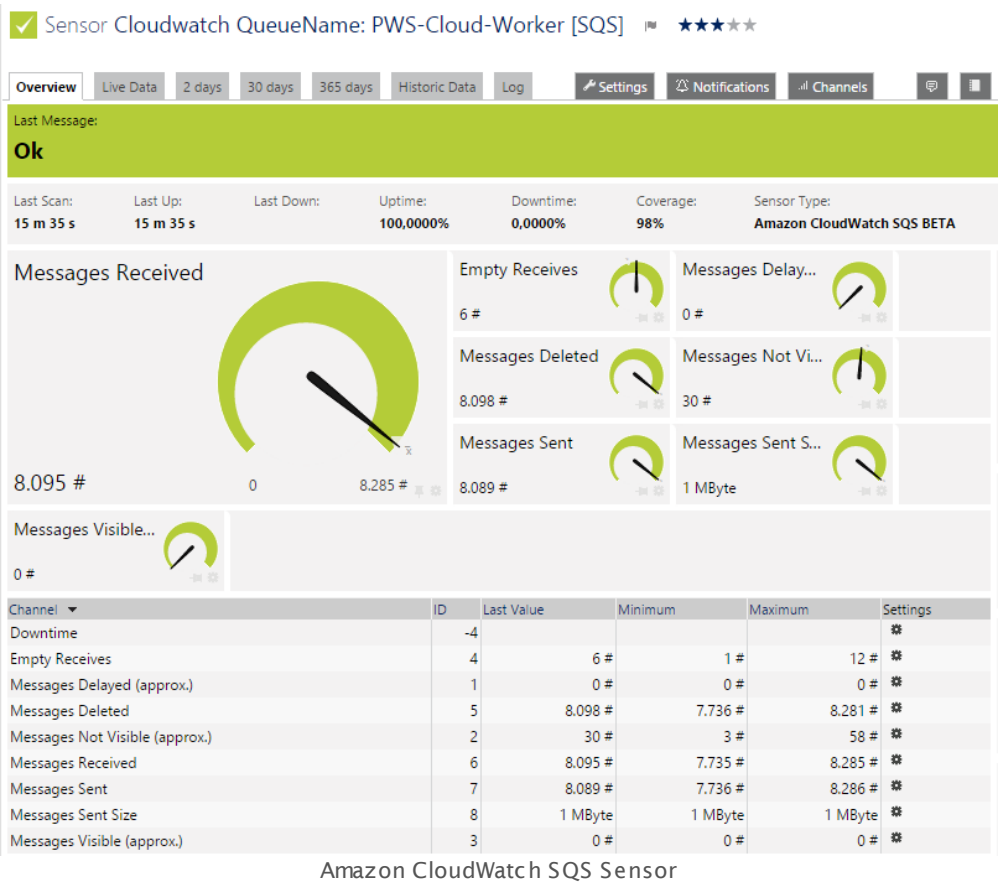
The Amazon CloudWatch SQS sensor monitors the performance of the Amazon Cloud service Simple Queue Service (SQS).

The sensor can show the following:

- Message Counting
- Error Counting
- Delay

See **Supported Metrics** 526 for a list of data that this sensor can potentially show in dedicated channels.

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Amazon CloudWatch SQS Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/amazon_cloudwatch_sqs_sensor.png

Remarks

- Requires access rights for CloudWatch queries. For details, please see the Knowledge Base: How do I define access rights for Amazon CloudWatch queries?

- Requires .NET 4.0 or higher on the probe system.
- Define **Credentials for Amazon CloudWatch** [372] in settings that are higher in the **Object Hierarchy** [118], for example, in the parent device settings [360].
- The minimum scanning interval for this sensor is **15 minutes**.
- Configure notification triggers [2791] with a latency of **0 seconds** to receive all notifications for this sensor ([...] for at least 0 seconds).
- This sensor will only show those channels for which it receives data from Amazon. You can check the availability of data in your CloudWatch Console on the AWS website. To know which channels are possible for the various services of this Amazon CloudWatch sensor, see the manual section **Supported Metrics**. If the sensor does not receive data from Amazon for more than 6 hours, it will go into error status.
- To know which dimensions you can monitor, see the manual section **Supported Dimensions**.
- Amazon will charge you (a small amount) for each "Amazon CloudWatch API Request" query the sensor sends to the Amazon servers. Depending on the service, each Amazon CloudWatch sensor sends about 10 to 30 requests with each scanning interval. Last time we checked the Amazon price list, they charged max. US$ 0.014 per 1,000 requests (depending on your region).
  For details, please see the Knowledge Base: How much does Amazon charge for using the CloudWatch API?
- BETA Currently, this sensor type is in beta status. The methods of operating can change at any time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.

Requirement: Access Rights for Amazon CloudWatch Queries

The AWS Identity and Access Management (IAM) account that you use with the Amazon CloudWatch sensor needs specific rights to query any metrics. For details, see section **More** [526].

Requirement: .NET Framework

This sensor type requires the Microsoft .NET Framework to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the remote probe [3196]. If the framework is missing, you cannot create this sensor.

Required .NET version (with latest updates): .NET 4.0 (Client Profile is sufficient), .NET 4.5, or .NET 4.6.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/60543

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

PRTG looks for available instances.

This can take up to several minutes.

Select which service instance(s) you want to monitor. PRTG creates one sensor for each instance you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

AMAZON CLOUDWATCH SPECIFIC

Services	Select the Queues you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items. To better find what you want to monitor, especially in large tables, use the search function in the upper right corner.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets

BASIC SENSOR SETTINGS

Parent Tags	Shows **Tags** that this sensor inherits from its parent device, group, and probe. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags**, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

AMAZON CLOUDWATCH SPECIFIC

Region	Shows the region in which the monitored AWS instance runs. It is one of the following regions: ▪ US East (Northern Virginia) ▪ US West (Oregon) ▪ US West (Northern California) ▪ Canada (Central) ▪ EU (Ireland) ▪ EU (Frankfurt) ▪ Asia Pacific (Singapore) ▪ Asia Pacific (Tokyo) ▪ Asia Pacific (Sydney) ▪ Asia Pacific (Seoul) ▪ Asia Pacific (Mumbai) ▪ South America (Sao Paulo)

AMAZON CLOUDWATCH SPECIFIC

	Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Description	Shows the description of the AWS service instance that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
ID	Shows the ID of the AWS instance that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Result Handling	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section **Data Storage** 3226. You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor.

SENSOR DISPLAY

- **Show channels independently (default)**: Show an own graph for each channel.
- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

This sensor type has a fixed minimum scanning interval for performance reasons. You cannot run the sensor in shorter intervals than this minimum interval. Consequently, shorter scanning intervals as defined in **System Administration—Monitoring** 2955 are not available for this sensor.

For Amazon CloudWatch sensors, the minimum scanning interval is **15 minutes**.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

Supported Metrics

AMAZON CLOUDWATCH METRICS

Simple Notification Service (SNS)	▪ SentMessageSize (Sum) ▪ NumberOfMessagesSent (Sum) ▪ NumberOfMessagesReceived (Sum) ▪ NumberOfMessagesDeleted (Sum) ▪ NumberOfEmptyReceives (Sum) ▪ ApproximateNumberOfMessagesVisible (Average) ▪ ApproximateNumberOfMessagesNotVisible (Average) ▪ ApproximateNumberOfMessagesDelayed (Average)

Supported Dimensions

AMAZON CLOUDWATCH DIMENSIONS

Simple Notification Service (SNS)	▪ Queue

More

Knowledge Base: How do I define access rights for Amazon CloudWatch queries?

▪ https://kb.paessler.com/en/topic/38083

Knowledge Base: How much does Amazon charge for using the CloudWatch API?

▪ https://kb.paessler.com/en/topic/37543

Knowledge Base: Which .NET version does PRTG require?

▪ https://kb.paessler.com/en/topic/60543

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.12 Business Process Sensor

The Business Process sensor is a powerful and very flexible sensor that allows you to give a summary status of whole business processes while monitoring several process components.

This means that you can create your very own and individual sensor with channels based on data from other sensors ("source sensors") that are specific to your network.

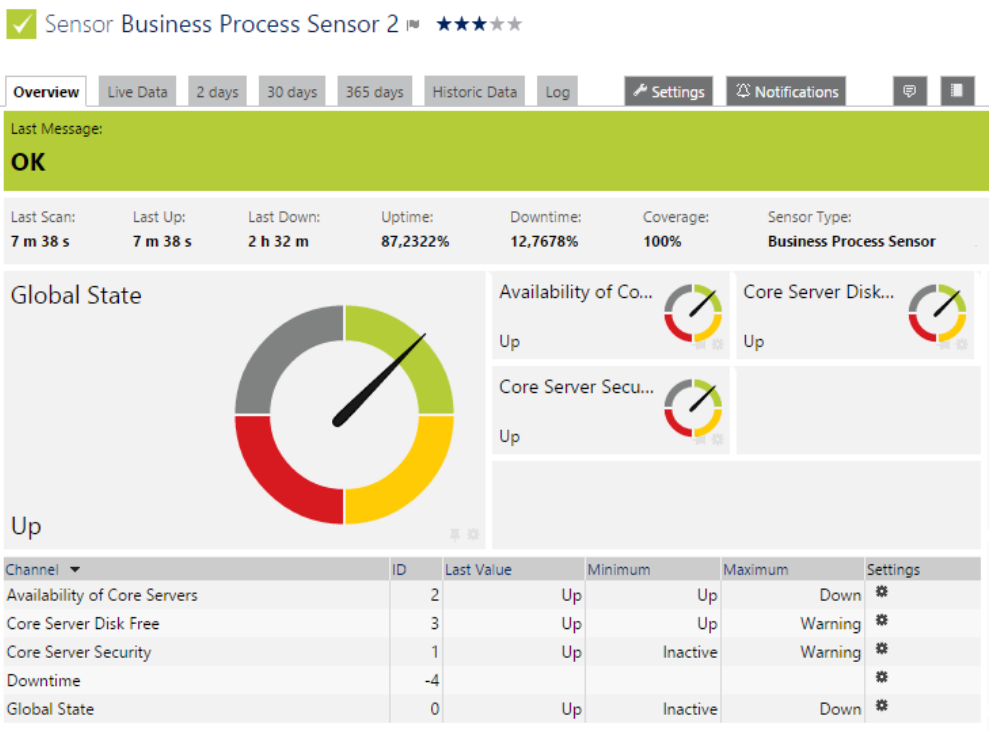
The sensor can show the following:

- The summarized status of the objects contained in each channel according to the individually defined error and warning thresholds
- The overall and summarized status of all channels in the Global State channel

The Business Process sensor does not show values in the "Downtime" channel because they cannot be calculated for this sensor type.

If you want to process values from other sensors and you want to perform calculations with these values, for example, please use the **Sensor Factory Sensor** 1438 instead.

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Business Process Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/business_process.png

Remarks

- Knowledge Base: How does the Business Process sensor calculate summarized sensor states?
- This sensor does not support more than 50 channels 529 officially.
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.

Limited to 50 Sensor Channels

PRTG does not support more than 50 sensor channels officially. Depending on the data used with this sensor type, you might exceed the maximum number of supported sensor channels. In this case, PRTG will try to display all sensor channels. However, please be aware that you will experience limited usability and performance.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

BUSINESS PROCESS SPECIFIC SETTINGS

Channel Name	Enter a meaningful name to identify the channel. To add a new channel to the sensor, click the **Enter Channel Name** field, enter a name for the channel, and confirm with the enter or tab key.
Error Threshold %	Set a percentage limit to define when the sensor channel displays a **Down** status. Please enter an integer value. Default is 50%. ⓘ This value depends on how many objects you feed into a business process channel. If a channel contains less source objects in "up" condition than the error threshold defines, this channel and the **Global State** channel of the Business Process sensor will show a **Down**. The **Sensor States** 163 which allow for the "up" condition ▲ of a Business Process channel are the following: ▪ Up ▪ Warning ▪ Unusual ▪ Partial Down All other sensor states will support the "down" condition ▼ (see the table below).

BUSINESS PROCESS SPECIFIC SETTINGS

For example, if you define 4 source sensors for a channel, an error threshold of 50% means that 3 source sensors have to be in "down" condition to set this channel to a **Down** status. So, 50% means that more than half of the source sensors must not be in "up" condition to set the sensor to **Down**.

To get more information, an illustration of the business process mechanisms and some use cases of the Business Process sensor, see the table below, the Knowledge Base, or the **More** 538 section below.

Warning Threshold %

Set a percentage limit to define when the sensor channel displays a **Warning** status. Please enter an integer value. Default is 75%.

This value depends on how many objects you feed into a business process channel.

If a channel contains less source objects in "up" condition than the threshold defines, this channel and the **Global State** channel of the Business Process sensor will show a **Warning** status (and so the sensor status is **Warning**).

The **Sensor States** 163 which allow for the "up" condition ▲ of a Business Process channel are the following:

- Up
- Warning
- Unusual
- Partial Down

All other sensor states will support the "down" condition ▼ (see the table below).

For example, if you define 4 source sensors for a channel, a warning threshold of 75% means that all 4 source sensors have to be in "down" condition to set this channel to a **Warning** status. So, 75% means that more than three out of four of the source sensors must not be in "up" condition to set the sensor to **Warning**.

To get more information, an illustration of the business process mechanisms and some use cases of the Business Process sensor, see the table below, the Knowledge Base, or the **More** 538 section below.

BUSINESS PROCESS SPECIFIC SETTINGS

Objects	Enter the objects you want to have in a channel using the + sign. This way, you can choose the desired objects from the device tree with the **Object Selector** 210. You can also start typing the object's ID, name, or a tag. PRTG then suggests the possible objects to be selected. You can add sensors, devices, groups, and probes to a channel. Each object you add is weighted equally, no matter if it is a single sensor or a whole device with many sensors. To give more weight to a specific object, add it several times. For example, add it twice to give double weight to an object, add it three times to give it triple weight. A probe, group, or device is as long in "up" condition ▲ as it does not contain any sensors in "down" condition ▼.

The **Business Process** Up ▲ and Down ▼ **conditions** are different from the normal PRTG up and down **Sensor States** 163. This is necessary for the Business Process sensor to be able to calculate summarized states and to show a calculated result for a whole business process. This table illustrates which sensor status leads to which Business Process condition.

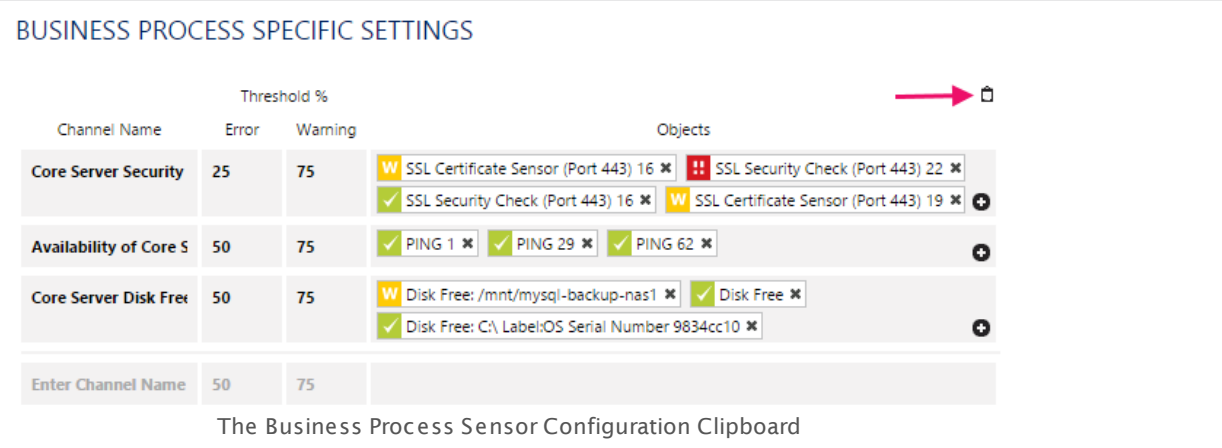
THE RELATION BETWEEN OBJECT STATES AND BUSINESS PROCESS CONDITIONS

Channel Object Status	Business Process Condition	Reason: Why does a given sensor status correspond to a given Business Process condition?
Up	Up ▲	The monitored object works, so everything is fine.
Warning	Up ▲	The sensor may show a warning, but the monitored object still works.
Partial Down	Up ▲	This status is available in a cluster setup and is displayed if at least one cluster node reports the sensor as up and at least one cluster node reports it as down. With at least one up report, the monitored object is supposed to be working and meets the business process up condition.

THE RELATION BETWEEN OBJECT STATES AND BUSINESS PROCESS CONDITIONS

Unusual	Up ▲	The sensor may show unusual values, but the monitored object works.
Collecting	Up ▲	The sensor still waits for more monitoring data to definitely decide about the sensor status, but so far the monitored object works. This PRTG internal status is visualized as Unknown in the PRTG web interface.
Down	Down ▼	The monitored object does not work.
Unknown	Down ▼	The sensor does not know if the monitored object works, for example because it has not yet received any data or because it has not received any data for a certain amount of time.
None	Down ▼	The sensor has not yet received any monitoring data from the monitored object. This PRTG internal status is visualized as Unknown in the PRTG web interface.
Paused	Down ▼	The monitored object does not work and monitoring has been paused, for example actively by the user, by inheritance, or by executed schedules. It might be convenient to exclude regularly or frequently paused objects from your business process monitoring, so you do not give more weight than necessary to a Business Process down status because of issues you already know about.
Down Acknowledged	Down ▼	The monitored object does not work and someone already knows.

If you encounter issues with your Business Process sensor and want to contact our support team 3022, please send us your exact configuration. It helps us find the cause more easily and quickly. Click the little clipboard icon in the upper-right of the **Business Process Specific Settings** table to copy your configuration:



The Business Process Sensor Configuration Clipboard

Click here to enlarge: http://media.paessler.com/prtg-screenshots/business_process_sensor_clipboard-m.png

You find your configuration in the window that opens. Copy the marked text and paste it into the support form 3022 to send it our support team.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.
- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: How does the Business Process sensor calculate summarized sensor states?

- https://kb.paessler.com/en/topic/66647

Knowledge Base: How can I use the Business Process sensor?

- https://kb.paessler.com/en/topic/67109

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.13 Cisco IP SLA Sensor

The Cisco IP SLA sensor monitors Voice over IP (VoIP) network parameters using IP Service Level Agreement (SLA) from Cisco via Simple Network Management Protocol (SNMP).

It shows different aspects provided by the queried device:

- Average, maximum, and minimum Round Trip Time (RTT)
- Average jitter
- Average jitter from source to destination and vice versa
- Average latency from source to destination and vice versa
- Impairment Calculated Planning Impairment Factor (ICPIF)
- Late packets in percent
- Average, maximum, and minimum latency from source to destination and vice versa
- Mean Opinion Score (MOS)
- Number of lost packets and in percent
- Packets out of sequence in percent
- Sense code (status code of RTT entry)

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

Cisco IP SLA Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/cisco_ip_sla.png

Remarks

- For a general introduction to the technology behind Quality of Service monitoring, please see manual section **Monitoring Quality of Service** 3104.
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select which SLAs you want to monitor. PRTG creates one sensor for each SLA you select in the Add Sensor dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

IP SLA SPECIFIC

IP SLAs

Select the IP SLAs you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

The list options depend on the configuration of the queried device. If you miss a type here, please check the configuration of your target device. PRTG can support the following operations with the given type IDs:

- **echo** (1)
- **pathEcho** (2)
- **fileIO** (3)
- **script** (4)
- **udpEcho** (5)
- **tcpConnect** (6)
- **http** (7)
- **dns** (8)
- **jitter** (9)
- **dlsw** (10)
- **dhcp** (11)
- **ftp** (12)
- **icmp-jitter** (16)

IP SLA SPECIFIC

- **path-jitter** (23)

The numbers above are the IDs of the SLA types as reported by the target device. PRTG translates them into the corresponding strings. These IDs are independent from the IDs that you see in the first column of the list. If the target device returns other values than given above, the sensor will show an error message that it cannot find the type.

Packet Loss values are summarized, but have no explicit channel for Source—Destination or Destination—Source values.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.

BASIC SENSOR SETTINGS

Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

IP SLA SPECIFIC

ID	These fields show SLA specific settings that the queried SLA device provides. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Type	
Name (Tag)	
Owner	
Frequency	

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

SENSOR DISPLAY

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.

SCANNING INTERVAL

- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

(i) To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

(i) Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.14 Citrix XenServer Host Sensor

The Citrix XenServer Host Sensor monitors a Xen host server via Hypertext Transfer Protocol (HTTP).

It can show the following:

- CPU usage
- Memory usage (free, used, allocation)
- Network usage
- Number of running virtual machines
- Load average

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

Channel	ID	Last Value	Minimum	Maximum	Settings
CPU _avg Usage	2	5 %	3 %	13 %	
CPU 0 Usage	3	5 %	3 %	14 %	
CPU 1 Usage	4	5 %	3 %	13 %	
Downtime	-4				
Load Average	5	0,23 #	0 #	0,47 #	
Memory allocation XAPI daemon	14	0,46 MByte	0,38 MByte	1 MByte	
Memory free XAPI daemon	15	1 MByte	0,29 MByte	1 MByte	
Memory live XAPI daemon	16	0,18 MByte	0,14 MByte	0,36 MByte	
Network aggr receive	8	26 KByte/s	23 KByte/s	862 KByte/s	
Network aggr send	9	12 KByte/s	7 KByte/s	557 KByte/s	
Network eth0 receive	10	24 KByte/s	22 KByte/s	860 KByte/s	
Network eth0 send	11	10 KByte/s	7 KByte/s	555 KByte/s	
Network lo receive	12	1 KByte/s	1 KByte/s	3 KByte/s	
Network lo send	13	1 KByte/s	1 KByte/s	3 KByte/s	
Total Memory free	6	155 MByte	155 MByte	155 MByte	
Total Memory used	7	3.070 MByte	3.070 MByte	3.070 MByte	
Total Memory XAPI	17	1 MByte	0,48 MByte	1 MByte	
VMs running	18	1 #	1 #	1 #	

Citrix XenServer Host Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/citrix_xenserver_host.png

Remarks

- The parent device must be a Citrix XenServer version 5.0 or later.
- The parent device has to represent one host server of your XenServer pool 552.
- Requires credentials for Xen servers to be defined for the device you want to use the sensor on.

- Requires 552 .NET 4.0 or higher on the probe system.
- This sensor type does not fully support TLS 1.2 connections and cannot be added to XenServers with security protocol setting "TLS 1.2 only".
- Knowledge Base: Does PRTG impair my Citrix environment?
- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.

Monitoring a XenServer Pool

In a XenServer pool there is one "pool master" that manages the pool. Incoming queries on any host are automatically forwarded to the pool master. If you want to monitor your virtual machines, or host servers, simply create respective sensors on a device that represents one host server of your pool. Internal processes will make sure that monitoring will take place and continue independently from the physical host.

In PRTG's device tree, the sensors for virtual machines will always remain on the host you originally created it on, also if it is currently running on a different host.

Requirement: .NET Framework

This sensor type requires the Microsoft .NET Framework to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the remote probe 3196. If the framework is missing, you cannot create this sensor.

Required .NET version (with latest updates): .NET 4.0 (Client Profile is sufficient), .NET 4.5, or .NET 4.6.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/60543

Add Sensor

The **Add Sensor** dialog appears when you manually 286 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select which XenServer hosts you want to monitor. PRTG creates one sensor for each host you select in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

HOST SETTINGS

Host	Select the hosts you want to add a sensor for, including the ones that are not running. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

HOST SETTINGS

UUID	Shows the Universally Unique Identifier (UUID) of the host that this sensor monitors. This value is shown for reference purposes only. We strongly recommend that you only change it if Paessler support explicitly asks you to do so. Wrong usage can result in incorrect monitoring data!
Name	Shows the name of the host that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

DEBUG OPTIONS

Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section **Data Storage** 3226. You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

SENSOR DISPLAY

Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. ⓘ To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: Which .NET version does PRTG require?

- https://kb.paessler.com/en/topic/60543

Knowledge Base: Does PRTG impair my Citrix environment?

- https://kb.paessler.com/en/topic/61880

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

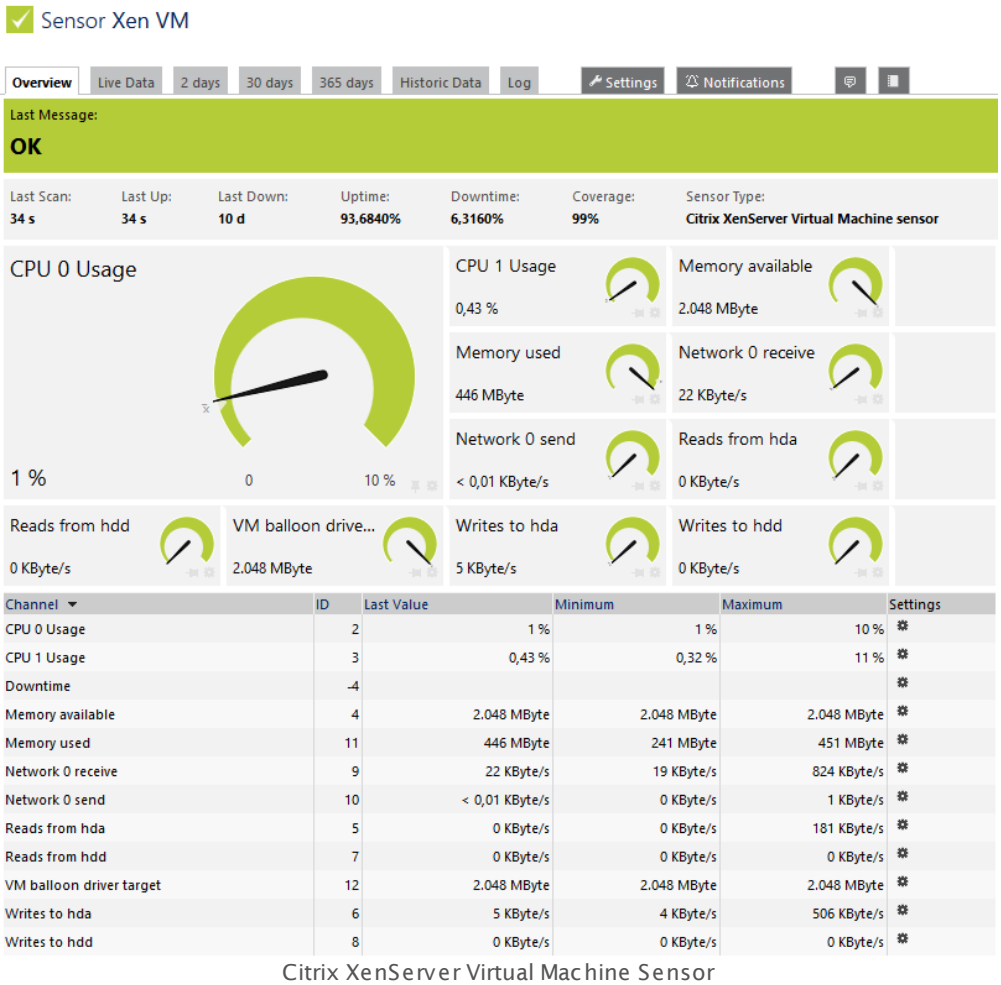
7.8.15 Citrix XenServer Virtual Machine Sensor

The Citrix XenServer Virtual Machine Sensor monitors a virtual machine on a Xen server via Hypertext Transfer Protocol (HTTP).

It can show the following:

- CPU usage
- Memory usage (available, used)
- Disk usage (reads and writes per second)
- Network usage (bytes received and sent)
- Balloon driver target size

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Channel	ID	Last Value	Minimum	Maximum	Settings
CPU 0 Usage	2	1 %	1 %	10 %	
CPU 1 Usage	3	0,43 %	0,32 %	11 %	
Downtime	-4				
Memory available	4	2.048 MByte	2.048 MByte	2.048 MByte	
Memory used	11	446 MByte	241 MByte	451 MByte	
Network 0 receive	9	22 KByte/s	19 KByte/s	824 KByte/s	
Network 0 send	10	< 0,01 KByte/s	0 KByte/s	1 KByte/s	
Reads from hda	5	0 KByte/s	0 KByte/s	181 KByte/s	
Reads from hdd	7	0 KByte/s	0 KByte/s	0 KByte/s	
VM balloon driver target	12	2.048 MByte	2.048 MByte	2.048 MByte	
Writes to hda	6	5 KByte/s	4 KByte/s	506 KByte/s	
Writes to hdd	8	0 KByte/s	0 KByte/s	0 KByte/s	

Citrix XenServer Virtual Machine Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/citrix_xenserver_virtual_machine.png

Remarks

- The parent device must be a Citrix XenServer (version 5.0 or later).
- The parent device has to represent one host server of your XenServer pool 562.
- Requires credentials for Xen servers to be defined for the device you want to use the sensor on.
- Requires 562 .NET 4.0 or higher on the probe system.
- This sensor type does not fully support TLS 1.2 connections and cannot be added to XenServers with security protocol setting "TLS 1.2 only".
- Knowledge Base: Does PRTG impair my Citrix environment?
- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.

Monitoring a XenServer Pool

In a XenServer pool there is one "pool master" that manages the pool. Incoming queries on any host are automatically forwarded to the pool master. If you want to monitor your virtual machines, or host servers, simply create respective sensors on a device that represents one host server of your pool. Internal processes will make sure that monitoring will take place and continue independently from the physical host.

In PRTG's device tree, the sensors for virtual machines will always remain on the host you originally created it on, also if it is currently running on a different host.

Requirement: .NET Framework

This sensor type requires the Microsoft .NET Framework to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the remote probe 3196. If the framework is missing, you cannot create this sensor.

Required .NET version (with latest updates): .NET 4.0 (Client Profile is sufficient), .NET 4.5, or .NET 4.6.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/60543

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

PRTG requests a full list of all virtual machines configured on the Xen server. Therefore, it may take a few seconds before the dialog is loaded.

Select which virtual machines you want to monitor. PRTG creates one sensor for each virtual machine you select in the **Add Sensor** dialog. The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

VIRTUAL MACHINE SETTINGS

Virtual Machine	Select the Virtual Machines (VM) you want to add a sensor for, including the ones that are not running. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.

BASIC SENSOR SETTINGS

Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

VIRTUAL MACHINE SETTINGS

UUID	Shows the Universally Unique Identifier (UUID) of the virtual machine. This value is shown for reference purposes only. We strongly recommend that you only change it if Paessler support explicitly asks you to do so. Wrong usage can result in incorrect monitoring data!
Name	Shows the name of the virtual machine. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

DEBUG OPTIONS

Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section Data Storage 3226. You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: Which .NET version does PRTG require?

- https://kb.paessler.com/en/topic/60543

Knowledge Base: Does PRTG impair my Citrix environment?

- https://kb.paessler.com/en/topic/61880

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

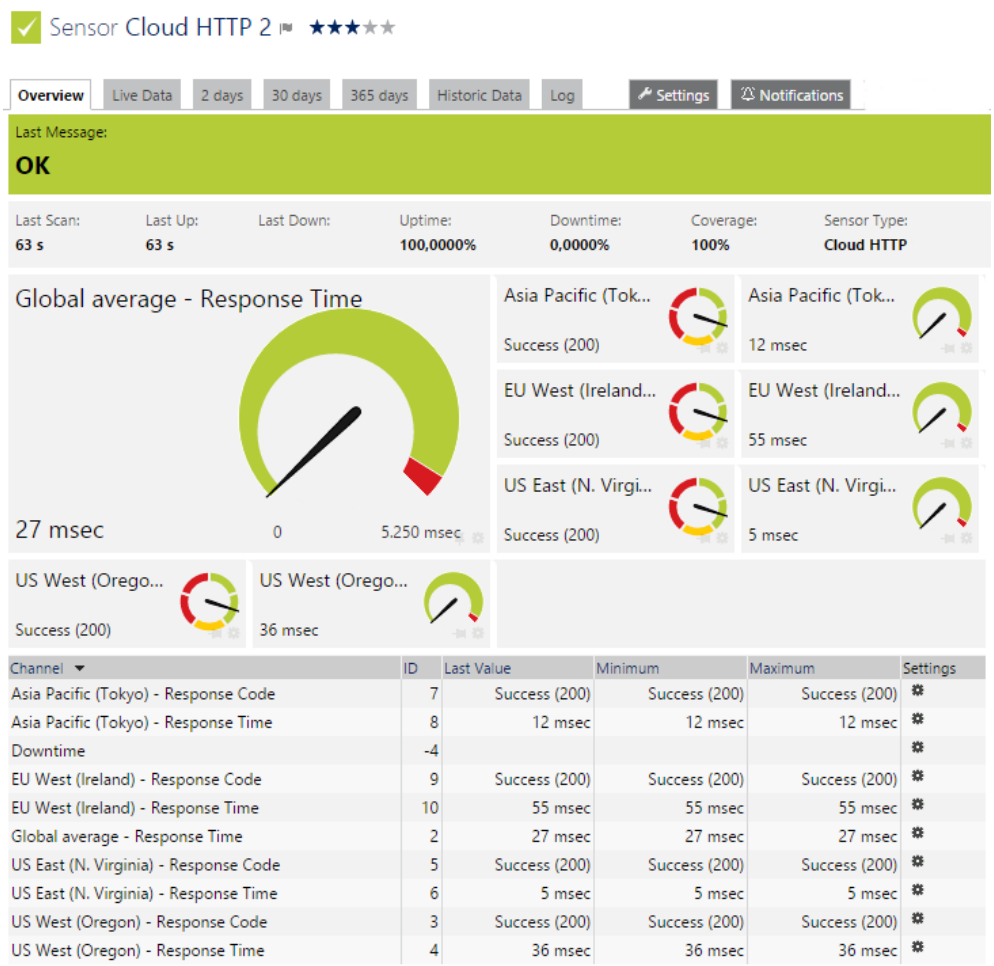
For more general information about settings, please see the **Object Settings** 188 section.

7.8.16 Cloud HTTP Sensor

The Cloud HTTP sensor monitors the loading time of a web server via Hypertext Transfer Protocol (HTTP) from different locations worldwide using the PRTG Cloud. The locations are distributed over three continents around the globe.

The sensor can show **response time** and **response code** of the target server monitored from the following locations:

- Asia Pacific: Tokyo
- EU West: Ireland
- US East: Northern Virginia
- US West: Oregon
- Global average response time



Cloud HTTP Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/cloud_http.png

Remarks

- The server on which the PRTG probe with this sensor runs must have access to the internet. The probe system needs to be able to reach **https://api.prtgcloud.com:443** to communicate with the PRTG Cloud.
- The URL you monitor must be reachable over the internet. You cannot use this sensor to monitor localhost (127.0.0.1) or other target devices that are only reachable within your private network.
- This sensor type supports proxy server usage 2967.
- This sensor type does not support IPv6.
- Knowledge Base: Are there any limits for using Cloud Ping and Cloud HTTP sensors?
- Knowledge Base: What is the PRTG Cloud Bot?
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.
- This sensor type has predefined limits for several metrics. You can change these limits individually in the channel settings. For detailed information about channel limits, please refer to the manual section **Sensor Channels Settings** 2782.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.

BASIC SENSOR SETTINGS

Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

HTTP SETTINGS

URL	Enter the URL the sensor connects to. It has to be URL encoded! If you enter an absolute URL, the sensor uses this address independently from the **IP address/DNS name** setting of the device on which you create this sensor. You can enter an URL leading to a webpage (to measure the page source code's loading time), or enter the URL of an image or of another page asset to measure this element's availability and loading time. PRTG uses a smart URL replacement which allows you to use the parent device's IP address or DNS name setting as part of the URL. For more information, please see section **Smart URL Replacement** below.
Request Method	Choose an HTTP request method to determine how the sensor will request the given URL. ▪ **GET**: Request the website directly, like browsing the web. We recommend using this setting for a simple check of a web page. ▪ **POST**: Send post form data to the URL. If this setting is chosen, you must enter the data that will be sent in the **Postdata** field below.

HTTP SETTINGS

- **HEAD**: Only request the HTTP header from the server; without the actual web page. Although this saves bandwidth since less data is transferred, it is not recommended because the measured request time is not the one experienced by your users and you might not be notified for slow results or timeouts.

Postdata

This field is only visible when you select the POST **Request Method** setting above. Enter the data part for the POST request here.

No XML is allowed here!

Timeout (Sec.)

Enter a timeout in seconds for the server request. If the reply takes longer than this value defines, the PRTG will cancel the request and shows an error message. The maximum timeout value is 5 seconds.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.
- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

This sensor type has a fixed minimum scanning interval for performance reasons. You cannot run the sensor in shorter intervals than this minimum interval. Consequently, shorter scanning intervals as defined in **System Administration—Monitoring** 2955 are not available for this sensor.

For Cloud HTTP sensors, the minimum scanning interval is **10 minutes**.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

Smart URL Replacement

Instead of entering a complete address in the URL field of an HTTP sensor, you can merely enter the protocol followed by colon and three slashes (that means you can enter either http:/// or https:/// or even a simple slash / as equivalent for http:///). PRTG will then fill in the parent device's **IP address** or **DNS name** in front of the third slash automatically. Whether this results in a valid URL or not, depends on the IP address or DNS name of the device where this HTTP sensor is created on. In combination with cloning devices, the smart URL replacement makes it easy to create many like devices.

For example, if you create a device with **DNS name** www.example.com and you put an HTTP sensor on it, you can provide values the following ways:

- Providing the value https:/// in the URL field, PRTG will automatically create the URL https://www.example.com/ from that.
- Using the value /help in the URL field, PRTG will automatically create and monitor the URL http://www.example.com/help
- It is also possible to provide a port number in the URL field which will be taken over by the device's DNS name and internally added, for example, http://:8080/

Smart URL replacement does not work for sensors running on the **Probe Device**.

More

Knowledge Base: Are there any limits for using Cloud Ping and Cloud HTTP sensors?

- https://kb.paessler.com/en/topic/63590

Knowledge Base: What is the PRTG Cloud Bot?

- https://kb.paessler.com/en/topic/65719

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

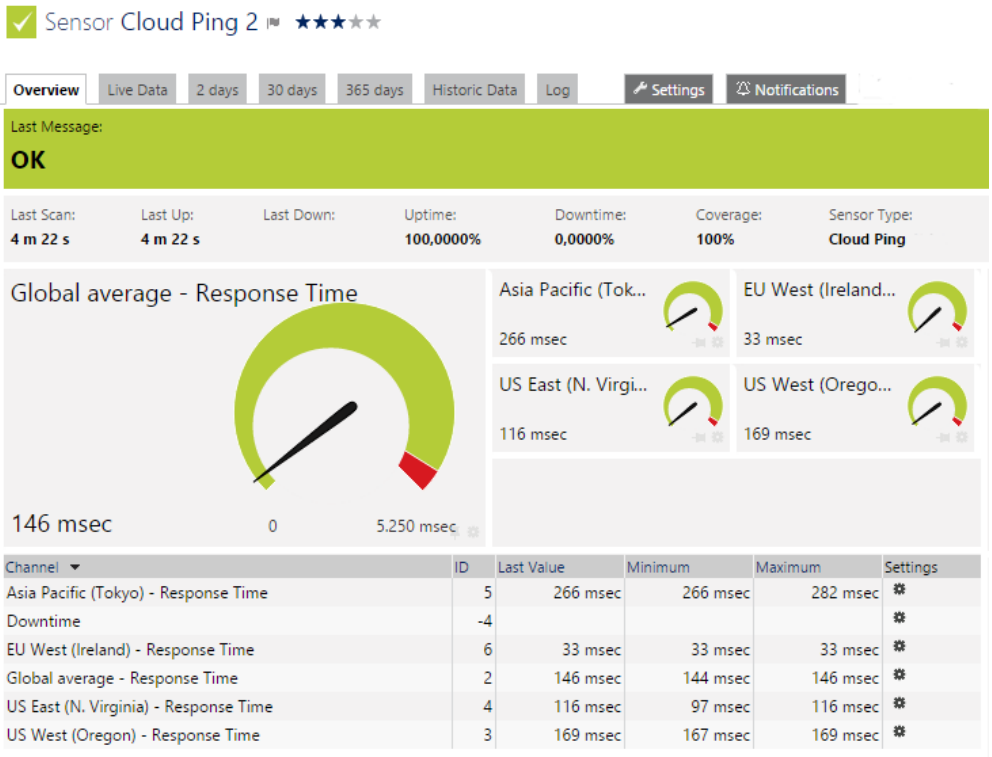
For more general information about settings, please see the **Object Settings** 188 section.

7.8.17 Cloud Ping Sensor

The Cloud Ping sensor monitors the Transport Control Protocol (TCP) ping times to its parent device from different locations worldwide using the PRTG Cloud. These locations are distributed over three continents around the globe.

The sensor can show the **response times** of the target server pinged from the following locations:

- Asia Pacific: Tokyo
- EU West: Ireland
- US East: Northern Virginia
- US West: Oregon
- Global average response time



Cloud Ping Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/cloud_ping.png

Remarks

- The server on which the PRTG probe [119] with this sensor runs must have access to the internet. The probe system needs to be able to reach **https://api.prtgcloud.com:443** to communicate with the PRTG Cloud.

- The address you define in the parent device settings 360 must be reachable over the internet. You cannot use this sensor to monitor localhost (127.0.0.1) or other target devices that are only reachable within your private network.
- This sensor type supports proxy server usage 2967.
- This sensor type does not support IPv6.
- Knowledge Base: Are there any limits for using Cloud Ping and Cloud HTTP sensors?
- Knowledge Base: What is the PRTG Cloud Bot?
- This sensor type has predefined limits for several metrics. You can change these limits individually in the channel settings. For detailed information about channel limits, please refer to the manual section **Sensor Channels Settings** 2782.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

BASIC SENSOR SETTINGS

	You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

PING SETTINGS

Packet Size (Bytes)	Enter the packet size in bytes for the Ping. You can choose any value between 1 and 10000. We recommend that you use the default value.
Ping Count	Enter the number of Pings to be sent in a row to the parent device with one scan. Please enter an integer value. The default value is 1, the maximum supported ping count is 5.
Timeout (Sec.)	Enter a timeout in seconds for the Ping. If the reply takes longer than this value defines, the PRTG will cancel the request and shows an error message. The maximum timeout value is 5 seconds.
Port	Enter the number of the port that the sensor uses for TCP ping. The default port is **80**.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel.

SENSOR DISPLAY

	▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. ⓘ This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.

SCANNING INTERVAL

- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

This sensor type has a fixed minimum scanning interval for performance reasons. You cannot run the sensor in shorter intervals than this minimum interval. Consequently, shorter scanning intervals as defined in **System Administration—Monitoring** 2955 are not available for this sensor.

For Cloud Ping sensors, the minimum scanning interval is **10 minutes**.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: Are there any limits for using Cloud Ping and Cloud HTTP sensors?

- https://kb.paessler.com/en/topic/63590

Knowledge Base: What is the PRTG Cloud Bot?

- https://kb.paessler.com/en/topic/65719

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

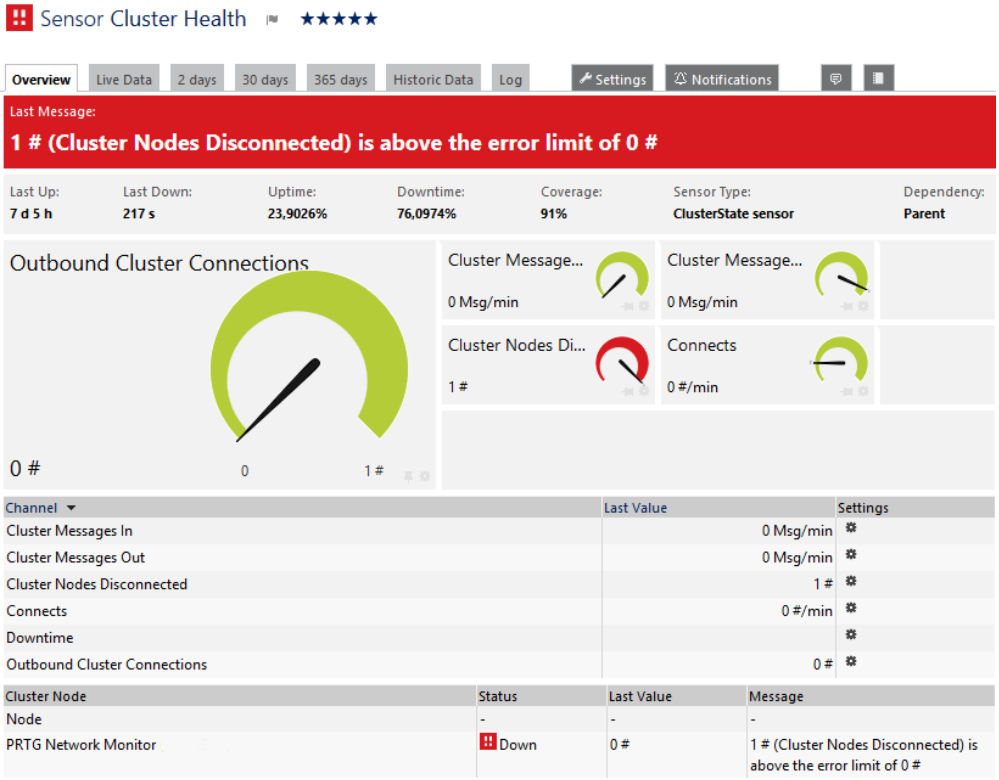
For more general information about settings, please see the **Object Settings** 188 section.

7.8.18 Cluster Health Sensor

The Cluster Health sensor monitors the health of a PRTG cluster [116] and indicates PRTG's own system health status.

It measures various internal system parameters of the cluster system:

- Number of connects per minute
- Cluster ingoing and outgoing messages per minute
- Number of connected and disconnected cluster nodes.



ClusterState Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/clusterstate.png

Remarks

- PRTG creates this sensor automatically with a cluster installation. You cannot delete or add it manually.
- If at least one cluster node is disconnected, this sensor will show a **Down** status [163] by default.
- You can review the states of each cluster node on the sensor's **Overview** tab .
- You can choose the cluster member of which you want to show data (or of all nodes) on the monitoring data review tabs [170].

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

SENSOR DISPLAY

Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

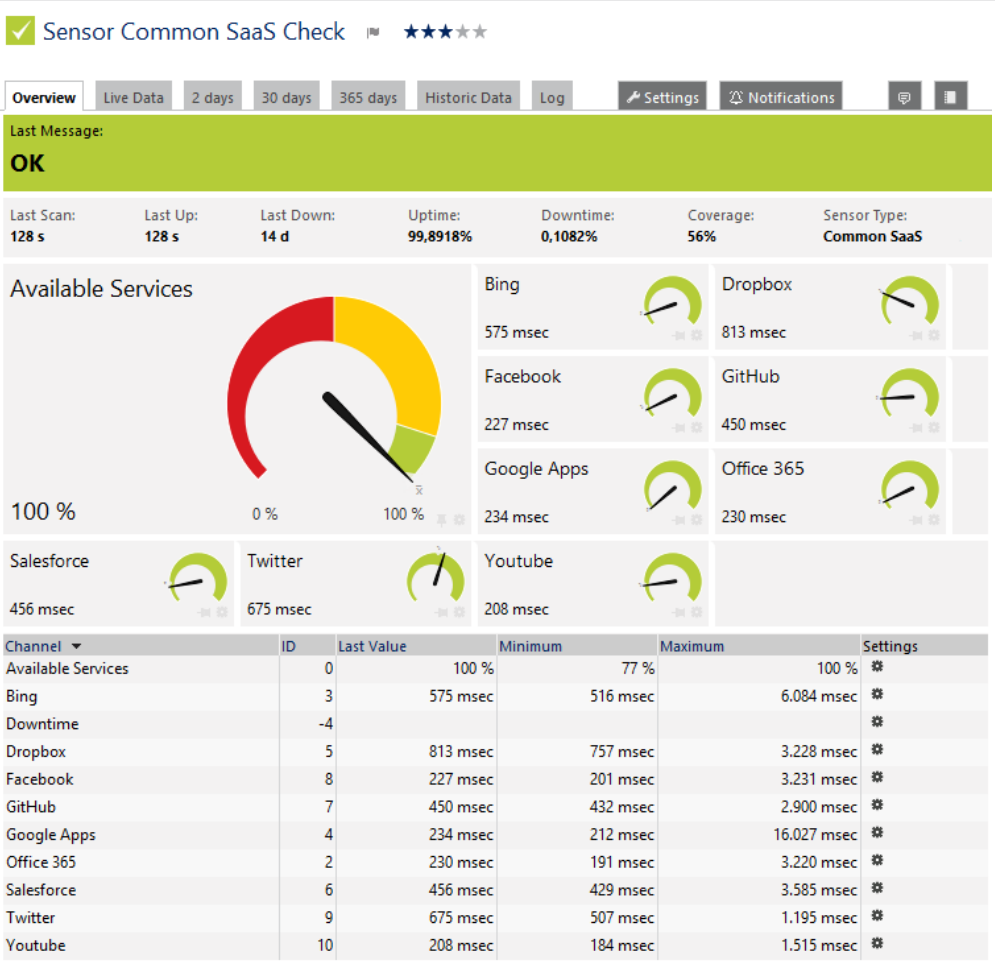
For more general information about settings, please see the **Object Settings** 188 section.

7.8.19 Common SaaS Sensor

The Common SaaS Sensor monitors the availability of several Software as a Service (SaaS) providers. Because your business processes depend more and more on cloud hosts, this sensor type is an important pillar for unified monitoring. With this sensor you can get alarms if your cloud services are not reachable anymore.

This sensor shows the following:

- Available services in percent
- Response times of the following SaaS providers:
  - Bing
  - Dropbox
  - Facebook
  - GitHub
  - Google Apps
  - Office 365
  - Salesforce
  - Twitter
  - Youtube



Channel	ID	Last Value	Minimum	Maximum	Settings
Available Services	0	100 %	77 %	100 %	
Bing	3	575 msec	516 msec	6.084 msec	
Downtime	-4				
Dropbox	5	813 msec	757 msec	3.228 msec	
Facebook	8	227 msec	201 msec	3.231 msec	
GitHub	7	450 msec	432 msec	2.900 msec	
Google Apps	4	234 msec	212 msec	16.027 msec	
Office 365	2	230 msec	191 msec	3.220 msec	
Salesforce	6	456 msec	429 msec	3.585 msec	
Twitter	9	675 msec	507 msec	1.195 msec	
Youtube	10	208 msec	184 msec	1.515 msec	

Common SaaS Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/common_saas.png

Remarks

- The server where the PRTG probe with this sensor runs must have access to the internet.
- PRTG creates this sensor automatically on every new probe device. If the system running the probe has no connection to the internet, please pause 214 or delete 226 this sensor manually to avoid error messages.
- This sensor type has a fixed scanning interval (15 minutes). You cannot change it.
- This sensor type supports proxy server usage 2967.
- This sensor type has predefined limits for several metrics. You can change these limits individually in the channel settings. For detailed information about channel limits, please refer to the manual section **Sensor Channels Settings** 2782.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select which SaaS providers you want to monitor. The sensor will create one channel for each service you choose in the **Add Sensor** dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

COMMON SAAS SPECIFIC

SaaS Checklist	Select the services you want to monitor with this sensor. You see a list with the names of all items that are available to monitor. Select the desired items by adding check marks in front of the respective lines. The sensor creates one channel for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	Enter one or more **Tags**, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DEBUG OPTIONS

Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section **Data Storage**. You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

SENSOR DISPLAY

	You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. ⓘ To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.20 Core Health Sensor

The Core Health sensor monitors internal PRTG parameters. It shows the status of the PRTG core server.

This sensor type checks various parameters of your PRTG core that have an impact on the stability of the system:

- Health: This index value sums up the core state into a value between 100% (healthy) and 0% (failing). Frequent or repeated health values below 100% should be investigated.
- Age of Code: This channel shows the time that has passed since the last update of your PRTG installation. Please update regularly to get best security and stability for PRTG, as well as the latest features. We recommend that you use the PRTG **Auto-Update** 3005 to get new versions automatically.
- CPU Load: This channel shows the current percentage CPU load. Extensive CPU load can lead to false, incomplete, and incorrect monitoring results. This value should usually stay below 50%.
- Handles: This is a counter for the data structures of the operating system. It is responsible for internal resource management. Repeated obviously increasing values should be investigated.
- Committed Memory: This channel shows the amount of memory committed to the PRTG core server as reported by the memory manager.
- Free Page File Memory: This channel shows the amount of free page file memory currently available on the system. Page file memory is aggregated RAM and the size of page file. It is the maximum amount of memory that is available on the system to be used for all currently running processes. If it gets too low the system can crash, at least some applications will throw "Out of memory" errors.
- Free Physical Memory: This channel shows the amount of free physical memory currently available on the system. This is the RAM that is physically built into the computer. If it gets too low the system will become very slow and PRTG is not usable in a reasonable way anymore. It can happen that some sensors will not be displayed correctly in that case, they will appear disabled (grayed out).
- Free Virtual Memory: This channel shows the accessible address space on the system for PRTG. PRTG cannot use more memory than reported here, independently from free page file and physical memory. On a 32-bit OS (operating system) the maximum is 2 GB (3 GB with special settings under Windows); on a 64-bit OS it is 4 GB if PRTG is running as 32-bit version, and unlimited as 64-bit version (only Core). If free virtual memory gets too low, PRTG will throw "Out of memory" errors or the message "not enough storage to process this command" (visible in the Core log).
- Maintenance Days: This channel shows the remaining maintenance days of your PRTG on premises license. Please renew your maintenance on time to be sure to get updates for your PRTG on premises installation. PRTG on demand instances show a fixed value here for technical reasons.
- Threads: This channel shows the number of program parts that are currently running simultaneously. This number can increase with heavy load. The number should not exceed 100 in normal operation.

- Raw Data Buffer: This channel shows how much raw data is temporarily stored on the physical memory while I/O operations on the disk. Usually, this value should be 0 (or very low). Investigate increasing values.

Channel	ID	Last Value	Minimum	Maximum	Settings
Age of Code	10	36 h 46 m	4 h 36 m	7 d 9 h	
Committed Memory	4	230 MByte	0 MByte	639 MByte	
CPU Load	5	1 %	0 %	49 %	
Downtime	-4				
Free Page File Memory	2	1.653 MByte	0,07 MByte	15.212.752 MByte	
Free Physical Memory	3	1.653 MByte	0 MByte	1.747 MByte	
Free Virtual Memory	1	3.724 MByte	2.245 MByte	3.772 MByte	
Handles	6	7.175 #	0 #	12.293 #	
Health	0	100 %	0 %	100 %	
Maintenance Days	9	711 #	711 #	712 #	
Raw Data Buffer	8	0 #	0 #	9.999 #	
Threads	7	51 #	0 #	91 #	

Core Health Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/core_health.png

Remarks

- PRTG creates this sensor automatically and you cannot delete it.
- You can set up this sensor only on a Local Probe device!
- You can find PRTG core system memory related information also in the **PRTG System Status** 2997. For details, see the Knowledge Base: What do the PRTG core system memory parameters mean?

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.

SCANNING INTERVAL

- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: What do the PRTG core system parameters mean?

- https://kb.paessler.com/en/topic/71671

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.21 Dell PowerVault MDi Logical Disk Sensor

The Dell PowerVault MDi Logical Disk sensor monitors a virtual disk on a Dell PowerVault MD3000i, MD3420, MD3620i, MD3000f, MD3620f, or MD3820i. It might work with other models, too.

This sensor can show the following:

- Total number of I/O operations
- Number of current and maximum I/O operations per second
- Current and maximum disk speed
- Read and cache hit percentages

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

Dell PowerVault MDi Logical Disk Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/dell_powervault_mdi_logical_disk.png

Remarks

- Works with Dell PowerVault MD3000i, MD3420, MD3620i, MD3000f, MD3620f, or MD3820i, and might support other models.

- Requires 610 Dell Modular Disk Storage Manager on the probe system. Please see the Knowledge Base: Where do I find the Dell PowerVault Modular Disk Storage Manager for use with my MDi SAN?
- Needs the IP address of the Storage Area Network (SAN) defined in the parent device settings.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Requirement: Dell Modular Disk Storage Manager

This sensor requires the installation of the Dell Modular Disk Storage Manager program. You have to install it on the computer running the PRTG probe: Either on the local system (on every node, if on a cluster probe), or on the system running the remote probe 3196. For details about setup, please see **More** section below.

Create this sensor on a device that has the SAN's IP address configured in the **IP Address/ DNS Name** field of the sensor settings.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select which virtual disks you want to monitor. PRTG will create one sensor for each disk you select in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SENSOR SETTINGS

Virtual Disks	Select the disks you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SETTINGS

Virtual Disk	Shows the name of the virtual disk that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result.

SENSOR SETTINGS

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section **Data Storage** 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Where do I find the Dell PowerVault Modular Disk Storage Manager for use with my MDi SAN?

- https://kb.paessler.com/en/topic/38743

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.22 Dell PowerVault MDi Physical Disk Sensor

The Dell PowerVault MDi Physical Disk sensor monitors a physical disk on a Dell PowerVault MD3000i, MD3420, MD3620i, MD3000f, or MD3620f. It might work with other models, too.

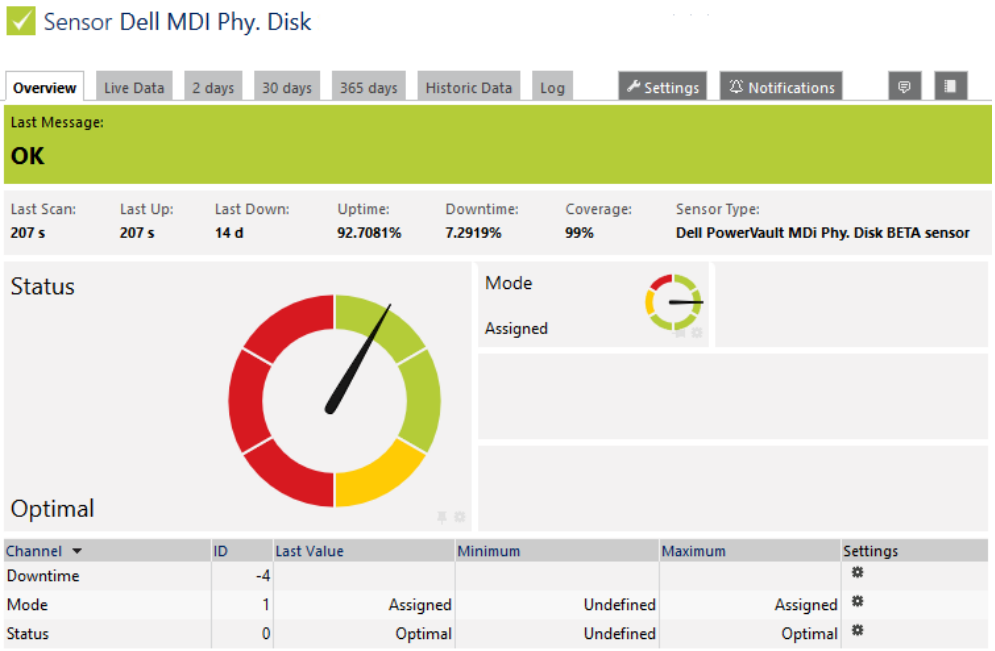
This sensor can show following:

- Mode of the physical disk
- Status of the physical disk

The sensor shows these channels as reported in the Modular Disk Storage Manager. Status and mode combined indicate the particular status of a RAID controller physical disk. The table below provides you with the status description according to the Dell documentation:

"STATUS" CHANNEL	"MODE" CHANNEL	DESCRIPTION
Optimal (status: up)	Unassigned (status: up)	The physical disk in the indicated slot is unused and available to be configured.
	Assigned (status: up)	The physical disk in the indicated slot is configured as part of a disk group.
	Hot Spare Standby (status: up)	The physical disk in the indicated slot is configured as a hot spare.
	Hot Spare In Use (status: up)	The physical disk in the indicated slot is in use as a hot spare within a disk group.
Failed (status: down)	▪ Assigned ▪ Unassigned ▪ Hot Spare In Use ▪ Hot Spare Standby	The physical disk in the indicated slot has been failed because of an unrecoverable error, an incorrect drive type or drive size, or by its operational state being set to failed.
Replaced (status: up)	Assigned	The physical disk in the indicated slot has been replaced and is ready to be, or is actively being, configured into a disk group.
Pending Failure (status: down)	▪ Assigned ▪ Unassigned ▪ Hot Spare In Use ▪ Hot Spare Standby	A SMART error has been detected on the physical disk in the indicated slot.

"STATUS" CHANNEL	"MODE" CHANNEL	DESCRIPTION
None (status: warning)	None (status: warning)	The indicated slot is empty, or the array cannot detect the physical disk.
Undefined (status: down)		



Dell PowerVault MDi Physical Disk Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/dell_powervault_mdi_physical_disk.png

Remarks

- Works with Dell PowerVault MD3000i, MD3420, MD3620i, MD3000f, MD3620f, or MD3820i, and might support other models.
- Requires 618 Dell Modular Disk Storage Manager on the probe system. Please see the Knowledge Base: Where do I find the Dell PowerVault Modular Disk Storage Manager for use with my MDi SAN?
- Needs the IP address of the Storage Area Network (SAN) defined in the parent device settings.
- This sensor supports devices with one drawer of hard-drives only. Multiple drawers are not supported and prevent sensor creation.

- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.
- Currently, this sensor type is in beta status. The methods of operating can change at any time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Requirement: Dell Modular Disk Storage Manager

This sensor requires the installation of the Dell Modular Disk Storage Manager program. You have to install it on the computer running the PRTG probe: Either on the local system (on every node, if on a cluster probe), or on the system running the remote probe 3196. For details about setup, please see **More** section below.

Create this sensor on a device that has the SAN's IP address configured in the **IP Address/ DNS Name** field of the sensor settings.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the physical disks you want to monitor. PRTG will create one sensor for each disk you select in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SENSOR SETTINGS

Physical Disks	Select the disks you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SETTINGS

Physical Disks	Shows the disk that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result.

SENSOR SETTINGS

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section **Data Storage** 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.
- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Where do I find the Dell PowerVault Modular Disk Storage Manager for use with my MDi SAN?

- https://kb.paessler.com/en/topic/38743

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

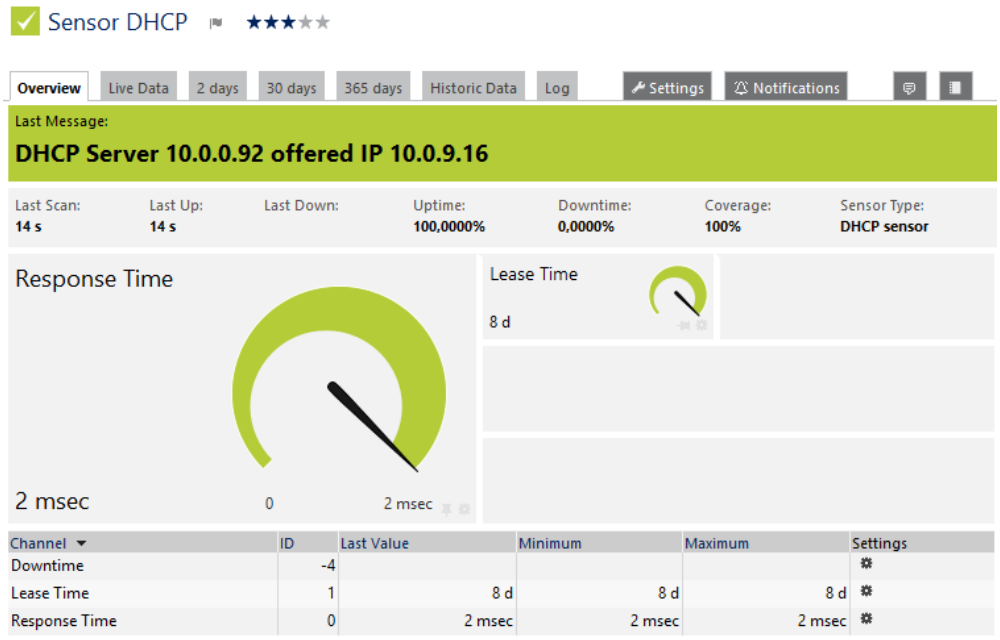
For more general information about settings, please see the **Object Settings** 188 section.

7.8.23 DHCP Sensor

The DHCP sensor monitors a Dynamic Host Configuration Protocol (DHCP) server. It sends a broadcast message to the network and waits for a DHCP server to respond. When creating this sensor, choose the network card on the probe system that will be used to send the broadcast message.

If a server responds, the sensor shows the following:

- Address of the server and the offered IP in the sensor message. You can check the server's response using **Regular Expressions** 3193.
- Response time (msec)
- Lease time given by the server (in days)



DHCP Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/dhcp.png

Remarks

- You can create this sensor only on a probe device (either local probe, a remote probe, or a cluster probe).
- The probe device where you create a DHCP sensor must have a static IP address. It cannot get its IP address from DHCP because this can cause a DHCP failure which will result in a severe issue for the probe device and you risk losing monitoring data.
- Do not use more than 2 DHCP sensors per device. Otherwise your DHCP sensors will show a timeout error.
- Knowledge Base: How can I monitor a DHCP server in a specific network if there are several DHCP networks?

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the desired network interfaces to monitor DHCP servers. PRTG will create one sensor for each network interface you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

DHCP SPECIFIC

Specify Network Interface	Select the network adapters you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DHCP SPECIFIC

MAC	Shows the MAC address of the network adapter that is used to send the broadcast message to the network. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Client IP	Specify if you want to check the returned client IP with a regular expression. Choose between: ▪ **Don't check**: The IP will only appear in the sensor message without further processes. ▪ **Check**: Enter the regular expression you want to use below.
Client IP Must Include	This field is only visible if you choose to **Check** the client IP above. In the response of the DHCP server, search using a regular expression. If the answer for the client IP does not contain the defined string, the sensor shows a **Down** status 163. For example, enter 10\.0\.5\..* to make sure any answering DHCP server returns an client IP address starting with "10.0.5.". If it does not, the sensor will show an error. For more details, see **Regular Expressions** 3193 section. Leave empty to not use this field.
Client IP Must Not Include	This field is only visible if you choose to check the client IP above. In the response of the DHCP server, search using a regular expression. If the answer for the client IP contains the defined string, the sensor shows a **Down** status.

DHCP SPECIFIC

	See example above. For more details, see **Regular Expressions** [3193] section. Leave empty to not use this field.
Server IP	Specify if you want to check the returned server IP with a regular expression. Choose between: ▪ **Don't check**: The IP will only appears in the sensor message without further processes. ▪ **Check**: Enter the regular expression you want to use below.
Server IP Must Include	This field is only visible if you choose to check the server IP above. In the response of the DHCP server, search using a regular expression. If the answer for the server IP does not contain the defined string, the sensor shows a **Down** status. See example above. For more details, see **Regular Expressions** [3193] section. Leave empty to not use this field.
Server IP Must Not Include	This field is only visible if you choose to check the server IP above. In the response of the DHCP server, search using a regular expression. If the answer for the server IP contains the defined string, the sensor shows a **Down** status. See example above. For more details, see **Regular Expressions** [3193] section. Leave empty to not use this field.
Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).
DHCP Server Change	If there is more than one DHCP server in the network that may answer to the broadcast message, the sensor can receive an answer from a different DHCP server, compared to the last scan of the sensor. In this case, PRTG can write an entry to the system Logs [198]. Choose between: ▪ **Ignore**: Do not write a log entry if the DHCP server changes. ▪ **Write log entry**: Write an entry to the system **Logs** whenever the DHCP server changes between two sensor scans. ⓘ Regardless of this setting, those entries will always be added to the sensor **Log**.
Offered IP Change	If the IP address offered by the DHCP server changes between two sensor scans, PRTG can write an entry to the system Logs [198]. Choose between:

DHCP SPECIFIC

- **Ignore**: Do not write a log entry if the offered IP address changes.
- **Write log entry**: Write an entry to the system **Logs** whenever the DHCP server offers a different IP address compared to the last sensor scan.

Regardless of this setting, those entries will always be added to the sensor **Log**.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.
- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. ⓘ Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: How can I monitor a DHCP server in a specific network if there are several DHCP networks?

- https://kb.paessler.com/en/topic/64601

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

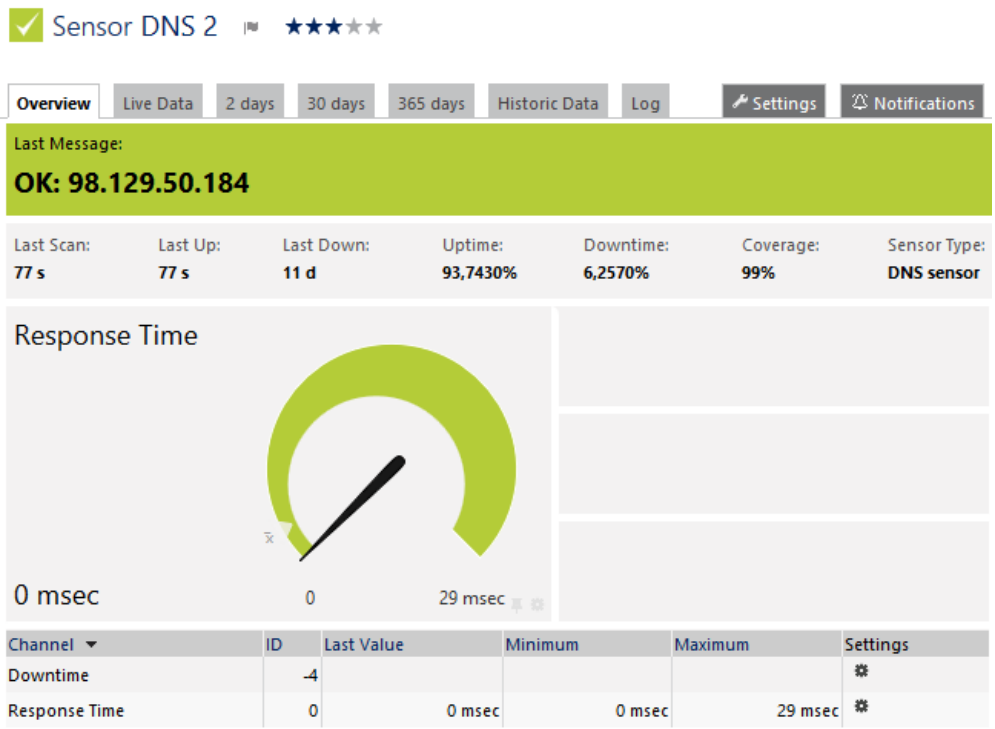
Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.24 DNS Sensor

The DNS sensor monitors a Domain Name Service (DNS) server. It resolves a domain name and compares it to a given IP address.

- The sensor shows the response time of the DNS server.
- It will show a **Down** status 163 if the DNS server does not resolve a given domain name correctly.



DNS Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/dns.png

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DNS SPECIFIC

Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).
Port	Enter the number of the port to which the sensor tries to connect. This must be the port the sensor's parent device is running the DNS service on. Usually you will use port **53**. We recommend that you use the default value. ⓘ The sensor connects to the **IP Address** or **DNS Name** value of the device 360 on which you create it.

DNS SPECIFIC

Domain	Enter the domain name that the sensor resolves using the Domain Name Service (DNS) server specified in the sensor's parent device settings. You can enter an internet domain name here (for example, example.com) or a DNS name in your internal network (such as computer-xyz), depending on the type of DNS server you monitor. You can also enter an IP address here, but there might occur an error with certain query types.
Query Type	Select the type of query that the sensor sends to the DNS server. Choose between: ▪ **Host address IPv4 (A)** ▪ **Host address IPv6 (AAAA)** ▪ **Authoritative name server (NS)** ▪ **Start of a zone of authority marker (SOA)** ▪ **Domain name pointer (PTR)** ▪ **Mail exchange (MX)** ▪ **Canonical name for an alias (CNAME)**
Check Result	Define if the sensor checks the result from the DNS server. Choose between: ▪ **Ignore result**: Accept any valid answer of the DNS server. ▪ **Check result**: Check if the response contains certain strings. Define below.
Value	This field is only visible if you enable result checking above. Enter elements that the response of the DNS server must contain. Enter each entry in one line. The received result must contain at least one of the elements. If none of the element matches the response, the sensor will show a red **Down** status. For example, you can enter an IP address here if your **Domain** field contains a host name. Only if the host name is resolved to the correct IP address, your sensor will show a green **Up** status.
Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result.

DNS SPECIFIC

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section Data Storage 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. ⓘ Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

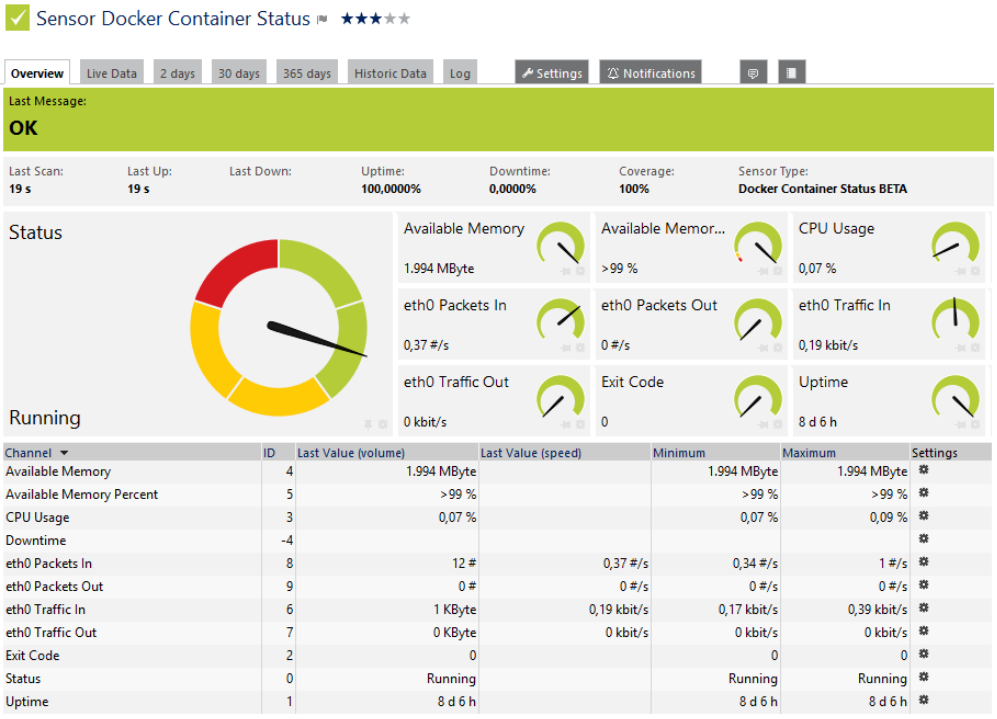
Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.25 Docker Container Status Sensor

The Docker Container Status sensor monitors the status of a Docker container. It can show the following:

- Overall status of the container (create, running, paused, restarting, exited)
- Uptime
- Exit code
- CPU usage
- Available memory in bytes and percent



Channel	ID	Last Value (volume)	Last Value (speed)	Minimum	Maximum	Settings
Available Memory	4	1.994 MByte		1.994 MByte	1.994 MByte	
Available Memory Percent	5	>99 %		>99 %	>99 %	
CPU Usage	3	0,07 %		0,07 %	0,09 %	
Downtime	-4					
eth0 Packets In	8	12 #	0,37 #/s	0,34 #/s	1 #/s	
eth0 Packets Out	9	0 #	0 #/s	0 #/s	0 #/s	
eth0 Traffic In	6	1 KByte	0,19 kbit/s	0,17 kbit/s	0,39 kbit/s	
eth0 Traffic Out	7	0 KByte	0 kbit/s	0 kbit/s	0 kbit/s	
Exit Code	2	0		0	0	
Status	0	Running		Running	Running	
Uptime	1	8 d 6 h		8 d 6 h	8 d 6 h	

Docker Container Status Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/docker_container_status.png

Remarks

- The parent device for this sensor must be the Docker machine on which the container runs that you want to monitor.
- You need to provide certificates and private keys to monitor Docker with this sensor. For details, see the Knowledge Base: How can I create private key and certificate for the Docker sensor?
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.

- Currently, this sensor type is in beta status. The methods of operating can change at any time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.

BETA

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

PRTG requires an authentication with certificate and private key before you can actually add this sensor. Provide **Port** (usually **2375**), **Private Key**, and **Certificate** in the appearing dialog window and click **OK**. PRTG can now scan Docker for existing containers.

Select which Docker containers you want to monitor. PRTG creates one sensor for each container you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

DOCKER SPECIFIC

Container	Select the containers you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items. To better find what you want to monitor, especially in large tables, use the search function in the upper-right corner.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DOCKER CREDENTIALS

Port	Enter the number of the port to which this sensor connects. The default port on which Docker over TLS runs is **2376**.
Private Key	Provide the private key for the connection to Docker. If you have already created a key, you can use it here. Otherwise, please create a certificate on Docker first. See this Knowledge Base article on how to create a Docker certificate: https://kb.paessler.com/en/topic/67250 Open the key with a text editor, copy everything that the file includes, and paste it here. Usually, the key starts with -----BEGIN RSA PRIVATE KEY----- and ends with -----END RSA PRIVATE KEY-----
Certificate	Provide the certificate for the connection to Docker. If you have already created a certificate, you can use it here. Otherwise, please create a certificate on Docker first. See this Knowledge Base article on how to create a Docker certificate: https://kb.paessler.com/en/topic/67250

DOCKER CREDENTIALS

Open the certificate with a text editor, copy everything that the file includes, and paste it here. Usually, the certificate starts with -----BEGIN CERTIFICATE----- and ends with -----END CERTIFICATE-----

DOCKER SPECIFIC

Container ID

Shows the ID of the container that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Container Name

Shows the name of the container that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Image

Shows the name of the image that was used to create the monitored Docker container. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Container Identification

Define how the sensor will identify the Docker container that it monitors. Choose between:

- **By container ID (default)**: Use the ID of the Docker container to identify it.
- **By container name**: Use the name of the Docker container to identify it. This is a good option if the IDs of your containers regularly change, for example, because of nightly deployments of your Docker containers.

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result**: Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section Data Storage 3226.

DOCKER SPECIFIC

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply. If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply. If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: How can I create private key and certificate for the Docker sensor?

- https://kb.paessler.com/en/topic/67250

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.26 Dropbox Sensor

The Dropbox sensor monitors a Dropbox account using the Dropbox Application Programming Interface (API) and OAuth2. It shows the following:

- Free storage in bytes and percent

Dropbox Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/dropbox.png

Remarks

- The minimum scanning interval for this sensor type is **30 minutes**.
- For details about OAuth2 authentication, please see manual section Authentication Using OAuth2 664.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

PRTG requires OAuth2 authorization before you can actually add this sensor type. Provide the requested credentials in the appearing window.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

DROPBOX CREDENTIALS

This sensor type uses OAuth2 authentication to get access to your Dropbox account.

For details about the authentication approach, please see section **Authentication Using OAuth2** 664.

OAuth URL	Click the button **Get Access Code** to connect this sensor to your Dropbox account using OAuth2. This is necessary to allow the sensor to query data from Dropbox. A new browser window appears. Please follow the steps there and confirm the permission for PRTG to connect to your Dropbox account. Copy the OAuth code you get and paste it into the **OAuth Code** field below.
OAuth Code	Paste the access code that you receive after completing the authorization process for PRTG at your Dropbox account. Click **OK** to define the sensor settings 840. It is mandatory to connect this sensor to your Dropbox account to create this sensor. Please complete the OAuth approach first to get the OAuth code.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	Enter one or more **Tags**, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DROPBOX CREDENTIALS

OAuth Code	Shows the authorization code that the sensor uses to get access to your Dropbox account. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. ⓘ You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.

SCANNING INTERVAL

- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

This sensor type has a fixed minimum scanning interval for performance reasons. You cannot run the sensor in shorter intervals than this minimum interval. Consequently, shorter scanning intervals as defined in **System Administration—Monitoring** 2955 are not available for this sensor.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

Authentication Using OAuth2

This sensor type uses the OAuth2 security protocol to access the account from which you want to retrieve and monitor data. OAuth2 enables you to grant access to the target account without sharing your password with PRTG. The authorization approach of PRTG using OAuth2 works as follows.

1. **Authorization Request**
   First, you have to request authorization for this sensor to access service resources from your account. For this purpose you are asked to get an access code for this sensor in the **Add Sensor** dialog. Click the **Get Access Code** button to start the authorization process using OAuth2. A new browser window will open on the authorization server of the target service.

2. **Verifying Identity**
   This new window contains a login form for your account that you want to monitor. Log in to your account using your credentials for this service to authenticate your identity. This is a common login to your account on the target server so PRTG will not see your password. The service will forward you to the authorization page and asks you to permit PRTG to access the data in your account.
   If you are already logged in to the service with a user account, you do not have to enter credentials in this step and get directly to the access permission page.

3. **Authorizing PRTG**
   Permit PRTG to access information on your account. Note that this permission holds only for this specific sensor, not for other sensors of this type or PRTG as a whole. For each sensor of this type you add, you have to confirm the access permission anew. You can change the account permissions at any time in your account at the target service.

4. **Getting Authorization Code**
   Permitting PRTG to access your account data forwards you to a page where the service provides an **authorization code**. Copy this code and switch back to the **Add Sensor** dialog in PRTG.
   The code is only valid a short period of time and expires after a few minutes. You can use a particular code only once.

5. **Providing Authorization Code**
   Paste the authorization code into the **OAuth Code** field and complete the **Add Sensor** dialog. You do not have to go through further configuration steps manually. The sensor will accomplish the following steps automatically.

6. **Requesting Access Token**
   After receiving the authorization code, PRTG will request an access token from the API of the target service. For this purpose, PRTG transmits the authorization code together with several authentication details. The API checks if the authorization is valid and returns the access token to PRTG. Access token are specific for one account and one application (here: PRTG). The authorization process to read data from your account is now complete.

7. **Retrieving Data**
   The sensor transmits the access token with each sensor scan in the defined scanning interval to authenticate with your account. It is not necessary to use the original account credentials anew. The used tokens will refresh automatically from time to time.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.27 Enterprise Virtual Array Sensor

The Enterprise Virtual Array sensor monitors an HP StorageWorks Enterprise Virtual Array (EVA) using the sssu.exe from HP Command View EVA Software.

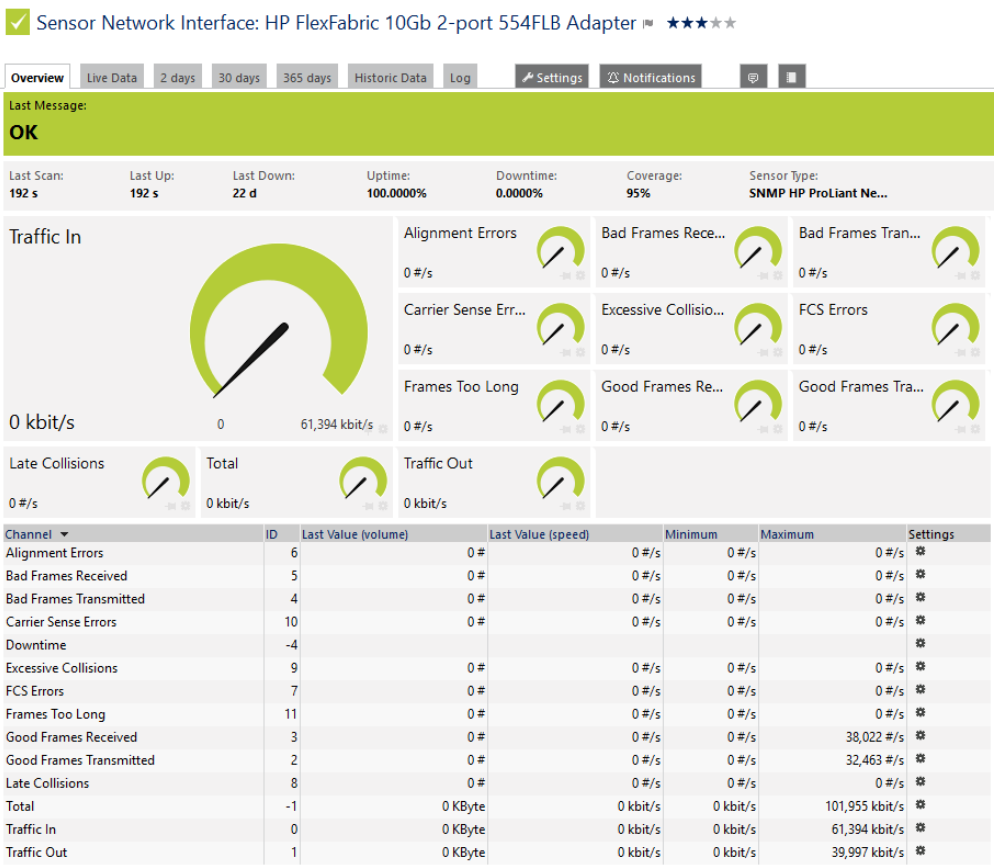
It can show the status of several EVA modules, depending on the available measurement components:

- System controllers
- Enclosures
- Disks
- Disk groups
- Folders
- Hosts
- Snapshots
- Data replication
- Cabinets
- If the devices have measuring tools for fans and temperature, the sensor displays corresponding data as well.

For these EVA components, this sensor type can show the following:

- Operational status
- Predicted failures
- Accessible media
- Allocation in percent
- Availability for VRaids in bytes
- Exaggerated bytes
- Group host access
- Number of grouped and ungrouped disks
- Age of snapshots
- License status

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



SNMP HP ProLiant Network Interface Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_hp_proliant_network_interface.png

Remarks

- You have to explicitly specify the credentials of the EVA in the sensor settings.
- Requires 668 the HP Command View EVA Software on the probe system (or the alternative below).
- Knowledge Base: Do I really have to install the whole Command View on the probe to use the EVA sensor?
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Requirement: Command View

The EVA sensor needs the HP Command View EVA Software to be installed on the probe system. If you do not want to install the whole command view tool, you can alternatively use another approach.

For details, please see this Knowledge Base article: https://kb.paessler.com/en/topic/55983

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

PRTG will perform a meta scan before you actually add this sensor type and requires basic information for this scan in advance. Provide the requested information in the appearing window. During the scan, PRTG will recognize all items available for monitoring based on your input. The following settings differ in comparison to the sensor's settings page:

EVA CREDENTIALS

Scanning Mode	Specify the depth of the meta scan. Choose between: ▪ **Basic**: We recommend using this scanning mode. Various modules of your EVA will be available for monitoring. ▪ **Full Detail**: PRTG will scan for each disk of your EVA. Every disk will be listed in the module selection.

Select which modules you want to monitor. PRTG will create one sensor for each module you choose. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

EVA SETTINGS

Modules	Select the modules you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

EVA CREDENTIALS

Username	Enter the username for the EVA.
Password	Enter the password for the EVA.

EVA SETTINGS

Module	Shows the monitored module. You can adjust this setting if the module was renamed or moved to another folder. This way, PRTG can find the module again and the monitoring history will not be lost.
System Module Type	Shows further information about the monitored module. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Description	
Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section **Data Storage** 3226. You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend

SENSOR DISPLAY

on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.
- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

SCANNING INTERVAL

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.

SCANNING INTERVAL

- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: Do I really have to install the whole Command View on the probe to use the EVA sensor?

- https://kb.paessler.com/en/topic/55983

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

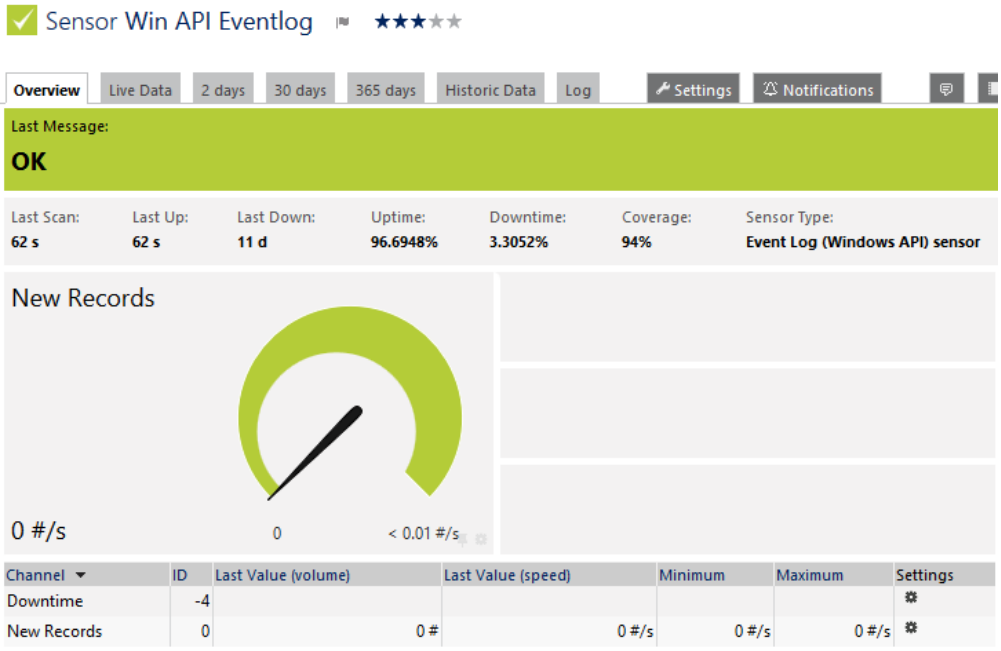
Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.28 Event Log (Windows API) Sensor

The Event Log (Windows API) sensor monitors Event Log entries using Windows Application Programming Interface (API).

- It shows the number of new records per second (speed).



Event Log (Windows API) Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/event_log_windows_api.png

Remarks

- Knowledge Base: My Event Log sensor ignores changes in the event log. What can I do?
- Knowledge Base: How can I configure sensors using speed limits to keep the status for more than scanning interval?
- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

WINDOWS API EVENT LOG SPECIFIC

Log File	Specify the log file that this sensor monitors. The Windows event log provides several different log files, which PRTG shows here. Choose between: ▪ **Application** ▪ **System**

WINDOWS API EVENT LOG SPECIFIC

- **Security**
- **Directory Service**
- **DNS Server**
- **File Replication Service**

FILTER EVENT LOG ENTRIES

Event Type	Specify the type of event that this sensor processes. Other event types cannot be processed. Choose between the following event types: ▪ **Any** ▪ **Error** ▪ **Warning** ▪ **Information** ▪ **Security Audit Success** ▪ **Security Audit Failure**
Filter by Source	Filter all received events for a certain event source. If you enable this option, this sensor only processes messages that match the defined value. Choose between: • **Off**: Do not filter by event source. • **On**: Enable filtering by event source.
Match String (Event Source)	This field is only visible if you enable source filtering above. Enter the source that the events come from. Only events from a source matching this string are regarded, other events are ignored. Please enter a string.
Filter by ID	Filter all received events for a certain event ID. If you enable this option, this sensor processes only messages that match the defined value(s). Choose between: • **Off**: Do not filter by event ID. • **On**: Enable filtering by event ID.

FILTER EVENT LOG ENTRIES

Match Values (Event ID)	This field is only visible if you enable ID filtering above. Enter an event ID that the events must have. Only events with an ID that matches this value are regarded. The **Event Log (Windows API) Sensor** 677 supports more than one event ID. Using this sensor type, you can enter a comma separated list of event IDs to filter for more than one ID. The **WMI Event Log Sensor** 2533 supports filtering for only one ID.
Filter by Category	Filter all received events for a certain event category. If you enable this option, this sensor only processes messages that match the defined value. Choose between: • **Off**: Do not filter by event category. • **On**: Enable filtering by event category.
Match String (Event Category)	This field is only visible if you enable category filtering above. Enter a category that the events must have. Only events with a category that matches this string are regarded. Please enter a string.
Filter by User	Filter all received events for a certain event user. If you enable this option, this sensor only processes messages that match the defined value. Choose between: • **Off**: Do not filter by event user. • **On**: Enable filtering by event user.
Match String (Event User)	This field is only visible if you enable user filtering above. Enter a username that the events must to be assigned to. Only events with a username that matches this string are regarded. Please enter a string.
Filter by Computer	Filter all received events for a certain event computer. If you enable this option, this sensor only processes messages that match the defined value. Choose between: • **Off**: Do not filter by event computer. • **On**: Enable filtering by event computer.
Match String (Event Computer)	This field is only visible if you enable computer filtering above. Enter a computer name that the events must be assigned to. Only events with a computer name that matches this string are regarded. Please enter a string.

FILTER EVENT LOG ENTRIES

Filter by Message	Filter all received events for a certain event message. If you enable this option, this sensor only processes messages that match the defined value. Choose between: • **Off**: Do not filter by event message. • **On**: Enable filtering by event message.
Match String (Event Message)	This field is only visible if you enable message filtering above. Enter a message that the event must contain. Only events with a message matching this string are regarded. Please enter a string.

The **Event Log (Windows API) Sensor** always performs a substring match. Please do not use any placeholder character. For example, enter **RAS** for any event source containing this string in partial or whole form.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: My Event Log sensor ignores changes in the event log. What can I do?

- https://kb.paessler.com/en/topic/59803

Knowledge Base: How can I configure sensors using speed limits to keep the status for more than one interval?

- https://kb.paessler.com/en/topic/73212

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

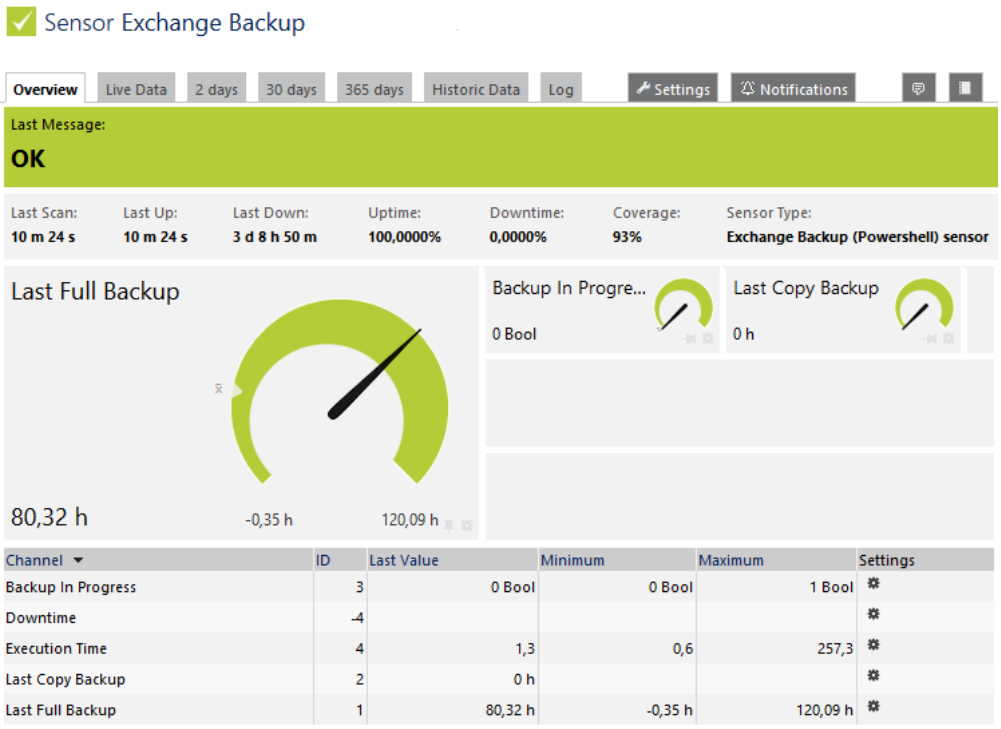
7.8.29 Exchange Backup (Powershell) Sensor

The Exchange Backup (Powershell) sensor monitors backups of an Exchange server using Remote PowerShell.

It can show several states of an Exchange database backup, for example:

- Past time since the last full backup
- Past time since the last copy backup
- If a backup is currently running

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Exchange Backup (Powershell) Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/exchange_backup.png

Remarks

- The parent device for this sensor must be the Exchange server (version 2010 or higher) that hosts the database you want to monitor.
- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- Requires 688 Remote PowerShell and Remote Exchange Management Shell on the target servers and PowerShell 2.0 on the probe system.

- Requires 688 the FQDN of the Exchange server in the parent device settings 360.
- Requires 688 .NET 4.0 or higher on the probe system.
- Knowledge Base: PowerShell Sensors: FAQ

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Requirement: Remote PowerShell and Remote Exchange Management Shell

This sensor type uses PowerShell commands. To monitor Exchange servers with this sensor, you have to enable **Remote PowerShell** and **Remote Exchange Management Shell** on the target servers which you want to monitor. Also ensure you have installed **PowerShell 2.0** or later on your probe machine.

In larger environments, the default memory limit for the remote shell might be insufficient. This might result in the error message The WSMan provider host process did not return a proper response. In this case, increase the memory limit for Remote PowerShell.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/44453

Requirement: Fully Qualified Domain Name (FQDN)

To connect to Exchange servers, this sensor type needs the **fully qualified domain name (FQDN)**. In PRTG's device settings of the Exchange server, provide the FQDN instead of the IP address.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/54353

Requirement: .NET Framework

This sensor type requires the Microsoft .NET Framework to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the remote probe 3196. If the framework is missing, you cannot create this sensor.

Required .NET version (with latest updates): .NET 4.0 (Client Profile is sufficient), .NET 4.5, or .NET 4.6.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/60543

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the Exchange server databases you want to monitor. PRTG creates one sensor for each database you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SENSOR SETTINGS

Exchange Databases	Select the databases you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.

BASIC SENSOR SETTINGS

Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SETTINGS

Database	Shows the name of the monitored database. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section Data Storage 3226. You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor.

SENSOR DISPLAY

- **Show channels independently (default)**: Show an own graph for each channel.
- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: Resolving Exchange PowerShell Sensors Issues

- https://kb.paessler.com/en/topic/54353

Knowledge Base: How do I enable and use remote commands in Windows PowerShell?

- https://kb.paessler.com/en/topic/44453

Knowledge Base: My Powershell sensor returns an error message. What can I do?

- https://kb.paessler.com/en/topic/59473

Knowledge Base: "No Logon Servers Available" when Using PowerShell Sensors

- https://kb.paessler.com/en/topic/59745

Knowledge Base: How can I increase memory for Remote PowerShell?

- https://kb.paessler.com/en/topic/61922

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

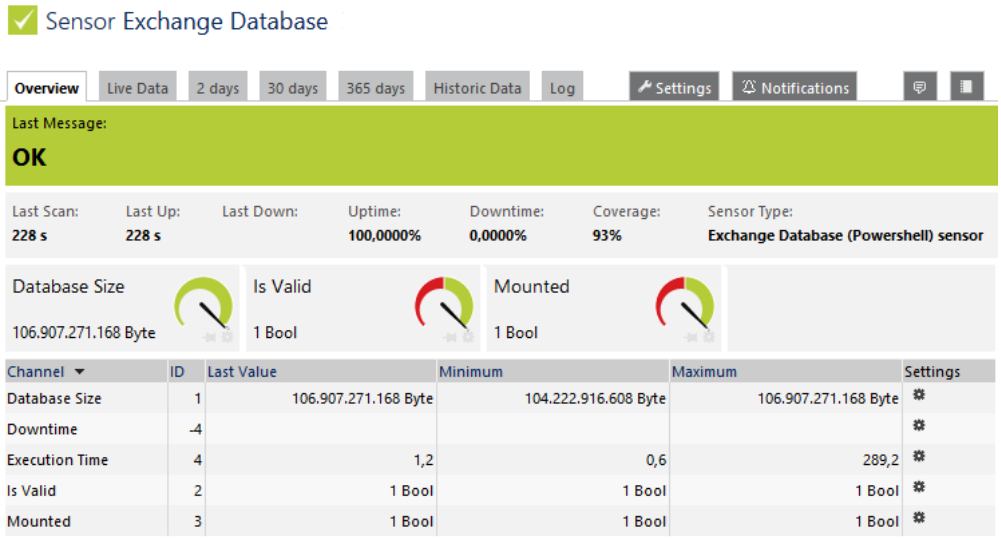
7.8.30 Exchange Database (Powershell) Sensor

The Exchange Database (Powershell) sensor monitors database information of an Exchange server using Remote PowerShell.

It shows several states of an Exchange database, for example:

- Database size
- If the database is mounted
- If the database is recognized as valid

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Exchange Database (Powershell) Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/exchange_database.png

Remarks

- The parent device for this sensor must be the Exchange server (version 2010 or higher) that hosts the database you want to monitor.
- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- Requires [698] Remote PowerShell and Remote Exchange Management Shell on the target servers and PowerShell 2.0 on the probe system.
- Requires [698] the FQDN of the Exchange server in the parent device settings [360].
- Requires [698] .NET 4.0 or higher on the probe system.
- Knowledge Base: PowerShell Sensors: FAQ
- Knowledge Base: How can I monitor additional values of Exchange databases?

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Requirement: Remote PowerShell and Remote Exchange Management Shell

This sensor type uses PowerShell commands. To monitor Exchange servers with this sensor, you have to enable **Remote PowerShell** and **Remote Exchange Management Shell** on the target servers which you want to monitor. Also ensure you have installed **PowerShell 2.0** or later on your probe machine.

In larger environments, the default memory limit for the remote shell might be insufficient. This might result in the error message The WSMan provider host process did not return a proper response. In this case, increase the memory limit for Remote PowerShell.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/44453

Requirement: Fully Qualified Domain Name (FQDN)

To connect to Exchange servers, this sensor type needs the **fully qualified domain name (FQDN)**. In PRTG's device settings of the Exchange server, provide the FQDN instead of the IP address.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/54353

Requirement: .NET Framework

This sensor type requires the Microsoft .NET Framework to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the remote probe 3196. If the framework is missing, you cannot create this sensor.

Required .NET version (with latest updates): .NET 4.0 (Client Profile is sufficient), .NET 4.5, or .NET 4.6.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/60543

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the Exchange server databases you want to monitor. PRTG creates one sensor for each database you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SENSOR SETTINGS

Exchange Databases	Select the databases you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SETTINGS

Database	Shows the name of the monitored database. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
AutoRemount Database	Define if you want the sensor to try to remount the database automatically if it is unmounted. Choose between: ▪ **Try to remount** ▪ **Just report the current reading and keep unmounted**
Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section Data Storage 3226. You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.

SCANNING INTERVAL

- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies [2822] in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector [210] to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** [360] or in the superior **Group Settings** [334].

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: Resolving Exchange PowerShell Sensors Issues

- https://kb.paessler.com/en/topic/54353

Knowledge Base: How do I enable and use remote commands in Windows PowerShell?

- https://kb.paessler.com/en/topic/44453

Knowledge Base: My Powershell sensor returns an error message. What can I do?

- https://kb.paessler.com/en/topic/59473

Knowledge Base: "No Logon Servers Available" when Using PowerShell Sensors

- https://kb.paessler.com/en/topic/59745

Knowledge Base: How can I increase memory for Remote PowerShell?

- https://kb.paessler.com/en/topic/61922

Knowledge Base: How can I monitor additional values of Exchange databases?

- https://kb.paessler.com/en/topic/63229

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.31 Exchange Database DAG (Powershell) Sensor

The Exchange Database DAG (Powershell) sensor monitors the Database Availability Group (DAG) status of a database on an Exchange server using Remote PowerShell.

It can show the following:

- Overall DAG status (for example, if it is mounted, failed, suspended)
- Copy status (active, not active)
- Content index status (healthy, crawling, error)
- If activation is suspended
- If log copy queue is increasing
- If replay queue is increasing
- Length of copy queue
- Length of Replay queue
- Number of single page restores

Exchange Database DAG (Powershell) Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/exchange_database_dag.png

Remarks

- The parent device for this sensor must be the Exchange server (version 2010 or higher) that hosts the database you want to monitor.
- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- Requires 708 Remote PowerShell and Remote Exchange Management Shell on the target servers and PowerShell 2.0 on the probe system.
- Requires 708 the FQDN of the Exchange server in the parent device settings 360.
- Requires 709 .NET 4.0 or higher on the probe system.
- Knowledge Base: PowerShell Sensors: FAQ
- Knowledge Base: How can I monitor additional values of Exchange databases?
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Requirement: Remote PowerShell and Remote Exchange Management Shell

This sensor type uses PowerShell commands. To monitor Exchange servers with this sensor, you have to enable **Remote PowerShell** and **Remote Exchange Management Shell** on the target servers which you want to monitor. Also ensure you have installed **PowerShell 2.0** or later on your probe machine.

In larger environments, the default memory limit for the remote shell might be insufficient. This might result in the error message The WSMan provider host process did not return a proper response. In this case, increase the memory limit for Remote PowerShell.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/44453

Requirement: Fully Qualified Domain Name (FQDN)

To connect to Exchange servers, this sensor type needs the **fully qualified domain name (FQDN)**. In PRTG's device settings of the Exchange server, provide the FQDN instead of the IP address.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/54353

Requirement: .NET Framework

This sensor type requires the Microsoft .NET Framework to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the remote probe 3196. If the framework is missing, you cannot create this sensor.

Required .NET version (with latest updates): .NET 4.0 (Client Profile is sufficient), .NET 4.5, or .NET 4.6.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/60543

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the Exchange server databases you want to monitor. PRTG creates one sensor for each database you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SENSOR SETTINGS

Exchange Databases	Select the databases you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SETTINGS

Database	Shows the name of the monitored database. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section **Data Storage** 3226.

SENSOR SETTINGS

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply. If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply. If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: Resolving Exchange PowerShell Sensors Issues

- https://kb.paessler.com/en/topic/54353

Knowledge Base: How do I enable and use remote commands in Windows PowerShell?

- https://kb.paessler.com/en/topic/44453

Knowledge Base: My Powershell sensor returns an error message. What can I do?

- https://kb.paessler.com/en/topic/59473

Knowledge Base: "No Logon Servers Available" when Using PowerShell Sensors

- https://kb.paessler.com/en/topic/59745

Knowledge Base: How can I increase memory for Remote PowerShell?

- https://kb.paessler.com/en/topic/61922

Knowledge Base: How can I monitor additional values of Exchange databases?

- https://kb.paessler.com/en/topic/63229

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

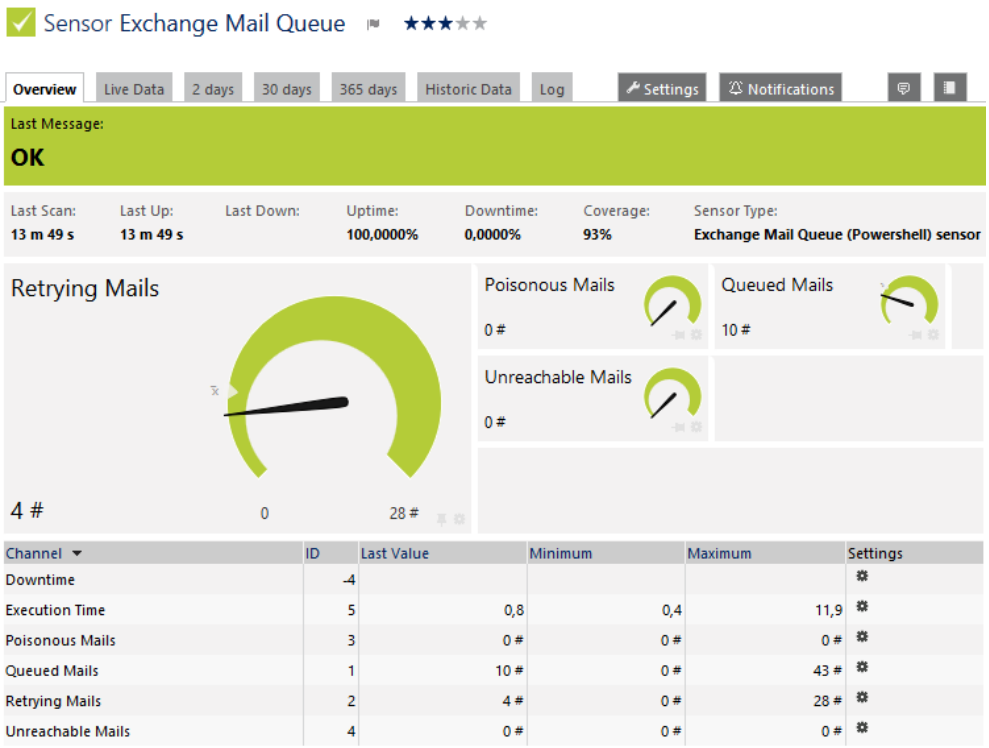
7.8.32 Exchange Mail Queue (Powershell) Sensor

The Exchange Mail Queue (Powershell) sensor monitors the number of items in the outgoing mail queue of an Exchange server using Remote PowerShell.

It can show, for example:

- Number of queued mails
- Number of retrying mails
- Number of unreachable mails
- Number of poisonous mails

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Exchange Mail Queue (Powershell) Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/exchange_mail_queue.png

Remarks

- The parent device for this sensor must be the Exchange server (version 2010 or higher) that hosts the database you want to monitor.
- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.

- Requires 718 Remote PowerShell and Remote Exchange Management Shell on the target servers and PowerShell 2.0 on the probe system.
- Requires 718 the FQDN of the Exchange server in the parent device settings 360.
- Requires 718 .NET 4.0 or higher on the probe system.
- Knowledge Base: PowerShell Sensors: FAQ
- Knowledge Base: What types of Exchange transport queues are there?

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Requirement: Remote PowerShell and Remote Exchange Management Shell

This sensor type uses PowerShell commands. To monitor Exchange servers with this sensor, you have to enable **Remote PowerShell** and **Remote Exchange Management Shell** on the target servers which you want to monitor. Also ensure you have installed **PowerShell 2.0** or later on your probe machine.

In larger environments, the default memory limit for the remote shell might be insufficient. This might result in the error message The WSMan provider host process did not return a proper response. In this case, increase the memory limit for Remote PowerShell.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/44453

Requirement: Fully Qualified Domain Name (FQDN)

To connect to Exchange servers, this sensor type needs the **fully qualified domain name (FQDN)**. In PRTG's device settings of the Exchange server, provide the FQDN instead of the IP address.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/54353

Requirement: .NET Framework

This sensor type requires the Microsoft .NET Framework to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the remote probe 3196. If the framework is missing, you cannot create this sensor.

Required .NET version (with latest updates): .NET 4.0 (Client Profile is sufficient), .NET 4.5, or .NET 4.6.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/60543

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the roles you want to monitor. PRTG creates one sensor for each role you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SENSOR SETTINGS

Hub-Transport or Edge-Server	Select the roles you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SETTINGS

Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section **Data Storage** 3226. You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

SENSOR DISPLAY

	You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

SCANNING INTERVAL

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: Resolving Exchange PowerShell Sensors Issues

- https://kb.paessler.com/en/topic/54353

Knowledge Base: How do I enable and use remote commands in Windows PowerShell?

- https://kb.paessler.com/en/topic/44453

Knowledge Base: My Powershell sensor returns an error message. What can I do?

- https://kb.paessler.com/en/topic/59473

Knowledge Base: "No Logon Servers Available" when Using PowerShell Sensors

- https://kb.paessler.com/en/topic/59745

Knowledge Base: How can I increase memory for Remote PowerShell?

- https://kb.paessler.com/en/topic/61922

Knowledge Base: What types of Exchange transport queues are there?

- https://kb.paessler.com/en/topic/55413

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

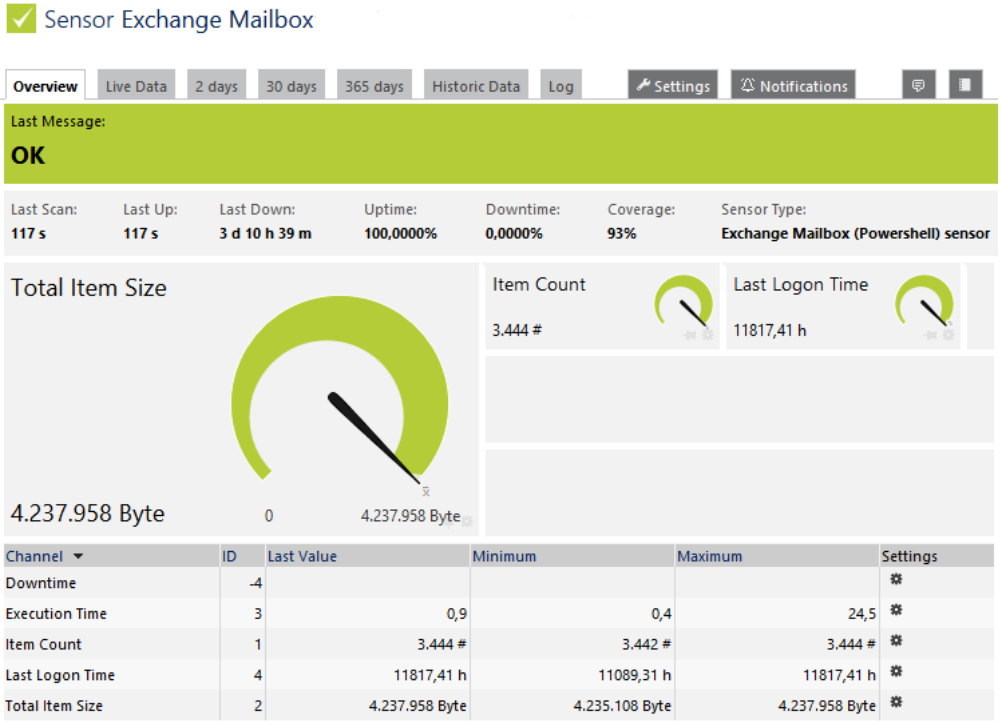
7.8.33 Exchange Mailbox (Powershell) Sensor

The Exchange Mailbox (Powershell) sensor monitors mailboxes of an Exchange server using Remote PowerShell.

It shows several states of a mailbox, for example:

- Total size of items in place
- Number of items in place
- Past time since the last mailbox logon

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Exchange Mailbox (Powershell) Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/exchange_mailbox.png

Remarks

- The parent device for this sensor must be the Exchange server (version 2010 or higher) that hosts the database you want to monitor.
- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- Requires 728 Remote PowerShell and Remote Exchange Management Shell on the target servers and PowerShell 2.0 on the probe system.

- Requires 728 the FQDN of the Exchange server in the parent device settings 360.
- Requires elevated rights for the user of this sensor on the Exchange system. It is not sufficient to have administrator rights. For details, please see the Knowledge Base: I have problems with the PowerShell Exchange sensors, what can I do? (solution (2) in the reply)
- Requires 728 .NET 4.0 or higher on the probe system.
- Knowledge Base: PowerShell Sensors: FAQ

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Requirement: Remote PowerShell and Remote Exchange Management Shell

This sensor type uses PowerShell commands. To monitor Exchange servers with this sensor, you have to enable **Remote PowerShell** and **Remote Exchange Management Shell** on the target servers which you want to monitor. Also ensure you have installed **PowerShell 2.0** or later on your probe machine.

In larger environments, the default memory limit for the remote shell might be insufficient. This might result in the error message The WSMan provider host process did not return a proper response. In this case, increase the memory limit for Remote PowerShell.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/44453

Requirement: Fully Qualified Domain Name (FQDN)

To connect to Exchange servers, this sensor type needs the **fully qualified domain name (FQDN)**. In PRTG's device settings of the Exchange server, provide the FQDN instead of the IP address.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/54353

Requirement: .NET Framework

This sensor type requires the Microsoft .NET Framework to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the remote probe 3196. If the framework is missing, you cannot create this sensor.

Required .NET version (with latest updates): .NET 4.0 (Client Profile is sufficient), .NET 4.5, or .NET 4.6.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/60543

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the Exchange server mailboxes you want to monitor. PRTG creates one sensor for each mailbox you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SENSOR SETTINGS

Mailboxes	Select the mailboxes you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SETTINGS

Mailbox Name	Shows the name of the monitored mailbox. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section **Data Storage** 3226. You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: Resolving Exchange PowerShell Sensors Issues

- https://kb.paessler.com/en/topic/54353

Knowledge Base: How do I enable and use remote commands in Windows PowerShell?

- https://kb.paessler.com/en/topic/44453

Knowledge Base: My Powershell sensor returns an error message. What can I do?

- https://kb.paessler.com/en/topic/59473

Knowledge Base: "No Logon Servers Available" when Using PowerShell Sensors

- https://kb.paessler.com/en/topic/59745

Knowledge Base: How can I increase memory for Remote PowerShell?

- https://kb.paessler.com/en/topic/61922

Knowledge Base: Which .NET version does PRTG require?

- https://kb.paessler.com/en/topic/60543

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

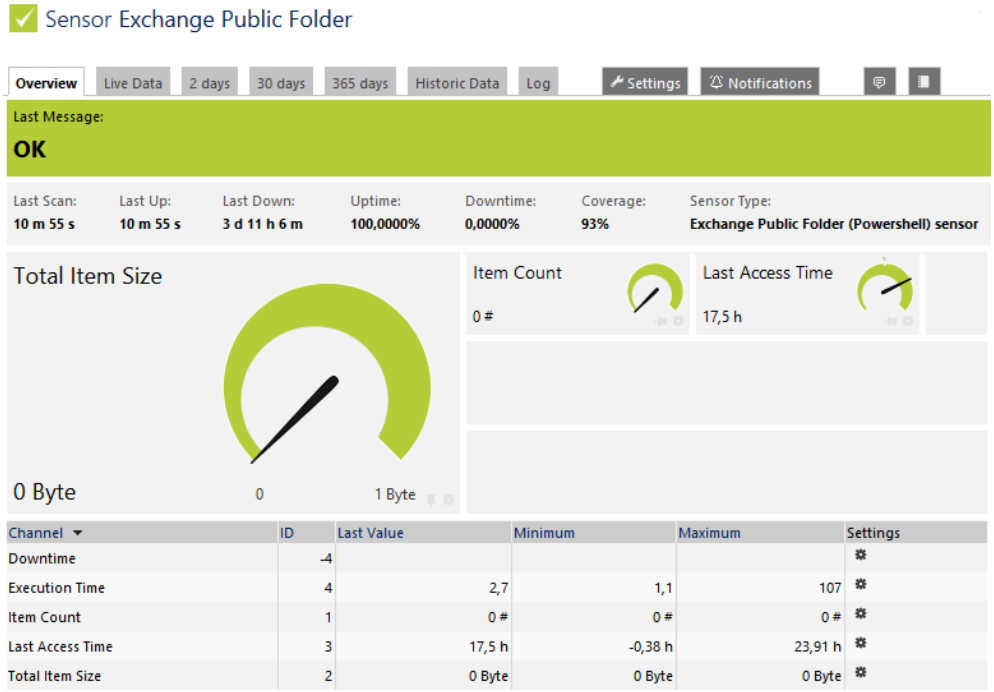
7.8.34 Exchange Public Folder (Powershell) Sensor

The Exchange Public Folder (Powershell) sensor monitors public folders of an Exchange server using Remote PowerShell.

It can show several states of a public folder, for example:

- Total size of items in place
- Number of items in place
- Past time since the last access

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Exchange Public Folder (Powershell) Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/exchange_public_folder.png

Remarks

- The parent device for this sensor must be the Exchange server (version 2010 or higher) that hosts the database you want to monitor.
- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- Requires 738 Remote PowerShell and Remote Exchange Management Shell on the target servers and PowerShell 2.0 on the probe system.
- Requires 738 the FQDN of the Exchange server in the parent device settings 360.

- Requires 738 .NET 4.0 or higher on the probe system.
- Knowledge Base: PowerShell Sensors: FAQ

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Requirement: Remote PowerShell and Remote Exchange Management Shell

This sensor type uses PowerShell commands. To monitor Exchange servers with this sensor, you have to enable **Remote PowerShell** and **Remote Exchange Management Shell** on the target servers which you want to monitor. Also ensure you have installed **PowerShell 2.0** or later on your probe machine.

In larger environments, the default memory limit for the remote shell might be insufficient. This might result in the error message The WSMan provider host process did not return a proper response. In this case, increase the memory limit for Remote PowerShell.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/44453

Requirement: Fully Qualified Domain Name (FQDN)

To connect to Exchange servers, this sensor type needs the **fully qualified domain name (FQDN)**. In PRTG's device settings of the Exchange server, provide the FQDN instead of the IP address.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/54353

Requirement: .NET Framework

This sensor type requires the Microsoft .NET Framework to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the remote probe 3196. If the framework is missing, you cannot create this sensor.

Required .NET version (with latest updates): .NET 4.0 (Client Profile is sufficient), .NET 4.5, or .NET 4.6.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/60543

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the Exchange server mailboxes you want to monitor. PRTG creates one sensor for each mailbox you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SENSOR SETTINGS

Public Folder	Select the folders you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.

BASIC SENSOR SETTINGS

Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SETTINGS

Public Folder	Shows the name of the monitored folder. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section Data Storage 3226. You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor.

SENSOR DISPLAY

- **Show channels independently (default)**: Show an own graph for each channel.
- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: Resolving Exchange PowerShell Sensors Issues

- https://kb.paessler.com/en/topic/54353

Knowledge Base: How do I enable and use remote commands in Windows PowerShell?

- https://kb.paessler.com/en/topic/44453

Knowledge Base: My Powershell sensor returns an error message. What can I do?

- https://kb.paessler.com/en/topic/59473

Knowledge Base: "No Logon Servers Available" when Using PowerShell Sensors

- https://kb.paessler.com/en/topic/59745

Knowledge Base: How can I increase memory for Remote PowerShell?

- https://kb.paessler.com/en/topic/61922

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

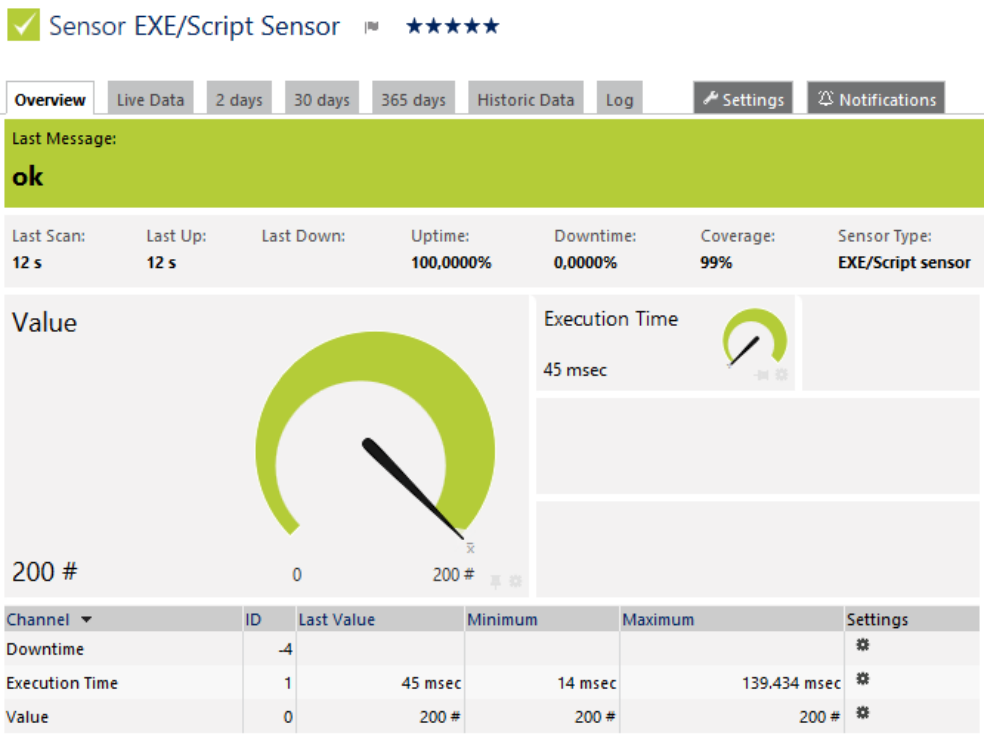
For more general information about settings, please see the **Object Settings** 188 section.

7.8.35 EXE/Script Sensor

The EXE/Script sensor runs an executable file (EXE, DLL) or a script (batch file, VBScript, Powershell) on the computer running the local or remote probe. This option is provided as part of the PRTG Application Programming Interface (API). For details about the return value format please see the **Application Programming Interface (API) Definition** 3174.

This sensor can show the following:

- One value returned by the executable file or script (in one channel only)
- Execution time



EXE/Script Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/exe_script.png

Remarks

- The executable or script file must be stored on the system of the probe the sensor is created on: If used on a remote probe, the file must be stored on the system running the remote probe. In a cluster setup, please copy the file to every cluster node.
- We recommend Windows 2012 R2 on the probe system for best performance of this sensor.
- If you want to execute a custom Windows Management Instrumentation Query Language (WQL) script, please use the **WMI Custom Sensor** 2512.
- Knowledge Base: What is the Mutex Name in PRTG's EXE/Script Sensor's settings?

- Knowledge Base: How can I test if parameters are correctly transmitted to my script when using an EXE/Script sensor?
- Knowledge Base: How can I show special characters with EXE/Script sensors?

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SENSOR SETTINGS

Script

Select an executable file from the list. The sensor will execute it with every scanning interval.

In this list, files in the corresponding **\Custom Sensors\EXE** sub-directory of the probe system's PRTG program directory are shown (see **Data Storage** 3226). To appear in this list, store the file into this folder ending in BAT, CMD, DLL, EXE, PS1, or VBS. To show the expected sensor values and status, your files must use the correct format for the returned values (in this case, value:message to standard output). The exit code of the file determines the sensor status 163.

For detailed information on how to build custom sensors and for the expected return format, please see the API documentation in your PRTG installation. There you will find detailed information on the **Custom Sensors** tab. See also manual section **Application Programming Interface (API) Definition** 3174 for more information.

When using custom sensors on the **Cluster Probe**, please copy your files to every cluster node installation.

Value Type

Define what kind of values your executable or script file gives back. Choose between:

- **Integer**: An integer is expected as return value. If the script gives back a float, PRTG will display the value **0**.
- **Float:** A float is expected as return value, with a dot (.) between pre-decimal position and decimal places. In this setting, the sensor will also display integer values unless they produce a buffer overflow.
- **Counter:** Your script returns an integer which increases. PRTG will show the difference between the values of two sensor scans.
  A counter must return an integer, float is not supported.

The sensor cannot handle string values.

Channel Name

Enter a name for the channel in which the sensor shows returned values. Please enter a string. This is for display purposes only. You can change the name later in the sensor's channel settings 2782.

Unit String

Enter a string that describes the unit of the returned values. Please enter a string. This is for display purposes only. You can change the name later in the sensor's channel settings 2782.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SETTINGS

EXE/Script	Shows the executable or script file that the sensor executes with each sensor scan as defined on sensor creation. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR SETTINGS

Parameters

If your executable or script file catches command line parameters, you can define them here. You can use placeholders as well.

For a full list of all placeholders please see the API documentation: **Application Programming Interface (API) Definition** 3174)

Note: Please make sure you write the placeholders in quotes to ensure that they are working properly if their values contain blanks. Use single quotation marks '' with PowerShell scripts, and double quotes "" with all others. Please enter a string or leave the field empty.

Environment

Choose if PRTG's command line parameters will also be available as environment parameters.

- **Default Environment**: Do not provide PRTG placeholders' values in the environment. Choose this secure option if you are not sure.
- **Set placeholders as environment values**: From within your executable or script, the values of PRTG's command line parameters will be available via environment variables. For example, you can then read and use the current host value of the PRTG device this EXE/script sensor is created on from within your script. This option can mean a security risk, because also credentials are provided in several variables.
  For a full list of all available variables, please see the API documentation in your PRTG installation. See manual section **Application Programming Interface (API) Definition** 3174 for more information.

Security Context

Define the Windows user account that the sensor uses to run the executable or script file. Choose between:

- **Use security context of probe service**: Run the selected file under the same Windows user account the probe runs on. By default, this is the Windows system user account (if not manually changed).
- **Use Windows credentials of parent device**: Use the Windows user account defined in the settings of the parent device this sensor is created on. Please open the parent device settings 360 of this sensor to change these Windows credentials.

Mutex Name

Define any desired mutex name for the process. All EXE/Script sensors having the same mutex name will be executed serially (not simultaneously). This is useful if you use a lot of sensors and want to avoid high resource usage caused by processes running simultaneously. Please enter a string or leave the field empty.

SENSOR SETTINGS

For more information, please see this Knowledge Base article: http://kb.paessler.com/en/topic/6673

Timeout (Sec.)

Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).

Value Type

Shows the expected value type that you chose on sensor creation. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

The sensor cannot handle string values.

If Value Changes

Define what this sensor will do when the sensor value changes. You can choose between:

- **Ignore changes (default)**: The sensor takes no action on change.
- **Trigger 'change' notification**: The sensor sends an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification 2791 whenever the sensor value changes.

EXE Result

Define what this sensor will do with the result that the executable file gives back. Choose between:

- **Discard EXE result**: Do not store the script result.
- **Write EXE result to disk**: Store the last result received from the script to the **Logs (Sensors)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File name: Result of Sensor [ID].txt. This is for debugging purposes. The file will be overridden with each scanning interval.
  For information on how to find the folder used for storage, see section **Data Storage** 3226.
- **Write EXE result to disk in case of error**: Store the last result received from the script only if the sensor is in a down status. File name: Result of Sensor [ID].txt, located in the **Logs (Sensors)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). Enable this option if you do not want failures to be overwritten by a following success of the script.

SENSOR SETTINGS

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply. If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply. If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Information about custom scripts and executables

- **Application Programming Interface (API) Definition** 3174
- **Additional Sensor Types (Custom Sensors)** 2778

Knowledge Base: What is the Mutex Name in PRTG's EXE/Script Sensor's settings?

- https://kb.paessler.com/en/topic/6673

Knowledge Base: How and Where Does PRTG Store its Data?

- https://kb.paessler.com/en/topic/463

Knowledge Base: How can I test if parameters are correctly transmitted to my script when using an EXE/Script sensor?

- https://kb.paessler.com/en/topic/11283

Knowledge Base: For which sensor types do you recommend Windows Server 2012 R2 and why?

- https://kb.paessler.com/en/topic/64331

Knowledge Base: How can I show special characters with EXE/Script sensors?

- https://kb.paessler.com/en/topic/64817

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

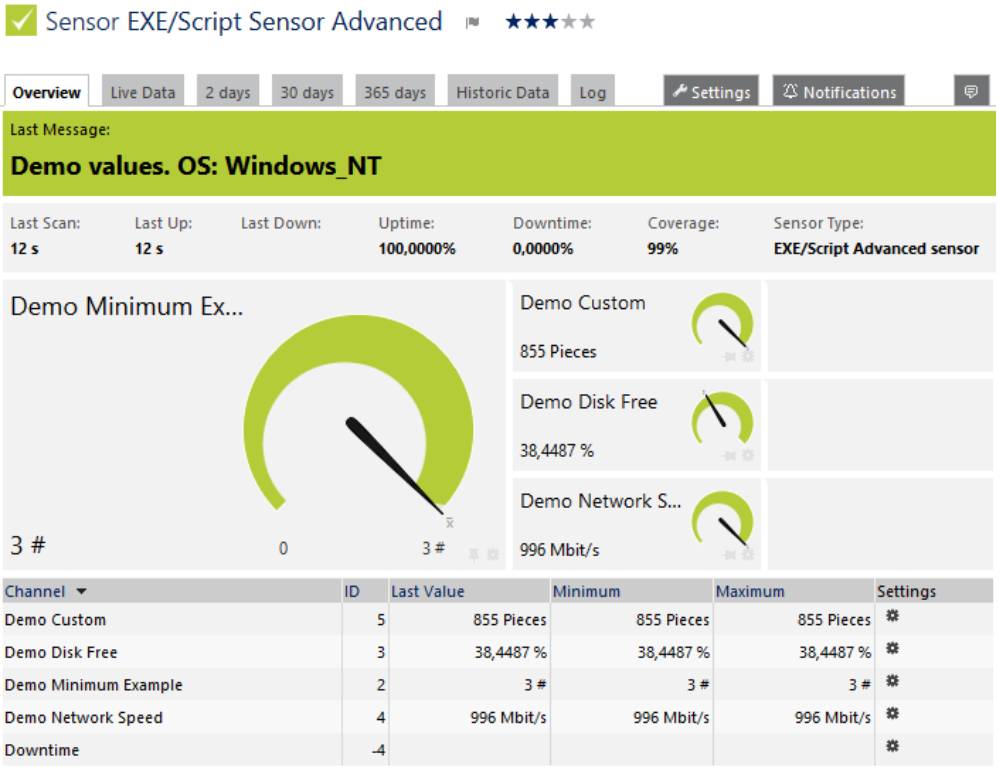
Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.36 EXE/Script Advanced Sensor

The EXE/Script Advanced sensor runs an executable file (EXE, DLL) or a script (batch file, VBScript, Powershell) on the computer running the local or remote probe. This option is provided as part of the PRTG Application Programming Interface (API). The return value of this sensor must be valid XML or JSON. For details about the return value format please see the **Application Programming Interface (API) Definition** 3174.

- The sensor can show values returned by the executable file or script in multiple channels.



EXE/Script Advanced Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/exe_script_advanced.png

Remarks

- This sensor does not support more than 50 channels 760 officially.
- The executable or script file must be stored on the system of the probe the sensor is created on: If used on a remote probe, the file must be stored on the system running the remote probe. In a cluster setup, please copy the file to every cluster node.
- We recommend Windows 2012 R2 on the probe system for best performance of this sensor.
- If you want to execute a custom Windows Management Instrumentation Query Language (WQL) script, please use the **WMI Custom Sensor** 2512.
- Knowledge Base: What is the Mutex Name in PRTG's EXE/Script Sensor's settings?
- Knowledge Base: How can I test if parameters are correctly transmitted to my script when using an EXE/Script sensor?

- Knowledge Base: How can I show special characters with EXE/Script sensors?
- Knowledge Base: How can I use meta-scans for custom EXE/Script sensors?

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Limited to 50 Sensor Channels

PRTG does not support more than 50 sensor channels officially. Depending on the data used with this sensor type, you might exceed the maximum number of supported sensor channels. In this case, PRTG will try to display all sensor channels. However, please be aware that you will experience limited usability and performance.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SENSOR SETTINGS

EXE/Script	Select an executable file from the list. The sensor will execute it with every scanning interval. This list shows all files available in the corresponding **\Custom Sensors\EXEXML** sub-directory of the probe system's PRTG program directory (see **Data Storage** 3226). To appear in this list, please store the files into this folder ending in BAT, CMD, DLL, EXE, PS1, or VBS. To show the expected values and sensor status, your files must return the expected XML or JSON format to standard output. Values and message must be embedded in the XML or JSON. For detailed information on how to build custom sensors and for the expected return format, please see the API documentation in your PRTG installation. There, find detailed information on the **Custom Sensors** tab. See also manual section **Application Programming Interface (API) Definition** 3174 for more information. When using custom sensors on the **Cluster Probe**, please copy your files to every cluster node installation.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SETTINGS

EXE/Script	Shows the executable or script file that the sensor executes with each scan as defined on sensor creation. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Parameters	If your executable or script file catches command line parameters, you can define them here. You can use placeholders as well.

SENSOR SETTINGS

For a full list of all placeholders, please see the API documentation in your PRTG installation. See manual section Application Programming Interface (API) Definition 3174 for more information.

Note: Please make sure you write the placeholders in quotes to ensure that they are working properly if their values contain blanks. Use single quotation marks '' with PowerShell scripts, and double quotes "" with all others. Please enter a string or leave the field empty.

Environment

Choose if PRTG's command line parameters will also be available as environment parameters.

- **Default Environment**: Do not provide PRTG placeholders' values in the environment. Choose this secure option if you are not sure.
- **Set placeholders as environment values**: From within your executable or script, the values of PRTG's command line parameters will be available via environment variables. For example, you can then read and use the current host value of the PRTG device this EXE/Script sensor is created on from within your script. This option can mean a security risk, because also credentials are provided in several variables.
  For a full list of all available variables please see the API documentation: Application Programming Interface (API) Definition 3174

Security Context

Define the Windows user account that the sensor uses to run the executable or script file. Choose between:

- **Use security context of probe service**: Run the selected file under the same Windows user account the probe is running on. By default, this is the Windows system user account (if not manually changed).
- **Use Windows credentials of parent device**: Use the Windows user account defined in the settings of the parent device this sensor is created on. Please open the parent device settings 360 of this sensor to change these Windows credentials.

Mutex Name

Define any desired mutex name for the process. All EXE/Script sensors having the same mutex name will be executed serially (not simultaneously). This is useful if you use a lot of sensors and want to avoid high resource usage caused by processes running simultaneously. Please enter a string or leave the field empty.

For more information, please see this Knowledge Base article: http://kb.paessler.com/en/topic/6673

SENSOR SETTINGS

Timeout (Sec.)

Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).

EXE Result

Define what the sensor will do with the results the executable file gives back. Choose between:

- **Discard EXE result**: Do not store the script result.
- **Write EXE result to disk**: Store the last result received from the script to the **Logs (Sensors)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File name: Result of Sensor [ID].txt. This is for debugging purposes. The file will be overridden with each scanning interval.
  For information on how to find the folder used for storage, see section Data Storage 3226.
- **Write EXE result to disk in case of error**: Store the last result received from the script only if the sensor is in a down status. File name: Result of Sensor [ID].txt, located in the **Logs (Sensors)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). Enable this option if you do not want failures to be overwritten by a following success of the script.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

The **Stack Unit** option for stacking graphs will only work if you explicitly define the same <unit> for at least two channels. For detailed information about sensor settings please see the API documentation: **Application Programming Interface (API) Definition** 3174

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Information about custom scripts and executables

- **Application Programming Interface (API) Definition** 3174
- **Additional Sensor Types (Custom Sensors)** 2778

Knowledge Base: What is the Mutex Name in PRTG's EXE/Script Sensor's settings?

- https://kb.paessler.com/en/topic/6673

Knowledge Base: How and Where Does PRTG Store its Data?

- https://kb.paessler.com/en/topic/463

Knowledge Base: How can I test if parameters are correctly transmitted to my script when using an EXE/Script sensor?

- https://kb.paessler.com/en/topic/11283

Knowledge Base: For which sensor types do you recommend Windows Server 2012 R2 and why?

- https://kb.paessler.com/en/topic/64331

Knowledge Base: How can I show special characters with EXE/Script sensors?

- https://kb.paessler.com/en/topic/64817

Knowledge Base: How can I use meta-scans for custom EXE/Script sensors?

- https://kb.paessler.com/en/topic/68109

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

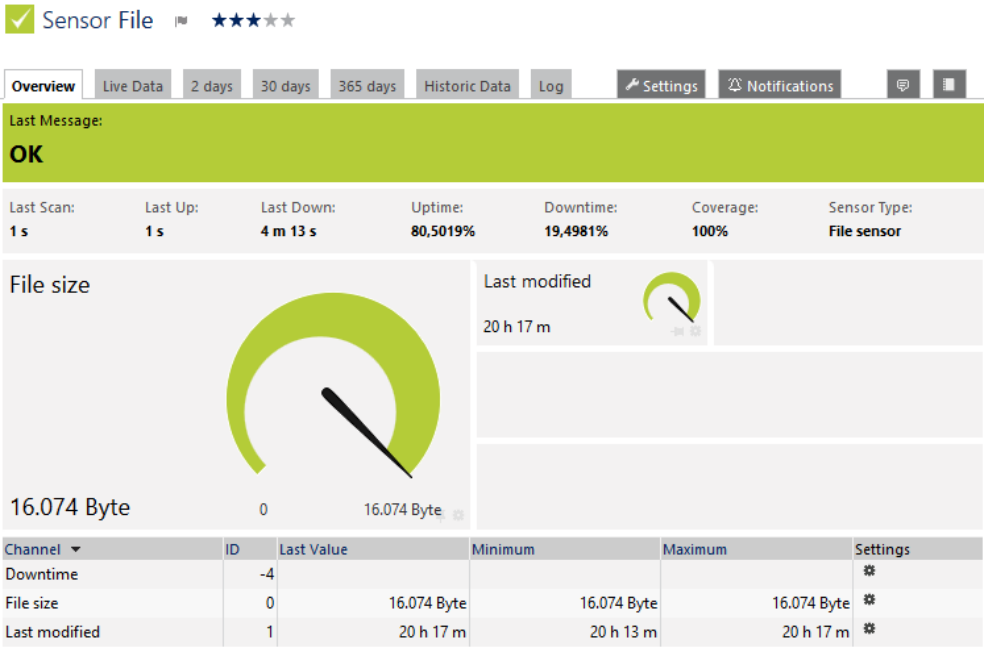
For more general information about settings, please see the **Object Settings** 188 section.

7.8.37 File Sensor

The File sensor monitors a file located on the local disk on the parent probe system, parent device, or a file accessible via Server Message Block (SMB). You can monitor changes to the file content and file time stamp.

It can show the following:

- File size
- Passed time since the file was modified the last time (in days, hours, and minutes, depending on the elapsed time)
- In contrast to the Folder sensor[789], you can also monitor if the actual content of a specific file has changed.



File Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/file.png

Remarks

- Requires[771] the LanmanServer ("Server") Windows service to be running on the target computer to monitor files on a share.
- Try using the Fully Qualified Domain Name (FQDN) of the target device if the sensor does not get a connection with the IP address.
- Knowledge Base: What can I do if PRTG doesn't succeed with monitoring a share? PE029 PE032

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Requirement: LanmanServer ("Server") Windows Service

To monitor files on Windows shares, please make sure the LanmanServer ("Server") Windows service is running on the target computer.

To enable the service, please log in to the respective computer and open the services manager (for example, via services.msc). In the list, find the respective service and set its Start Type to Automatic.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.

BASIC SENSOR SETTINGS

Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SPECIFIC

File Name	Enter the full path to the file that this sensor will monitor. For example, enter C:\Windows\file.txt to monitor a file on the parent probe system. If you use a local path, the sensor will only look for the target file on the system on which the parent probe runs, not on the parent device! To monitor a file on the parent device, use the dollar sign ($) like C$\User\johnqpublic\file.txt. If the file is located on a network device, use the Uniform Naming Convention (UNC) path without the server part: only enter share \folder\file.txt. The server part \\server\ is taken from the parent device settings 360 of this sensor. Enter a valid path and file name. To provide any shares, the LanmanServer "Server" Windows service must be running on the target computer.
Sensor Behavior	Specify when the sensor shows a **Down** status 163. Choose between: ▪ **Show 'Down' status if file does not exist**: The sensor will show an error if the file does **not** exist. ▪ **Show 'Down' status if file exists**: The sensor will show an error if the file does exist.
Monitor File Content	Specify if the sensor will send a change notification when the content of the file changes (based on a checksum). Choose between: ▪ **Ignore changes**: No action will be taken on change. ▪ **Trigger 'change' notification**: The sensor will send an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification 2791 whenever the sensor value changes.
Monitor File Time Stamp	Specify if the sensor will send a change notification when the content of the file's time stamp changes. Choose between:

SENSOR SPECIFIC

- **Ignore changes**: No action will be taken on change.
- **Trigger 'change' notification**: The sensor will send an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification [2791] whenever the sensor value changes.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.
- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** [2782] settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** [294] group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply. If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply. If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: What can I do if PRTG doesn't succeed with monitoring a share? PE029 PE032

- https://kb.paessler.com/en/topic/513

Knowledge Base: Can I use placeholders in file names to monitor log files?

- https://kb.paessler.com/en/topic/67965

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

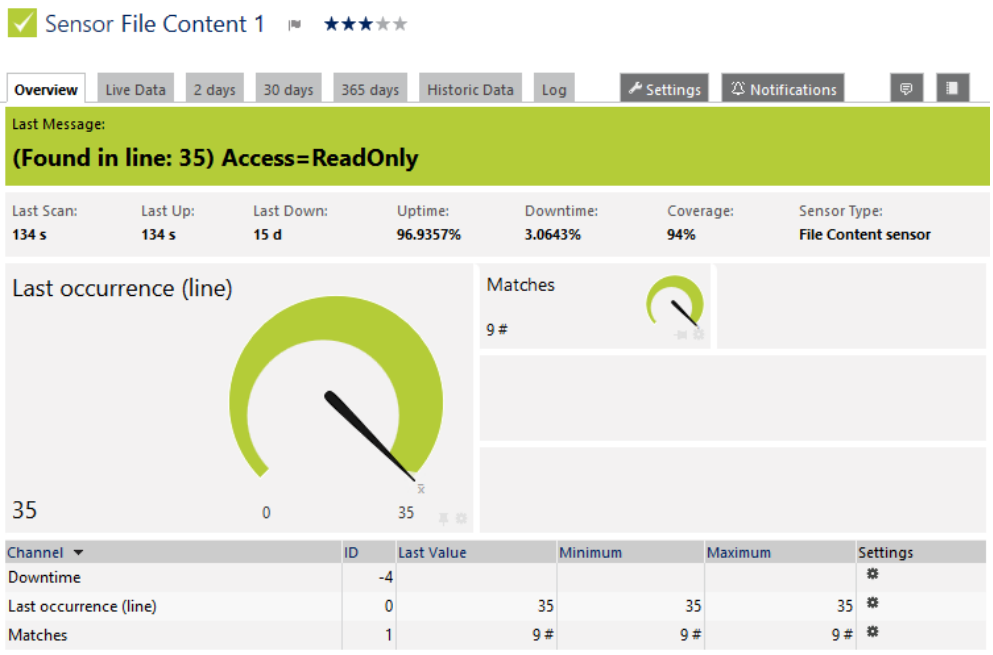
Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.38 File Content Sensor

The File Content sensor checks a text file (for example, logfiles) for certain strings and returns the following:

- Line number of the last match
- Number of total matches.
- Additionally, the sensor quotes matching lines in the sensor message field.



File Content Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/file_content.png

Remarks

- This sensor does not support UTF-16 encoded files! In this case, please try use a custom sensor like the EXE/Script Sensor 747 or the EXE/Script Advanced Sensor 759.
- This sensor does not support binary files officially! If you would still like to monitor binary files contrary to our recommendation, then please choose the option **Always transmit to PRTG the entire file** in section **Network Usage** in the sensor settings.
- This sensor supports Unix line feeds.
- Requires 780 the LanmanServer ("Server") Windows service to be running on the target computer to monitor files on a share.
- To monitor files on a Linux system, the folder has to be accessible via SMB.
- Try using the Fully Qualified Domain Name (FQDN) of the target device if the sensor does not get a connection with the IP address.

- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Requirement: LanmanServer ("Server") Windows Service

To monitor files on Windows shares, please make sure the LanmanServer ("Server") Windows service is running on the target computer.

To enable the service, please log in to the respective computer and open the services manager (for example, via services.msc). In the list, find the respective service and set its Start Type to Automatic.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	Enter one or more **Tags**, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SPECIFIC

File Name	Enter the full path to the file that this sensor will monitor. For example, enter C:\Windows\file.txt. to monitor a file on the parent probe system. If you use a local path, the sensor looks for the target file only on the system on which the parent probe runs, not on the parent device! To monitor a file on the parent device, use the dollar sign ($) like C$\User\johnqpublic\file.txt. If the file is located on a network device, use the Uniform Naming Convention (UNC) path without the server part (only enter share \folder\file.txt). The server part (\\server\) is taken from the parent device settings of this sensor. Enter a valid path and file name. To provide any Windows shares, the LanmanServer "Server" Windows service must run on the target computer. To monitor any Linux files, the folder with these files has to be accessible via Server Message Block (SMB). Please be aware that it might produce high network traffic if you define PRTG to query an entire file on your network with every scanning interval.
Search String	Define the string inside the logfile you want to check for. The input is not case-sensitive. Please enter a string.

SENSOR SPECIFIC

Network Usage	Define in which way the sensor will transmit the target file to PRTG. Choose between: ▪ **Only transmit to PRTG new lines at the end of the file (default)**: This option improves the performance of the sensor. It sends the whole file only with the first scan to PRTG. With the following sensor scans, the sensor will only transmit lines which were appended since the last scan. All other lines (which already existed in the previous scan) are not sent. The sensor assumes that they are unchanged and still counts them. BETA This option is currently in beta status. Please do not expect that it will work as expected in every usage scenario! ▪ **Always transmit to PRTG the entire file**: The sensor sends the whole file with every sensor scanning interval to PRTG. If this results in too much traffic on the target system, we recommend that you choose the new lines option. The sensor can only transmit newly added lines in the following cases: ▪ the file is bigger than at the previous scan, and ▪ the last line in the file at the previous scan still has to be at the same place in the file. The sensor supports Windows and Linux line endings (CRLF resp. LF).
Search Method	Define the method you want to provide the search string with. The pattern must be in one line and only the last matching line will be given back. Choose between: ▪ **Simple string search**: Search for a simple plain text expression. ▪ **Regular Expression**: Search using a regular expression. For more details, see this manual section: **Regular Expressions** 3193
File Encoding	Specify the encoding of the file that this sensor monitors. Choose between: ▪ **Windows-1252** ▪ **UTF-8** ▪ **UTF-16**
Warning Behavior	Define under which condition the sensor will show a **Warning** status 163. Choose between:

SENSOR SPECIFIC

- **Go into warning status when string is not found**: The sensor will show a **Warning** status if there is no match. Otherwise it will remain in **Up** status.
- **Go into warning status when string is found**: The sensor will show a **Warning** status if there is a match. Otherwise it will remain in **Up** status.

If Value Changes

Define what this sensor will do when the sensor value changes. You can choose between:

- **Ignore changes (default)**: The sensor takes no action on change.
- **Trigger 'change' notification**: The sensor sends an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification 2791 whenever the sensor value changes.

The change notification for this sensor is triggered if the value of the channel **Last occurrence (line)** changes. It is not triggered when the number of **Matches** changes.

DEBUG OPTIONS

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result**: Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section **Data Storage** 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.39 Folder Sensor

The Folder sensor monitors a folder using Server Message Block (SMB). You can monitor file changes and file ages.

It can show the following:

- Folder size in bytes
- Number of files in the folder
- Passed time since the last change to a file in the folder ("newest file")
- Passed time since the oldest modification of a file in the folder ("oldest file")

The Folder sensor counts all files in a folder, including hidden files.

Folder Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/folder.png

Remarks

- This sensor counts all files in a folder, including hidden files.
- Requires 790 the LanmanServer ("Server") Windows service to be running on the target computer to monitor shares.
- Knowledge Base: What can I do if PRTG doesn't succeed with monitoring a share? PE029 PE032

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Requirement: LanmanServer ("Server") Windows Service

To monitor shares on Windows machines, please make sure the LanmanServer ("Server") Windows service is running on the target computer.

To enable the service, please log in to the respective computer and open the services manager (for example, via services.msc). In the list, find the respective service and set its Start Type to Automatic.

Add Sensor

The **Add Sensor** dialog appears when you manually [288] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page. You can change the file age check later via the **Limits** section in the channel settings [2783] of **Newest File** and **Oldest File**.

FOLDER MONITOR

Check of File Ages	Specify if the sensor will monitor the folder for certain file ages and show a corresponding status [163]. Choose between: ▪ **Don't check**: Do not check for the age of the files in the specified folder(s). ▪ **Show Warning if older**: Set the sensor to **Warning** status if one of the files in the specified folder is older than a specific time unit. ▪ **Show Error if older**: Set the sensor to **Down** status if one of the files in the specified folder is older than a specific time unit. ▪ **Show Warning if younger**: Set the sensor to **Warning** status if one of the files in the specified folder is younger than a specific time unit. ▪ **Show Error if younger**: Set the sensor to **Down** status if one of the files in the specified folder is younger than a specific time unit.
File Age Limit	This field is only visible if you enable a file age check above. Enter the age of a file in the folder that will trigger the sensor status change if the defined age is undercut respectively exceeded. Please enter an integer value.

FOLDER MONITOR

	The value will be interpreted as days, hours, or minutes, according to your setting below.
File Age Limit Unit	This field is only visible if you enable a file age above. Specify the unit for the file age value that you entered above. Choose between: • **In days**: Choose this option if you entered a number of days in the field above. • **In hours**: Choose this option if you entered a number of hours in the field above. • **In minutes**: Choose this option if you entered a number of minutes in the field above.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

BASIC SENSOR SETTINGS

	You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

FOLDER MONITOR

Folder Name	Enter the full path to the folder this sensor will monitor. For example, enter C:\Windows. If the file is located on a network device, use the Uniform Naming Convention (UNC) path without the server part (you would only enter share\folder). The server part (\\server\) is taken from parent device settings 360 of this sensor. Please enter a valid path name. To monitor shares, the LanmanServer "Server" Windows service must be running on the target computer.
Subfolder Recursion	Specify if the sensor will include subfolders in the folder monitoring. Choose between: ▪ **Do not recurse subfolders**: Only monitor the folder specified above and do not monitor its subfolders. ▪ **Monitor the folder and its subfolders (use with caution!)**: Monitor the folder specified above and all of its subfolders. Recursing subfolders in large directories with a high number of branches may evoke timeout errors or performance issues.
Monitor Folder Changes	Specify if the sensor will send a change notification when the content of the folder changes. Choose between: ▪ **Ignore changes**: Changes to the folder will not trigger a change notification. ▪ **Trigger 'On Change' notification**: The sensor will trigger a change notification if a file changes its timestamp or filename, or if there are new or deleted files. Create a change trigger 2800 on the **Notifications** tab of this sensor to receive a notification whenever there is a change.

FOLDER MONITOR

Timeout	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).

DEBUG OPTIONS

Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section **Data Storage** 3226. You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel.

SENSOR DISPLAY

	▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. ⓘ This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.

SCANNING INTERVAL

- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: What can I do if PRTG doesn't succeed with monitoring a share? PE029 PE032

- https://kb.paessler.com/en/topic/513

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

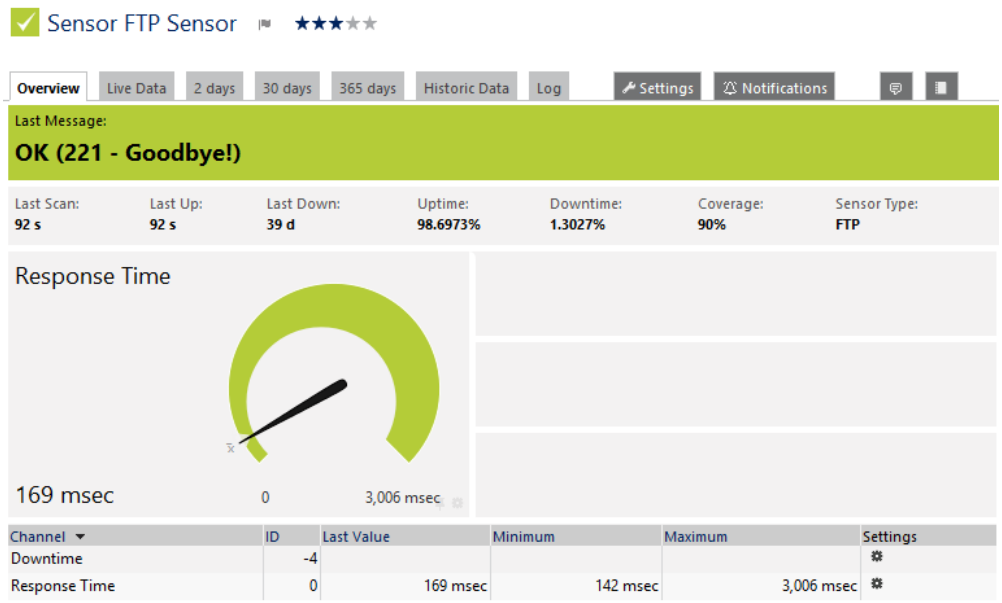
Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.40 FTP Sensor

The FTP sensor monitors file servers using File Transfer Protocol (FTP) and FTP over SSL (FTPS). It can show the following:

- Response time of the server
- Response message of the server



FTP Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/ftp.png

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SPECIFIC

Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).
Port	Enter the number of the port the sensor tries to connect to. Please enter an integer value. We recommend that you use the default value. If you cannot make a connection, please try another port number.
FTP Mode	Specify which FTP mode the sensor uses for the connection. Choose between: ▪ **Use active mode** ▪ **Use passive mode** We recommend that you use the default value. If you cannot make a connection, please try the passive mode.

TRANSPORT-LEVEL SECURITY

FTP Specific

Specify if the sensor uses encryption for the connection. Choose between:

- **Use Transport-Level Security if available**: The sensor tries to connect via TLS. It determines automatically whether to connect via explicit or implicit mode. If TLS is not supported by the server, the sensor will try connecting without encryption and show an **Up** status if this works.
- **Enforce Transport-Level Security**: The connection must be established using TLS (explicit or implicit mode). Otherwise, the sensor will show a **Down** status.
- **Do not use Transport-Level-Security**: The sensor connects to the FTP server without encryption.

You can see in the sensor logs which method the sensor used previously to connect to the FTP server.

AUTHENTICATION

Username

Enter a username for the FTP login. Please enter a string or leave the field empty.

Default username is "anonymous". If the sensor cannot log into the FTP server with this username (or another one that you define), the sensor message will show that the credentials are incorrect but the sensor will remain in **Up** status.

Password

Enter a password for the FTP login. Please enter a string or leave the field empty.

If the sensor cannot log onto the FTP server with this password, the sensor message will show that the credentials are incorrect but the sensor will remain in **Up** status.

DEBUG OPTIONS

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

DEBUG OPTIONS

- **Discard sensor result**: Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section **Data Storage** 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.
- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

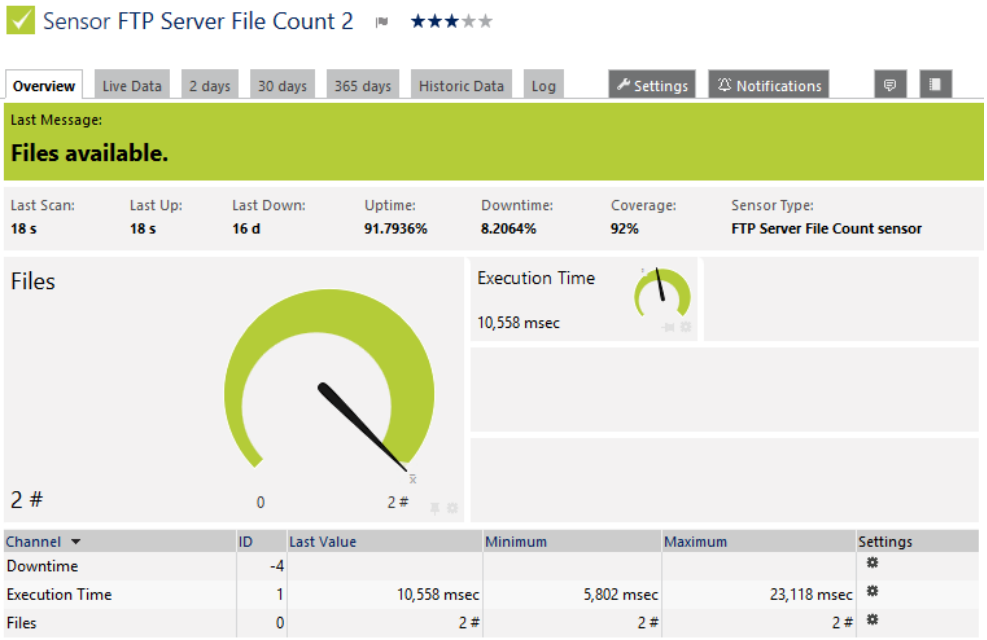
Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.41 FTP Server File Count Sensor

The FTP Server File Count sensor logs in to an File Transfer Protocol (FTP) server and can monitor changes to files.

- It can show the number of files available in the directory listing.



FTP Server File Count Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/ftp_server_file_count.png

Remarks

- Requires 808 .NET 4.0 or higher on the probe system. If the sensor shows the error PE087, please additionally install .NET 3.5 on the probe system.
- We recommend Windows 2012 R2 on the probe system for best performance of this sensor.
- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.

Requirement: .NET Framework

This sensor type requires the Microsoft .NET Framework to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the remote probe 3196. If the framework is missing, you cannot create this sensor.

Required .NET version (with latest updates): .NET 4.0 (Client Profile is sufficient), .NET 4.5, or .NET 4.6.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/60543

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SETTINGS

Check Method	Define how to access the FTP server directory that this sensor monitors. Choose between: ▪ **Check URL**: The sensor uses an explicitly defined URL of an FTP server to access the target directory. ▪ **Check folder on parent device**: The sensor uses the IP address or DNS name of the parent device where you add this sensor to and monitors a defined folder on this device.
FTP URL	This field is only visible if you select the URL method above. Enter the URL that this sensor checks. The URL can look like this: ftp://10.0.0.1/upload If you use this method, this sensor will not use the **IP Address/DNS value** of the parent device. You can add a port number to the URL by using a colon, for example, ftp://10.0.0.1/upload:21
FTP Port	This field is only visible if you select the parent device method above. Enter the number of the port to which this sensor connects. Default port is **21**.
FTP Folder	This field is only visible if you select the parent device method above. Enter the name of the folder on the parent device that this sensor monitors, for example: upload
Subfolder Recursion	This field is only visible if your select the parent device method above. Define if the sensor additionally monitors the subfolders of the FTP folder you specify above. Choose between: ▪ **Do not recurse subfolders**: The sensor monitors only the folder that you define above and ignores its subfolders. ▪ **Monitor the folder and its subfolders (use with caution!)**: The sensor recursively checks all subfolders in addition to the folder that you define above. Recursing subfolders in large directories with a high number of branches may evoke timeout errors or performance issues.
Username	Enter the username for the login to the FTP server. Please enter a string.
Password	Define the password for the login to the FTP server. Please enter a string.

SENSOR SETTINGS

File Count

Define which file the sensor counts. Choose between:

- **Count the total number of files**: The sensor always shows the total number of all files in the defined folder.
- **Count only new files**: The sensor shows only the number of new files since the last sensor scan. You can define the frequency of sensor scans in section **Scanning Interval** 813.
  With the every sensor scan, any new files from the previous scan will be regarded as old.

Security

Define the the encryption of the connection. Choose between:

- **Do not use an encryption**: The sensor connects without encryption.
- **Use explicit SSL**: The sensor establishes the connection to the FTP server via SSL.
  This sensor type only supports explicit SSL.

If Value Changes

Define what this sensor will do when the sensor value changes. You can choose between:

- **Ignore changes (default)**: The sensor takes no action on change.
- **Trigger 'change' notification**: The sensor sends an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification 2791 whenever the sensor value changes.

DEBUG OPTIONS

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result**: Do not store the sensor result.

DEBUG OPTIONS

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section **Data Storage** 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. ⓘ Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: Which .NET version does PRTG require?

- https://kb.paessler.com/en/topic/60543

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

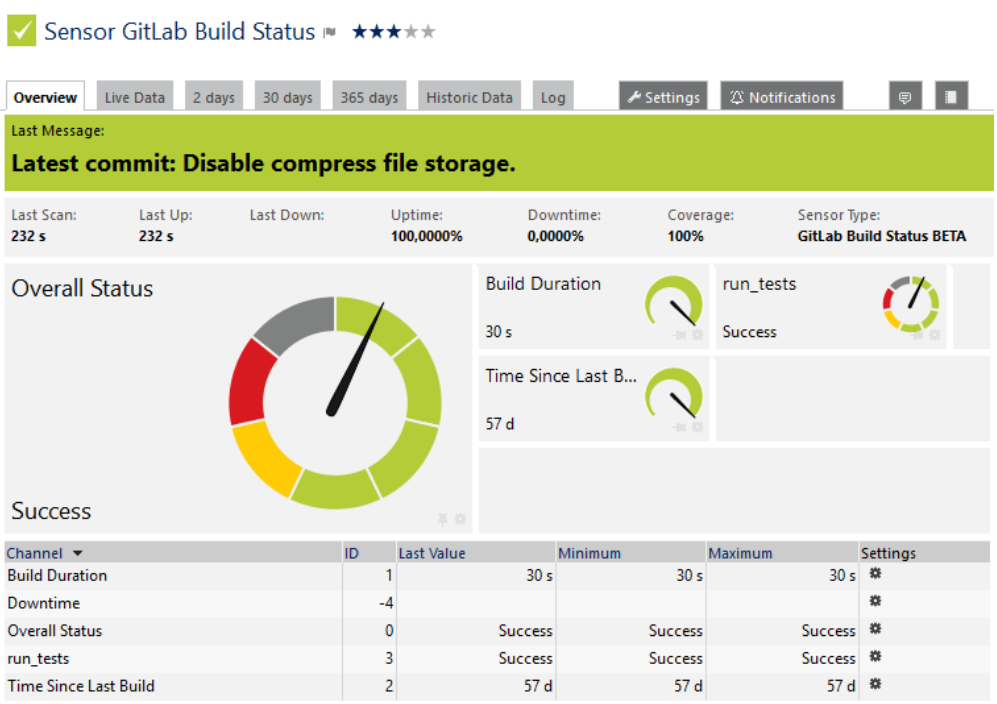
7.8.42 GitLab Build Status Sensor

The GitLab Build Status sensor monitors the status of the latest build on one specific branch. You can monitor your builds in either your own GitLab environment or on GitLab.com.

It can show the following:

- Overall status of the latest build (unknown, success, pending, canceled, failed)
- Duration of the latest build
- Time since the last build
- Status of the different build steps

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



GitLab Build Status Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/gitlab_build_status.png

Remarks

- The sensor uses the IP or DNS address of the parent device to find the GitLab server. To monitor branches in the GitLab cloud, enter gitlab.com as address in the parent device settings 360.
- The sensor can only monitor builds that are using GitLab Continuous Integration (CI). Builds using external CI tools (for example, Jenkins) are not supported.

- Use with care! This sensor has high impact on the performance of your GitLab server. Please do not add too many sensors of this type to your GitLab server, only monitor the most important branches.
- We do not recommend to add this sensor for temporarily existing branches. This is not useful in most cases.
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.
- BETA Currently, this sensor type is in beta status. The methods of operating can change at any time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

The sensor requires an **Access Token** to access your projects on GitLab. Before you can actually create the sensor, it will ask you for this token. You can create it on the GitLab web interface in your profile under **Profile Settings** | **Access Token**. Copy the created token and paste it into the **GitLab Access Token** field in the **GitLab Credentials** dialog of the sensor.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

GITLAB REPOSITORY

Branch	Select the branches you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items. To better find what you want to monitor, especially in large tables, use the search function in the upper right corner. For example, you can filter for a specific project to show related branches only. The sensor scans the last 100 builds of all projects during sensor creation (meta-scan). If you miss a branch in the overview, start a build on the branch that is missing and add the sensor anew.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

GITLAB CREDENTIALS

GitLab Access Token	Enter the **Access Token** that you have defined in your GitLab profile. You can create the token on the GitLab web interface in your profile under **Profile Settings** | **Access Token**. By default, this field show the access token that you have provided during sensor creation.

GITLAB REPOSITORY

Project ID	These fields show various information about the project and branch that this sensor monitors.
Project Name	
Branch	

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply. If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply. If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

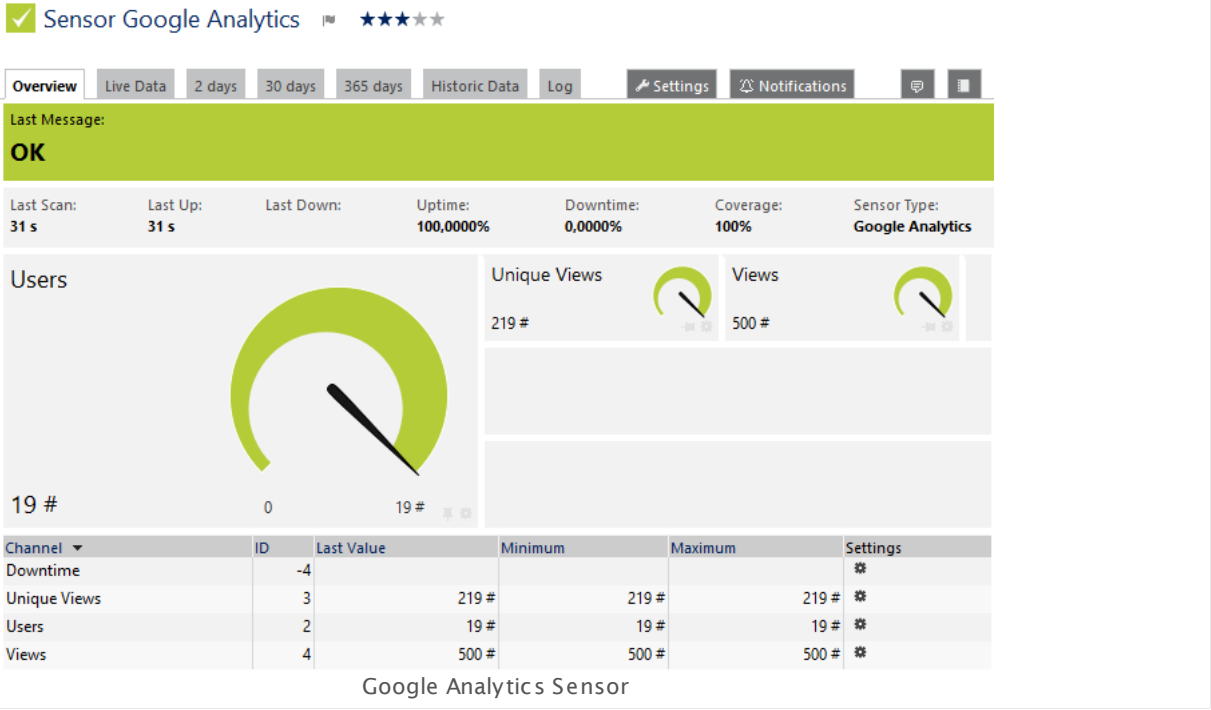
Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.43 Google Analytics Sensor

The Google Analytics sensor queries and monitors several metrics from a Google Analytics account using the Google Application Programming Interface (API) and OAuth2.

- It can show the values for all available Google Analytics metrics in different sensor channels.



Google Analytics Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/google_analytics_v2.png

Remarks

- The minimum scanning interval for this sensor type is **30 minutes**.
- For details about OAuth2 authentication, please see manual section **Authentication Using OAuth2** 837.
- Some dimensions and metrics cannot be queried together. See the Knowledge Base: Where do I find available Google Analytics metrics?

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

PRTG requires OAuth2 authorization before you can actually add this sensor type. Provide the requested credentials in the appearing window.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

GOOGLE CREDENTIALS

This sensor type uses OAuth2 authentication to get access to your Google account. For details about the authentication approach, please see section **Authentication Using OAuth2** 837.

OAuth URL	Click the button **Get Access Code** to connect this sensor to your Google Analytics account using OAuth2. This is necessary to allow the sensor to query data from Google Analytics. A new browser window appears. Please follow the steps there and confirm the permission for PRTG to connect to your Google Analytics account. Copy the OAuth code you get and paste it into the **OAuth Code** field below.
OAuth Code	Paste the access code that you receive after completing the authorization process for PRTG at your Google Analytics account. Click **OK** to define the sensor settings 829. It is mandatory to connect this sensor to your Google Analytics account to create this sensor. Please complete the OAuth approach first to get the OAuth code.

GOOGLE ANALYTICS SPECIFIC

Profile	Choose the Google Analytics profile that you want to monitor. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Sensor Channel #2 – #10	You can create up to 10 different sensor channels for this sensor. You have to define at least one data channel, so you will see all available settings for Sensor Channel #1 without enabling it manually. Additionally you can define Sensor Channel #2 up to Sensor Channel #10. To do so, choose between: ▪ **Disable:** The sensor will not create this channel. ▪ **Enable:** Create an additional channel and define all its characteristics below (name, metric, mode, and unit).

GOOGLE ANALYTICS SPECIFIC

Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

It is not possible to enable or disable sensor channels after the creation of this sensor!

Channel #x Mode

Define how to display the retrieved value in the channel. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew. Choose between:

- **Absolute (recommended)**: Shows the value as the sensor retrieves it from Google Analytics.
- **Difference**: The sensor calculates and shows the difference between the last and the current value returned from Google Analytics.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name

Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.

Parent Tags

Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.

Tags

Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

BASIC SENSOR SETTINGS

	You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

GOOGLE CREDENTIALS

OAuth Code	Shows the authorization code that the sensor uses to get access to your Google Analytics account. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

GOOGLE ANALYTICS SPECIFIC

Profile	Shows the Google Analytics profile that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Time Span	Define the time that the queried monitoring covers. Choose between: ▪ **Last week (default)** ▪ **Yesterday** ▪ **Today**
Sensor Channel #x Name	Enter a name for the channel in which the sensor shows the results for the metric you choose below. Please enter a string.
Sensor Channel #x Metric	Select a metric that you want to monitor. You can choose between available Google Analytics. If your desired metric is not listed, choose **Custom Metric** and specify below.
Sensor Channel #x Custom Metric	This field is only visible if you choose custom metric above. Enter the identifier of the metric that you want to monitor. Type it exactly as shown in Google Analytics. Metric identifiers always start with ga:

GOOGLE ANALYTICS SPECIFIC

Please enter a string.

Sensor Channel #x Mode

Shows how the sensor displays the retrieved value in the channel. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Channel #x Unit

Define the unit of the channel value. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew. Choose between:

- BytesBandwidth
- BytesMemory
- BytesDisk
- Temperature
- Percent
- TimeResponse
- TimeSeconds
- TimeHours
- Count
- CPU
- BytesFile
- SpeedDisk
- SpeedNet
- Custom
- Value Lookup

For more information about the available units, please refer to the PRTG Application Programming Interface (API) Definition 3174 for custom sensors.

To use lookups 3183 with this channel, choose the unit **Value Lookup** and select your lookup file below. Do not use the unit **Custom** for using lookups with this sensor and do not use the channel settings 2782 to define a lookup file!

Sensor Channel #x Custom Unit

This setting is only visible if you select the **Custom** unit option above. Define a unit for the channel value. Please enter a string.

GOOGLE ANALYTICS SPECIFIC

Sensor Channel #x Value Lookup	This setting is only visible if you select the **Value Lookup** option above. Choose a lookup 3183 file that you want to use with this channel.
Sensor Channel #x	Shows if you enabled or disabled a channel. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew. You can define up to 10 different sensor channels per sensor.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. ⓘ Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

This sensor type has a fixed minimum scanning interval for performance reasons. You cannot run the sensor in shorter intervals than this minimum interval. Consequently, shorter scanning intervals as defined in **System Administration—Monitoring** 2955 are not available for this sensor.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** Custom channel types can be set on sensor level only.

Authentication Using OAuth2

This sensor type uses the OAuth2 security protocol to access the account from which you want to retrieve and monitor data. OAuth2 enables you to grant access to the target account without sharing your password with PRTG. The authorization approach of PRTG using OAuth2 works as follows.

1. **Authorization Request**
   First, you have to request authorization for this sensor to access service resources from your account. For this purpose you are asked to get an access code for this sensor in the **Add Sensor** dialog. Click the **Get Access Code** button to start the authorization process using OAuth2. A new browser window will open on the authorization server of the target service.

2. **Verifying Identity**
   This new window contains a login form for your account that you want to monitor. Log in to your account using your credentials for this service to authenticate your identity. This is a common login to your account on the target server so PRTG will not see your password. The service will forward you to the authorization page and asks you to permit PRTG to access the data in your account.
   If you are already logged in to the service with a user account, you do not have to enter credentials in this step and get directly to the access permission page.

3. **Authorizing PRTG**
   Permit PRTG to access information on your account. Note that this permission holds only for this specific sensor, not for other sensors of this type or PRTG as a whole. For each sensor of this type you add, you have to confirm the access permission anew. You can change the account permissions at any time in your account at the target service.

4. **Getting Authorization Code**
   Permitting PRTG to access your account data forwards you to a page where the service provides an **authorization code**. Copy this code and switch back to the **Add Sensor** dialog in PRTG.
   The code is only valid a short period of time and expires after a few minutes. You can use a particular code only once.

5. **Providing Authorization Code**
   Paste the authorization code into the **OAuth Code** field and complete the **Add Sensor** dialog. You do not have to go through further configuration steps manually. The sensor will accomplish the following steps automatically.

6. **Requesting Access Token**
   After receiving the authorization code, PRTG will request an access token from the API of the target service. For this purpose, PRTG transmits the authorization code together with several authentication details. The API checks if the authorization is valid and returns the access token to PRTG. Access token are specific for one account and one application (here: PRTG). The authorization process to read data from your account is now complete.

7. **Retrieving Data**
   The sensor transmits the access token with each sensor scan in the defined scanning interval to authenticate with your account. It is not necessary to use the original account credentials anew. The used tokens will refresh automatically from time to time.

More

Knowledge Base: Where do I find available Google Analytics metrics?

- https://kb.paessler.com/en/topic/35373

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

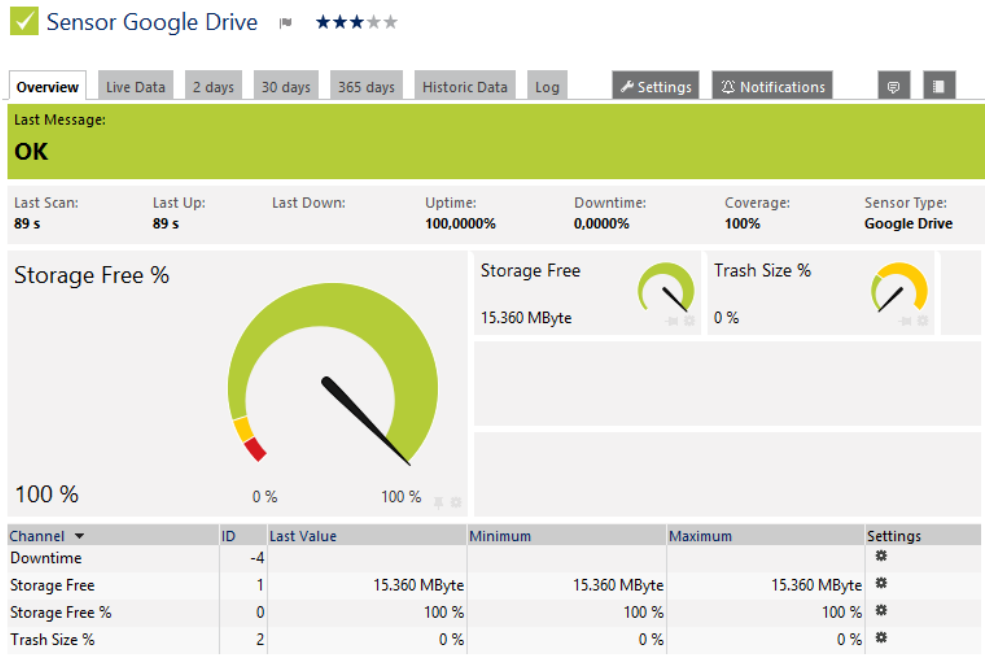
Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.44 Google Drive Sensor

The Google Drive sensor monitors a Google Drive account using the Google Application Programming Interface (API) and OAuth2. It shows the following:

- Free storage in bytes and percent
- Trash size in percent



Google Drive Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/google_drive.png

Remarks

- The minimum scanning interval for this sensor type is **30 minutes**.
- For details about OAuth2 authentication, please see manual section Authentication Using OAuth2 846.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

PRTG requires OAuth2 authorization before you can actually add this sensor type. Provide the requested credentials in the appearing window.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

GOOGLE CREDENTIALS

This sensor type uses OAuth2 authentication to get access to your Google account. For details about the authentication approach, please see section **Authentication Using OAuth2** 846.

OAuth URL	Click the button **Get Access Code** to connect this sensor to your Google Drive account using OAuth2. This is necessary to allow the sensor to query data from Google Drive. A new browser window appears. Please follow the steps there and confirm the permission for PRTG to connect to your Google Drive account. Copy the OAuth code you get and paste it into the **OAuth Code** field below.
OAuth Code	Paste the access code that you receive after completing the authorization process for PRTG at your Google Drive account. Click **OK** to define the sensor settings 840. It is mandatory to connect this sensor to your Google Drive account to create this sensor. Please complete the OAuth approach first to get the OAuth code.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	Enter one or more **Tags**[124], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited[124] from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

GOOGLE CREDENTIALS

OAuth Code	Shows the authorization code that the sensor uses to get access to your Google Drive account. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. ⓘ You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. ⓘ This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings**[2782] settings).

SENSOR DISPLAY

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.

SCANNING INTERVAL

- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

This sensor type has a fixed minimum scanning interval for performance reasons. You cannot run the sensor in shorter intervals than this minimum interval. Consequently, shorter scanning intervals as defined in **System Administration—Monitoring** 2955 are not available for this sensor.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** Custom channel types can be set on sensor level only.

Authentication Using OAuth2

This sensor type uses the OAuth2 security protocol to access the account from which you want to retrieve and monitor data. OAuth2 enables you to grant access to the target account without sharing your password with PRTG. The authorization approach of PRTG using OAuth2 works as follows.

1. **Authorization Request**
   First, you have to request authorization for this sensor to access service resources from your account. For this purpose you are asked to get an access code for this sensor in the **Add Sensor** dialog. Click the **Get Access Code** button to start the authorization process using OAuth2. A new browser window will open on the authorization server of the target service.

2. **Verifying Identity**
   This new window contains a login form for your account that you want to monitor. Log in to your account using your credentials for this service to authenticate your identity. This is a common login to your account on the target server so PRTG will not see your password. The service will forward you to the authorization page and asks you to permit PRTG to access the data in your account.
   If you are already logged in to the service with a user account, you do not have to enter credentials in this step and get directly to the access permission page.

3. **Authorizing PRTG**
   Permit PRTG to access information on your account. Note that this permission holds only for this specific sensor, not for other sensors of this type or PRTG as a whole. For each sensor of this type you add, you have to confirm the access permission anew. You can change the account permissions at any time in your account at the target service.

4. **Getting Authorization Code**
   Permitting PRTG to access your account data forwards you to a page where the service provides an **authorization code**. Copy this code and switch back to the **Add Sensor** dialog in PRTG.
   The code is only valid a short period of time and expires after a few minutes. You can use a particular code only once.

5. **Providing Authorization Code**
   Paste the authorization code into the **OAuth Code** field and complete the **Add Sensor** dialog. You do not have to go through further configuration steps manually. The sensor will accomplish the following steps automatically.

6. **Requesting Access Token**
   After receiving the authorization code, PRTG will request an access token from the API of the target service. For this purpose, PRTG transmits the authorization code together with several authentication details. The API checks if the authorization is valid and returns the access token to PRTG. Access token are specific for one account and one application (here: PRTG). The authorization process to read data from your account is now complete.

7. **Retrieving Data**
   The sensor transmits the access token with each sensor scan in the defined scanning interval to authenticate with your account. It is not necessary to use the original account credentials anew. The used tokens will refresh automatically from time to time.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the Sensor Channels Settings 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the Sensor Notifications Settings 2791 section.

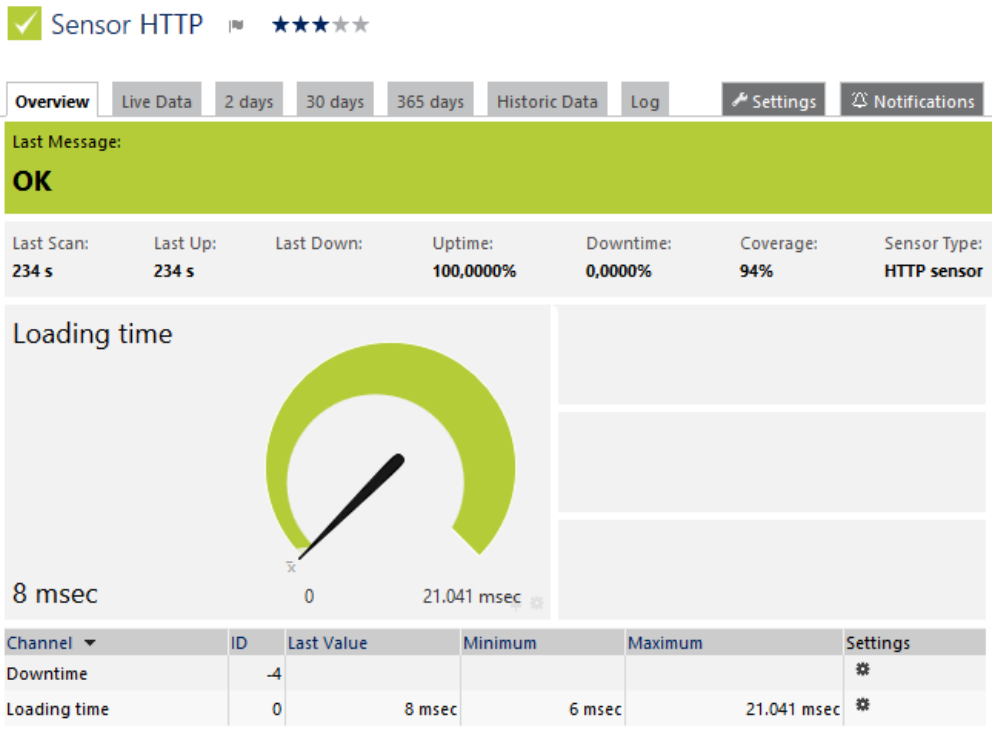
Others

For more general information about settings, please see the Object Settings 188 section.

7.8.45 HTTP Sensor

The HTTP sensor monitors a web server using Hypertext Transfer Protocol (HTTP). This is the easiest way to monitor if a website (or a specific website element) is reachable.

- It shows the loading time of a web page or element.



HTTP Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/http.png

Remarks

- Knowledge Base: My HTTP sensors fail to monitor websites which use SNI. What can I do?
- Knowledge Base: Which HTTP status code leads to which HTTP sensor status?
- This sensor type does not support Secure Remote Password (SRP) ciphers.

Add Sensor

The **Add Sensor** dialog appears when you manually add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

HTTP SPECIFIC

Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).
URL	Enter the URL the sensor connects to. It has to be URL encoded! If you enter an absolute URL, the sensor uses this address independently from the **IP address/DNS name** setting of the device on which you create this sensor. You can enter an URL leading to a webpage (to measure the page source code's loading time), or enter the URL of an image or of another page asset to measure this element's availability and loading time.

HTTP SPECIFIC

PRTG uses a smart URL replacement which allows you to use the parent device's IP address/DNS name setting as part of the URL. For more information, please see section **Smart URL Replacement** below.

Request Method

Choose an HTTP request method to determine how the sensor will request the given URL.

- **GET**: Request the website directly, like browsing the web. We recommend using this setting for a simple check of a web page.
- **POST**: Send post form data to the URL. If this setting is chosen, you must enter the data that will be sent in the **Postdata** field below.
- **HEAD**: Only request the HTTP header from the server; without the actual web page. Although this saves bandwidth since less data is transferred, it is not recommended because the measured request time is not the one experienced by your users and you might not be notified for slow results or timeouts.

Postdata

This field is only visible when you select the POST **Request Method** setting above. Enter the data part for the POST request here.

No XML is allowed here!

Content Type

This setting is only visible when you select the POST **Request Method** setting above. Define the content type of a POST request. Choose between:

- **Default (application/x-www-form-urlencoded)**: This is the default content type used to encode the form data set for submission to the server.
- **Custom**: If you need another content type than default, enter this content type below.

Custom Content Type

This field is only visible when you select **Custom** above. Define the content type which is needed, for example, XML, JSON, HTTP.

Server Name Indication

Shows the Server Name Identification (SNI) that the sensor automatically determined from the host address of the parent device or the target URL of the sensor. SNI has to be a Fully Qualified Domain Name (FQDN). Please ensure it matches the configuration of the target server.

For details, see the Knowledge Base article My HTTP sensors fail to monitor websites which use SNI. What can I do?

HTTP SPECIFIC

SNI Inheritance	Define if you want to inherit the Server Name Identification (SNI) from the parent device. See the **Server Name Indication** setting above which SNI is determined. Choose between: ▪ **Inherit SNI from parent device**: The sensor determines the SNI from the host address of the parent device. ▪ **Do not inherit SNI from parent device**: The sensor determines the SNI from the target **URL** as defined in the settings of this sensor.

This sensor type implicitly supports Server Name Identification (SNI), an extension to the TLS protocol.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

PROXY SETTINGS FOR HTTP SENSORS

HTTP Proxy Settings	The proxy settings determine how a sensor connects to a given URL. You can enter data for an HTTP proxy server that sensors will use when connecting via HTTP or HTTPS. This setting affects monitoring only and determines the behavior of HTTP sensors. To change proxy settings for the core server, please see **System Administration—Core & Probes** 2967. The **SSL Certificate Sensor** 2289 and the **SSL Security Check Sensor** 2299 do not support HTTP proxies, but you can configure connections via SOCKS proxies in their sensor settings.
Name	Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.
Port	Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.
User	If the proxy requires authentication, enter the username for the proxy login. Only basic authentication is available! Please enter a string or leave the field empty.
Password	If the proxy requires authentication, enter the password for the proxy login. Only basic authentication is available! Please enter a string or leave the field empty.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply. If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply. If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

Smart URL Replacement

Instead of entering a complete address in the URL field of an HTTP sensor, you can merely enter the protocol followed by colon and three slashes (that means you can enter either http:/// or https:/// or even a simple slash / as equivalent for http:///). PRTG will then fill in the parent device's **IP address** or **DNS name** in front of the third slash automatically. Whether this results in a valid URL or not, depends on the IP address or DNS name of the device where this HTTP sensor is created on. In combination with cloning devices, the smart URL replacement makes it easy to create many like devices.

For example, if you create a device with **DNS name** www.example.com and you put an HTTP sensor on it, you can provide values the following ways:

- Providing the value https:/// in the URL field, PRTG will automatically create the URL https://www.example.com/ from that.
- Using the value /help in the URL field, PRTG will automatically create and monitor the URL http://www.example.com/help
- It is also possible to provide a port number in the URL field which will be taken over by the device's DNS name and internally added, for example, http://:8080/

Smart URL replacement does not work for sensors running on the **Probe Device**.

More

Knowledge Base: Which HTTP status code leads to which HTTP sensor status?

- https://kb.paessler.com/en/topic/65731

Knowledge Base: My HTTP sensors fail to monitor websites which use SNI. What can I do?

- https://kb.paessler.com/en/topic/67398

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

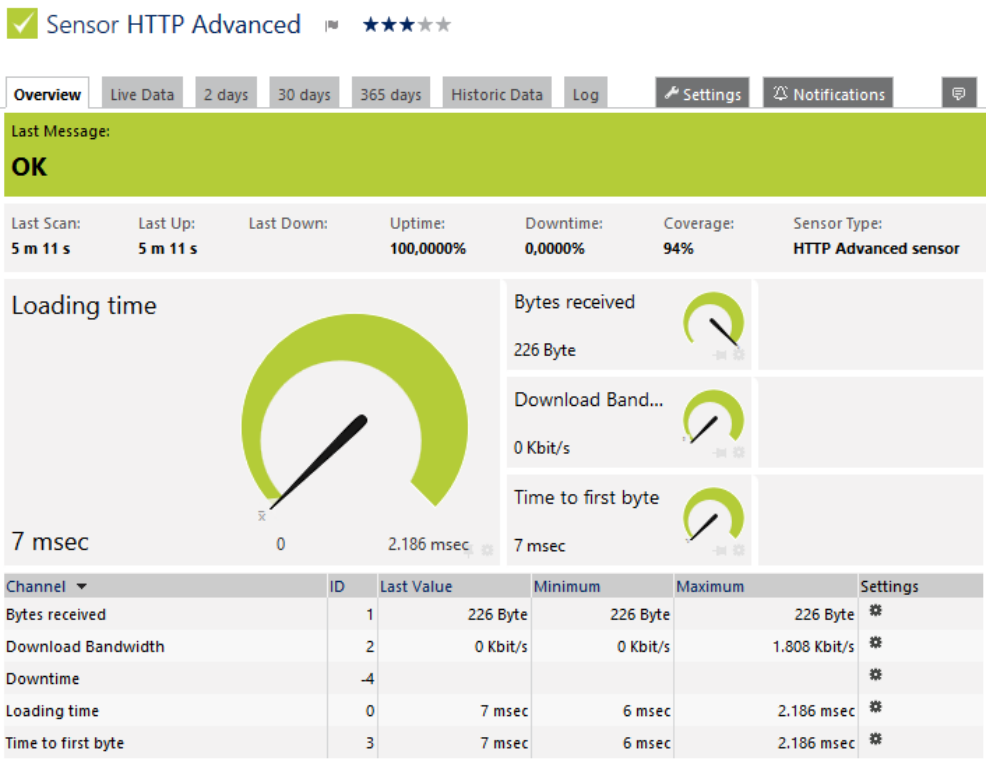
For more general information about settings, please see the **Object Settings** 188 section.

7.8.46 HTTP Advanced Sensor

The HTTP Advanced sensor monitors the source code of a web page using Hypertext Transfer Protocol (HTTP). It supports authentication, content checks, and other advanced parameters.

The sensor can show the following:

- Loading time
- Bytes received
- Download bandwidth (speed)
- Time to first byte



HTTP Advanced Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/http_advanced.png

Remarks

- Supports Smart URL Replacement 872.
- Knowledge Base: Which user agent should I use in the HTTP Advanced sensor's settings?
- Knowledge Base: My HTTP sensors fail to monitor websites which use SNI. What can I do?
- Knowledge Base: Which HTTP status code leads to which HTTP sensor status?
- This sensor type does not support Secure Remote Password (SRP) ciphers.

- If you need to use SRP ciphers, please choose the **Alternate/Compatibility Mode** in the sensor settings.
- Bandwidth monitoring of fast internet connections may be inaccurate.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

HTTP SPECIFIC

Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).
URL	Enter the URL the sensor connects to. It has to be URL encoded! If you enter an absolute URL, the sensor uses this address independently from the **IP address/DNS name** setting of the device on which you create this sensor. You can enter an URL leading to a webpage (to measure the page source code's loading time), or enter the URL of an image or of another page asset to measure this element's availability and loading time. PRTG uses a smart URL replacement which allows you to use the parent device's IP address/DNS name setting as part of the URL. For more information, please see section **Smart URL Replacement** below.
Request Method	Choose an HTTP request method to determine how the sensor will request the given URL. ▪ **GET**: Request the website directly, like browsing the web. We recommend using this setting for a simple check of a web page. ▪ **POST**: Send post form data to the URL. If this setting is chosen, you must enter the data that will be sent in the **Postdata** field below. ▪ **HEAD**: Only request the HTTP header from the server; without the actual web page. Although this saves bandwidth since less data is transferred, it is not recommended because the measured request time is not the one experienced by your users and you might not be notified for slow results or timeouts.
Postdata	This field is only visible when you select the POST **Request Method** setting above. Enter the data part for the POST request here. No XML is allowed here!
Content Type	This setting is only visible when you select the POST **Request Method** setting above. Define the content type of a POST request. Choose between: ▪ **Default (application/x-www-form-urlencoded)**: This is the default content type used to encode the form data set for submission to the server. ▪ **Custom**: If you need another content type than default, enter this content type below.

HTTP SPECIFIC

Custom Content Type	This field is only visible when you select **Custom** above. Define the content type which is needed, for example, XML, JSON, HTTP.
Server Name Indication	Shows the Server Name Identification (SNI) that the sensor automatically determined from the host address of the parent device or the target URL of the sensor. SNI has to be a Fully Qualified Domain Name (FQDN). Please ensure it matches the configuration of the target server. For details, see the Knowledge Base article My HTTP sensors fail to monitor websites which use SNI. What can I do?
SNI Inheritance	Define if you want to inherit the Server Name Identification (SNI) from the parent device. See the **Server Name Indication** setting above which SNI is determined. Choose between: ▪ **Inherit SNI from parent device**: The sensor determines the SNI from the host address of the parent device. ▪ **Do not inherit SNI from parent device**: The sensor determines the SNI from the target **URL** as defined in the settings of this sensor.

HTTP ENGINE

Monitoring Engine	If you encounter unexpected errors with the standard method that is used to monitor a URL, try to use the compatibility mode which is based on .NET. Choose between: ▪ **Default/High Performance (recommended)**: This is the default monitoring method for this sensor type. ▪ **Alternate/Compatibility Mode**: Try this method as an alternative for websites that do not work with the default approach. Using the compatibility mode, this sensor executes an external exe. Because of this, this method needs more resources, but it can be helpful in particular cases. If you select the compatibility mode, the options for the SSL method will be slightly different. You can also check for trusted certificates. Please see below. When using the Compatibility Mode, **Smart URL Replacement** will not work, so this sensor will not use the **IP Address/DNS value** of the parent device automatically then.

SSL SPECIFIC (WHEN USING COMPATIBILITY MODE)

SSL Method

When using the compatibility mode, the SSL specific settings are a bit different to the default (automatically used) SSL settings. You can choose between:

- **SSL V3**
- **TLS V1**
- **SSL V3 or TLS V1**: This is the default setting.

Check SSL Certificates

Specify if the sensor will check the certificate of the monitored URL. Choose between:

- **Do not check used certificates**: Do not consider the certificates of the monitored web pages. This the default setting.
- **Check if the used certificates are trusted**: Inspect the certificates. If the certificate of the server is not trusted, the sensor shows a **Down** status and displays a corresponding message.

This sensor type implicitly supports Server Name Identification (SNI), an extension to the TLS protocol.

ADVANCED SENSOR DATA

Protocol Version

Define the HTTP protocol version that the sensor will use when connecting to the target URL. Choose between:

- **HTTP 1.0**
- **HTTP 1.1**: This is the default setting.

User Agent

Choose which user agent string the sensor will send when connecting to the target URL. Choose between:

- **Use PRTG's default string**: Do not enter a specific user agent, use the default setting. Usually, this is: Mozilla/5.0 (compatible; PRTG Network Monitor (www.paessler.com); Windows)
- **Use a custom string**: Use a custom user agent. Define below.

Custom User Agent

This field is only visible if you enable custom user agent above. Enter a string to be used as user agent when connecting to the URL specified above.

ADVANCED SENSOR DATA

Use Custom HTTP Headers	Define if you want to send custom HTTP headers to the target URL. Choose between: ▪ **Do not use custom HTTP headers** ▪ **Use custom HTTP headers**
Custom HTTP Headers	This field is only available if you select using custom headers above. Enter a list of custom HTTP headers with theirs respective values that you want to transmit to the URL you define above, each pair in one line. The syntax of a header-value pair is header1:value1 The sensor does not support the header field names user-agent, content-length, host. Ensure the HTTP header statement is valid! Otherwise, the sensor request will not be successful.

Content Changes	Define what the sensor will do if the content of the monitored web page (element) changes. You can choose between: • **Ignore changes**: No action will be taken on change. • **Trigger 'change' notification**: The sensor will send an internal message indicating that the web page content has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification 2791 whenever the web page content changes.
Require Keyword	Define if the sensor will check the result at the configured URL for keywords. Choose between: ▪ **Do not check for keyword (default)**: Do not search for keywords in the result returned at the URL. ▪ **Set sensor to warning if keyword is missing**: Check if a keyword exists in the result and set the sensor to a **Warning** status 163 if yes. ▪ **Set sensor to error if keyword is missing**: Check if a keyword exists in the result and set the sensor to a **Down** status 163 if yes. The content check is only intended for HTML websites and might not work with other target URLs. For example, binary files are not supported.

Response Must Include	This field is only visible if you enable keyword checking above (include). Define which string must be part of the source code at the given URL. You can either enter plain text or a **Regular Expression**[3193]. Specify below. If the data does not include the search pattern, the sensor will show the status defined above. Please enter a string.
Check Method	Define the format of the search expression in the field above. ▪ **String search (default)**: Search for the string as plain text. The characters * and ? work here as placeholder, whereas * stands for no or any number of characters and ? stands for exactly one character (as known from Windows search). This behavior cannot be disabled, so the literal search for these characters is not possible with plain text search. You can also search for HTML tags. ▪ **Regular Expression**: Use the search pattern as a **Regular Expression**[3193].
Exclude Keyword	Define if the sensor will check the result at the configured URL for keywords. Choose between: ▪ **Do not check for keyword (default)**: Do not search for keywords in the result returned at the URL. ▪ **Set sensor to warning if keyword is found**: Check if a keyword exists in the result and set the sensor to a **Warning** status[163] if yes. ▪ **Set sensor to error if keyword is found**: Check if a keyword exists in the result and set the sensor to a **Down** status[163] if yes. The content check is only intended for HTML websites and might not work with other target URLs. For example, binary files are not supported.
Response Must Not include	This field is only visible if you enable keyword checking (exclude) above. Define which string must not be part of the source code at the given URL. You can either enter plain text or a **Regular Expression**[3193]. If the data does include this string, the sensor will show the status defined above. Please enter a string.
Check Method	Define in which format you have entered the search expression in the field above.

	▪ **String Search (default)**: Search for the string as plain text. The characters asterisk (*) and question mark (?) work here as placeholder, whereas * stands for no or any number of characters and ? stands for exactly one character (as known from Windows search). This behavior cannot be disabled, so the literal search for these characters is not possible with plain text search. You can also search for HTML tags. ▪ **Regular Expression**: Use the search pattern as a **Regular Expression** 3193.
Limit Download (kb)	Enter a maximum amount of data that the sensor can transfer per every single request. If you set content checks, please be aware that only the content downloaded up to this limit can be checked for search expressions.
Result Handling	Define what the sensor will do with the data loaded at the given URL. Choose between: • **Discard HTML result**: Do not store the requested data. • **Store latest HTML result**: Store the last result of the requested data to the **Logs (Sensors)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File name: Result of Sensor [ID].txt. This is for debugging purposes, especially in combination with content checks. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, see section **Data Storage** 3226.

This sensor loads the source code at the given URL. If you set up a content check, only this source code is checked for the keywords. The code is not necessarily identical to the one used to display the page when opening the same URL in a web browser, as there may be a reload configured or certain information may be inserted after loading, for example, via JavaScript.

PRTG does not follow links to embedded objects nor does it execute scripts. Only the first page at the given URL is loaded and checked against the expressions configured.

For debugging, please use the **Result Handling** option to write the source code file to disk and look up what exactly PRTG gets when calling the URL. If the URL configured does not point to a web page, but to a binary file, for example, to an image, you usually will not check for content.

AUTHENTICATION

Authentication	Define if the web page at the configured URL needs authentication. Choose between:

AUTHENTICATION

- **No authentication needed**
- **Web page needs authentication**

User — This field is only visible if you enable authentication above. Enter a username. Please enter a string.

Password — This field is only visible if you enable authentication above. Enter a password. Please enter a string.

Authentication Method — This field is only visible if enable authentication above. Select the authentication method the given URL is protected with. Choose between:

- **Basic access authentication (HTTP)**: Use simple HTTP authentication. This is the default setting and suitable for most cases.
  This authentication method transmits credentials as plain text.
- **Windows NT LAN Manager (NTLM)**: Use the Microsoft NTLM protocol for authentication. This is sometimes used in intranets for single sign-on.
- **Digest Access Authentication**: Use digest access authentication that applies a hash function to the password which is safer than basic access authentication.

We recommend that you use the default value.

SENSOR DISPLAY

Primary Channel — Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type — Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

PROXY SETTINGS FOR HTTP SENSORS

HTTP Proxy Settings	The proxy settings determine how a sensor connects to a given URL. You can enter data for an HTTP proxy server that sensors will use when connecting via HTTP or HTTPS. This setting affects monitoring only and determines the behavior of HTTP sensors. To change proxy settings for the core server, please see **System Administration—Core & Probes** 2967. The **SSL Certificate Sensor** 2289 and the **SSL Security Check Sensor** 2299 do not support HTTP proxies, but you can configure connections via SOCKS proxies in their sensor settings.
Name	Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.
Port	Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.
User	If the proxy requires authentication, enter the username for the proxy login.

PROXY SETTINGS FOR HTTP SENSORS

Only basic authentication is available! Please enter a string or leave the field empty.

Password

If the proxy requires authentication, enter the password for the proxy login.

Only basic authentication is available! Please enter a string or leave the field empty.

SCANNING INTERVAL

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

SCANNING INTERVAL

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices**	**Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** [360] or in the superior **Group Settings** [334].

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** [2982] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** [129].

CHANNEL UNIT CONFIGURATION

Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** Custom channel types can be set on sensor level only.

Smart URL Replacement

Instead of entering a complete address in the URL field of an HTTP sensor, you can merely enter the protocol followed by colon and three slashes (that means you can enter either http:/// or https:/// or even a simple slash / as equivalent for http:///). PRTG will then fill in the parent device's **IP address** or **DNS name** in front of the third slash automatically. Whether this results in a valid URL or not, depends on the IP address or DNS name of the device where this HTTP sensor is created on. In combination with cloning devices, the smart URL replacement makes it easy to create many like devices.

For example, if you create a device with **DNS name** www.example.com and you put an HTTP sensor on it, you can provide values the following ways:

- Providing the value https:/// in the URL field, PRTG will automatically create the URL https://www.example.com/ from that.
- Using the value /help in the URL field, PRTG will automatically create and monitor the URL http://www.example.com/help
- It is also possible to provide a port number in the URL field which will be taken over by the device's DNS name and internally added, for example, http://:8080/

Smart URL replacement does not work for sensors running on the **Probe Device**.

More

Knowledge Base: Which HTTP status code leads to which HTTP sensor status?

- https://kb.paessler.com/en/topic/65731

Knowledge Base: Which user agent should I use in the HTTP Advanced sensor's settings?

- https://kb.paessler.com/en/topic/30593

Knowledge Base: Is it possible to test a WSDL or SOAP service with PRTG?

- https://kb.paessler.com/en/topic/66680

Knowledge Base: My HTTP sensors fail to monitor websites which use SNI. What can I do?

- https://kb.paessler.com/en/topic/67398

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.47 HTTP Apache ModStatus PerfStats Sensor

The HTTP Apache ModStatus PerfStats sensor monitors performance statistics of an Apache web server using mod_status over Hypertext Transfer Protocol (HTTP).

It can show the following about the Apache at scan time:

- CPU load
- Server uptime
- Requests per second
- Bytes per request
- Number of current busy workers threads
- Number of idle worker threads

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

HTTP Apache ModStatus PerfStats Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/http_apache_modstatus_perfstats.png

Remarks

- Supports Smart URL Replacement 882.

- Knowledge Base: Which HTTP status code leads to which HTTP sensor status?
- This sensor type does not support Secure Remote Password (SRP) ciphers.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

HTTP SPECIFIC

Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).
URL	Enter the URL to the mod_status module on your Apache server. PRTG will append a "/server_status?auto" part automatically. If you enter an absolute URL, this address will be independent from the **IP address/DNS name** setting of the device this sensor is created on. PRTG uses a smart URL replacement which allows you to use the parent device's IP address/DNS name setting as part of the URL. For more information, please see section **Smart URL Replacement** below.

This sensor type implicitly supports Server Name Identification (SNI), an extension to the TLS protocol.

AUTHENTICATION

Authentication	Define if the web page at the configured URL needs authentication. Choose between: ▪ **No authentication needed** ▪ **Web page needs authentication**
User	This field is only visible if you enable authentication above. Enter a username. Please enter a string.
Password	This field is only visible if you enable authentication above. Enter a password. Please enter a string.
Authentication Method	This field is only visible if enable authentication above. Select the authentication method the given URL is protected with. Choose between: ▪ **Basic access authentication (HTTP)**: Use simple HTTP authentication. This is the default setting and suitable for most cases. This authentication method transmits credentials as plain text.

AUTHENTICATION

- **Windows NT LAN Manager (NTLM)**: Use the Microsoft NTLM protocol for authentication. This is sometimes used in intranets for single sign-on.
- **Digest Access Authentication**: Use digest access authentication that applies a hash function to the password which is safer than basic access authentication.

We recommend that you use the default value.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.
- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

PROXY SETTINGS FOR HTTP SENSORS

HTTP Proxy Settings	The proxy settings determine how a sensor connects to a given URL. You can enter data for an HTTP proxy server that sensors will use when connecting via HTTP or HTTPS. This setting affects monitoring only and determines the behavior of HTTP sensors. To change proxy settings for the core server, please see System Administration—Core & Probes 2967. The SSL Certificate Sensor 2289 and the SSL Security Check Sensor 2299 do not support HTTP proxies, but you can configure connections via SOCKS proxies in their sensor settings.
Name	Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.
Port	Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.
User	If the proxy requires authentication, enter the username for the proxy login. Only basic authentication is available! Please enter a string or leave the field empty.
Password	If the proxy requires authentication, enter the password for the proxy login. Only basic authentication is available! Please enter a string or leave the field empty.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

Smart URL Replacement

Instead of entering a complete address in the URL field of an HTTP sensor, you can merely enter the protocol followed by colon and three slashes (that means you can enter either http:/// or https:/// or even a simple slash / as equivalent for http:///). PRTG will then fill in the parent device's **IP address** or **DNS name** in front of the third slash automatically. Whether this results in a valid URL or not, depends on the IP address or DNS name of the device where this HTTP sensor is created on. In combination with cloning devices, the smart URL replacement makes it easy to create many like devices.

For example, if you create a device with **DNS name** www.example.com and you put an HTTP sensor on it, you can provide values the following ways:

- Providing the value https:/// in the URL field, PRTG will automatically create the URL https://www.example.com/ from that.
- Using the value /help in the URL field, PRTG will automatically create and monitor the URL http://www.example.com/help
- It is also possible to provide a port number in the URL field which will be taken over by the device's DNS name and internally added, for example, http://:8080/

Smart URL replacement does not work for sensors running on the **Probe Device**.

More

Knowledge Base: Which HTTP status code leads to which HTTP sensor status?

- https://kb.paessler.com/en/topic/65731

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

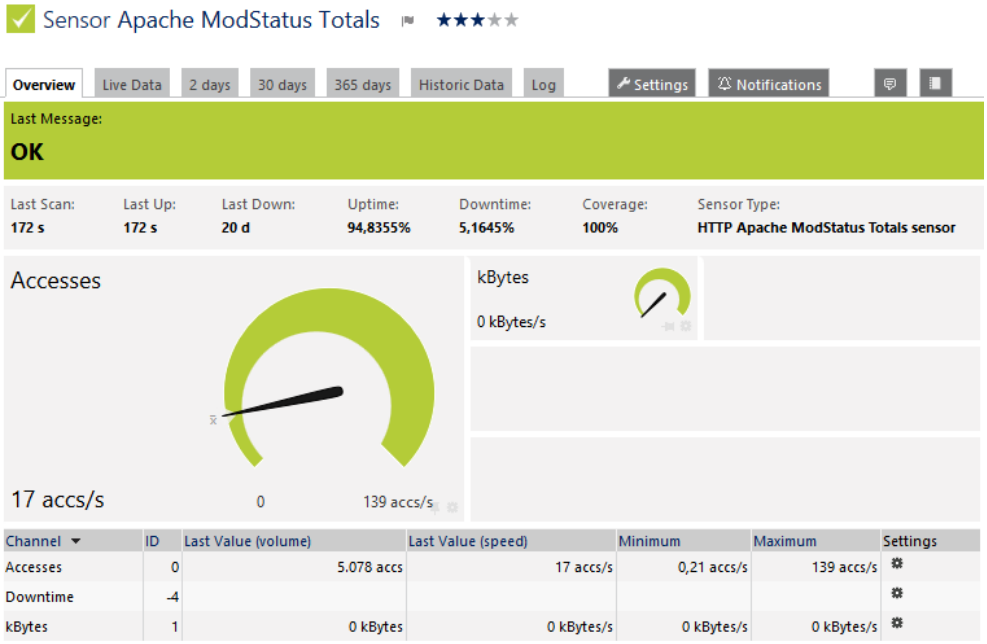
7.8.48 HTTP Apache ModStatus Totals Sensor

The HTTP Apache ModStatus Totals sensor monitors the activity of an Apache web server using mod_status over Hypertext Transfer Protocol (HTTP).

It can show the following:

- Number of accesses
- Transferred data in kilobytes per second

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



HTTP Apache ModStatus Totals Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/http_apache_modstatus_totals.png

Remarks

- Supports Smart URL Replacement 892.
- Knowledge Base: Which HTTP status code leads to which HTTP sensor status?
- This sensor type does not support Secure Remote Password (SRP) ciphers.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

HTTP SPECIFIC

Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).

HTTP SPECIFIC

URL	Enter the URL to the mod_status module on your Apache server. PRTG will append a "/server_status?auto" part automatically. If you enter an absolute URL, this address will be independent from the **IP address/DNS name** setting of the device this sensor is created on. PRTG uses a smart URL replacement which allows you to use the parent device's IP address/DNS name setting as part of the URL. For more information, please see section **Smart URL Replacement** below.

This sensor type implicitly supports Server Name Identification (SNI), an extension to the TLS protocol.

AUTHENTICATION

Authentication	Define if the web page at the configured URL needs authentication. Choose between: ▪ **No authentication needed** ▪ **Web page needs authentication**
User	This field is only visible if you enable authentication above. Enter a username. Please enter a string.
Password	This field is only visible if you enable authentication above. Enter a password. Please enter a string.
Authentication Method	This field is only visible if enable authentication above. Select the authentication method the given URL is protected with. Choose between: ▪ **Basic access authentication (HTTP)**: Use simple HTTP authentication. This is the default setting and suitable for most cases. This authentication method transmits credentials as plain text. ▪ **Windows NT LAN Manager (NTLM)**: Use the Microsoft NTLM protocol for authentication. This is sometimes used in intranets for single sign-on. ▪ **Digest Access Authentication**: Use digest access authentication that applies a hash function to the password which is safer than basic access authentication.

AUTHENTICATION

We recommend that you use the default value.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

PROXY SETTINGS FOR HTTP SENSORS

HTTP Proxy Settings	The proxy settings determine how a sensor connects to a given URL. You can enter data for an HTTP proxy server that sensors will use when connecting via HTTP or HTTPS. This setting affects monitoring only and determines the behavior of HTTP sensors. To change proxy settings for the core server, please see **System Administration—Core & Probes** 2967. The **SSL Certificate Sensor** 2289 and the **SSL Security Check Sensor** 2299 do not support HTTP proxies, but you can configure connections via SOCKS proxies in their sensor settings.
Name	Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.
Port	Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.
User	If the proxy requires authentication, enter the username for the proxy login. Only basic authentication is available! Please enter a string or leave the field empty.
Password	If the proxy requires authentication, enter the password for the proxy login. Only basic authentication is available! Please enter a string or leave the field empty.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

SCANNING INTERVAL

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

Smart URL Replacement

Instead of entering a complete address in the URL field of an HTTP sensor, you can merely enter the protocol followed by colon and three slashes (that means you can enter either http:/// or https:/// or even a simple slash / as equivalent for http:///). PRTG will then fill in the parent device's **IP address** or **DNS name** in front of the third slash automatically. Whether this results in a valid URL or not, depends on the IP address or DNS name of the device where this HTTP sensor is created on. In combination with cloning devices, the smart URL replacement makes it easy to create many like devices.

For example, if you create a device with **DNS name** www.example.com and you put an HTTP sensor on it, you can provide values the following ways:

- Providing the value https:/// in the URL field, PRTG will automatically create the URL https://www.example.com/ from that.
- Using the value /help in the URL field, PRTG will automatically create and monitor the URL http://www.example.com/help
- It is also possible to provide a port number in the URL field which will be taken over by the device's DNS name and internally added, for example, http://:8080/

Smart URL replacement does not work for sensors running on the **Probe Device**.

More

Knowledge Base: Which HTTP status code leads to which HTTP sensor status?

- https://kb.paessler.com/en/topic/65731

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

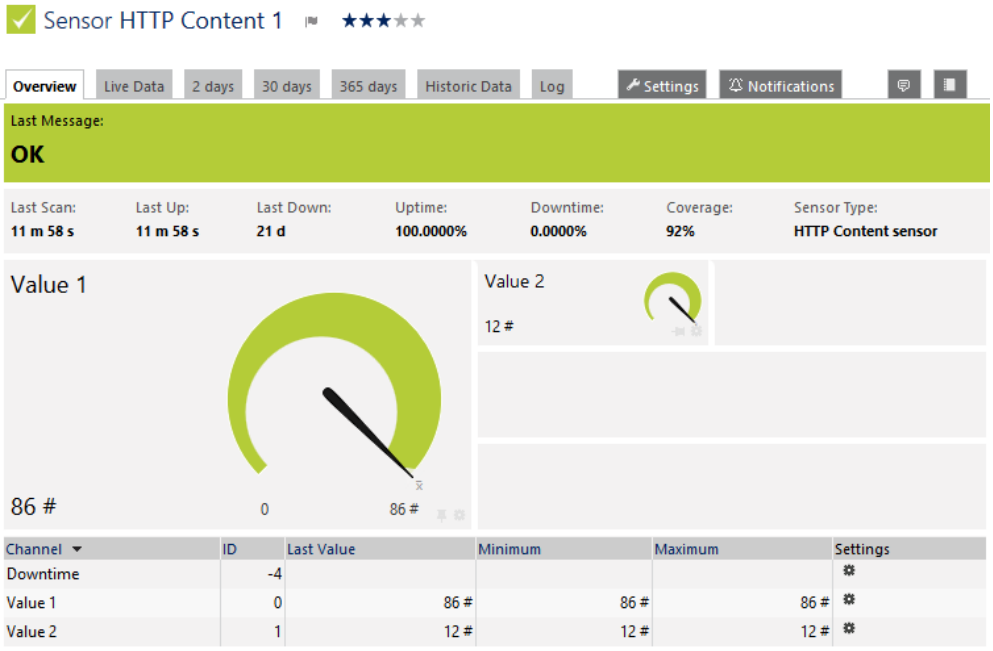
For more general information about settings, please see the **Object Settings** 188 section.

7.8.49 HTTP Content Sensor

The HTTP Content sensor monitors a numerical value returned by an Hypertext Transfer Protocol (HTTP) request. In the returned HTML page, each value must be placed between square brackets [ ]. See the example 903 below.

- It shows the returned numbers in dedicated channels, one channel for each value.

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



HTTP Content Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/http_content.png

Remarks

- This sensor does not support more than 50 channels 895 officially.
- Supports Smart URL Replacement 904.
- Knowledge Base: How can I monitor internal values of a web application with PRTG
- See also the PRTG manual: **HTTP Content Sensor—Example** 903
- Knowledge Base: Which HTTP status code leads to which HTTP sensor status?
- This sensor type does not support Secure Remote Password (SRP) ciphers.

Limited to 50 Sensor Channels

PRTG does not support more than 50 sensor channels officially. Depending on the data used with this sensor type, you might exceed the maximum number of supported sensor channels. In this case, PRTG will try to display all sensor channels. However, please be aware that you will experience limited usability and performance.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

HTTP SPECIFIC

Value Type	Define what kind of values your HTML file gives back. Choose between: ▪ **Integer**: An integer is expected as return value. ▪ **Float:** A float is expected as return value, with a dot (.) between pre-decimal position and decimal places. In this setting, the sensor will also display integer values unless they don't produce a buffer overflow. The sensor cannot handle string values.
Number of Channels	Define how many values your HTML file gives back. The sensor handles each value in its own sensor channel 121. Each value must be placed between square brackets [ ]. Enter the number of bracket-value pairs that the defined URL will return. Please enter an integer value. Do not enter a number less than the number of values returned. Otherwise you will get an error message.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

HTTP SPECIFIC

Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).
Script URL	Enter the URL the sensor connects to. It has to be URL encoded! If you enter an absolute URL, this address will be independent from the **IP address/DNS name** setting of the device this sensor is created on. PRTG uses a smart URL replacement which allows you to use the parent device's IP address/DNS name setting as part of the URL. For more information, please see section **Smart URL Replacement** below.
Value Type	Shows the kind of values that the HTML file returns. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

This sensor type implicitly supports Server Name Identification (SNI), an extension to the TLS protocol.

ADVANCED SENSOR DATA

Content Changes

Define what the sensor will do if the content of the monitored web page changes. Choose between:

- **Ignore changes**: No action will be taken on change.
- **Trigger 'change' notification**: The sensor will send an internal message indicating that the web page content has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification 2791 whenever the web page content changes.

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result**: Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section **Data Storage** 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

AUTHENTICATION

Authentication

Define if the web page at the configured URL needs authentication. Choose between:

- **No authentication needed**
- **Web page needs authentication**

User

This field is only visible if you enable authentication above. Enter a username. Please enter a string.

AUTHENTICATION

Password	This field is only visible if you enable authentication above. Enter a password. Please enter a string.
Authentication Method	This field is only visible if enable authentication above. Select the authentication method the given URL is protected with. Choose between: ▪ **Basic access authentication (HTTP)**: Use simple HTTP authentication. This is the default setting and suitable for most cases. ⓘ This authentication method transmits credentials as plain text. ▪ **Windows NT LAN Manager (NTLM)**: Use the Microsoft NTLM protocol for authentication. This is sometimes used in intranets for single sign-on. ▪ **Digest Access Authentication**: Use digest access authentication that applies a hash function to the password which is safer than basic access authentication. We recommend that you use the default value.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. ⓘ You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. ⓘ This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

SENSOR DISPLAY

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

PROXY SETTINGS FOR HTTP SENSORS

HTTP Proxy Settings	The proxy settings determine how a sensor connects to a given URL. You can enter data for an HTTP proxy server that sensors will use when connecting via HTTP or HTTPS. This setting affects monitoring only and determines the behavior of HTTP sensors. To change proxy settings for the core server, please see **System Administration—Core & Probes** 2967. The **SSL Certificate Sensor** 2289 and the **SSL Security Check Sensor** 2299 do not support HTTP proxies, but you can configure connections via SOCKS proxies in their sensor settings.
Name	Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.
Port	Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.
User	If the proxy requires authentication, enter the username for the proxy login. Only basic authentication is available! Please enter a string or leave the field empty.
Password	If the proxy requires authentication, enter the password for the proxy login.

PROXY SETTINGS FOR HTTP SENSORS

Only basic authentication is available! Please enter a string or leave the field empty.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

Example

For example, consider a URL http://www.example.com/status.html that returns a PHP script with the current system status in a simple HTML page as follows:

```
<html>
 <body>
  Description: Script gives back current status of disk free (%) and CPU usage (%).
  [85.5][12.0]
 </body>
</html>
```

You would configure the HTTP Content sensor using

- the script **URL** from above,
- value type **Float**,

- and number of channels **2**.

The sensor calls the URL with every scanning interval and only regard the two values in square brackets [ ], handling each of them in one sensor channel. The additional description text and HTML tags are not necessary. In this example they are added in case a human calls the URL.

If you define the number of channels as **1**, the sensor will read only the first value. The second value will be ignored. Using **3** as number of channels will result in a sensor error message.

Smart URL Replacement

Instead of entering a complete address in the URL field of an HTTP sensor, you can merely enter the protocol followed by colon and three slashes (that means you can enter either http:/// or https:/// or even a simple slash / as equivalent for http:///). PRTG will then fill in the parent device's **IP address** or **DNS name** in front of the third slash automatically. Whether this results in a valid URL or not, depends on the IP address or DNS name of the device where this HTTP sensor is created on. In combination with cloning devices, the smart URL replacement makes it easy to create many like devices.

For example, if you create a device with **DNS name** www.example.com and you put an HTTP sensor on it, you can provide values the following ways:

- Providing the value https:/// in the URL field, PRTG will automatically create the URL https://www.example.com/ from that.
- Using the value /help in the URL field, PRTG will automatically create and monitor the URL http://www.example.com/help
- It is also possible to provide a port number in the URL field which will be taken over by the device's DNS name and internally added, for example, http://:8080/

Smart URL replacement does not work for sensors running on the **Probe Device**.

More

Knowledge Base: Which HTTP status code leads to which HTTP sensor status?

- https://kb.paessler.com/en/topic/65731

Knowledge Base: How can I monitor internal values of a web application with PRTG?

- https://kb.paessler.com/en/topic/4

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

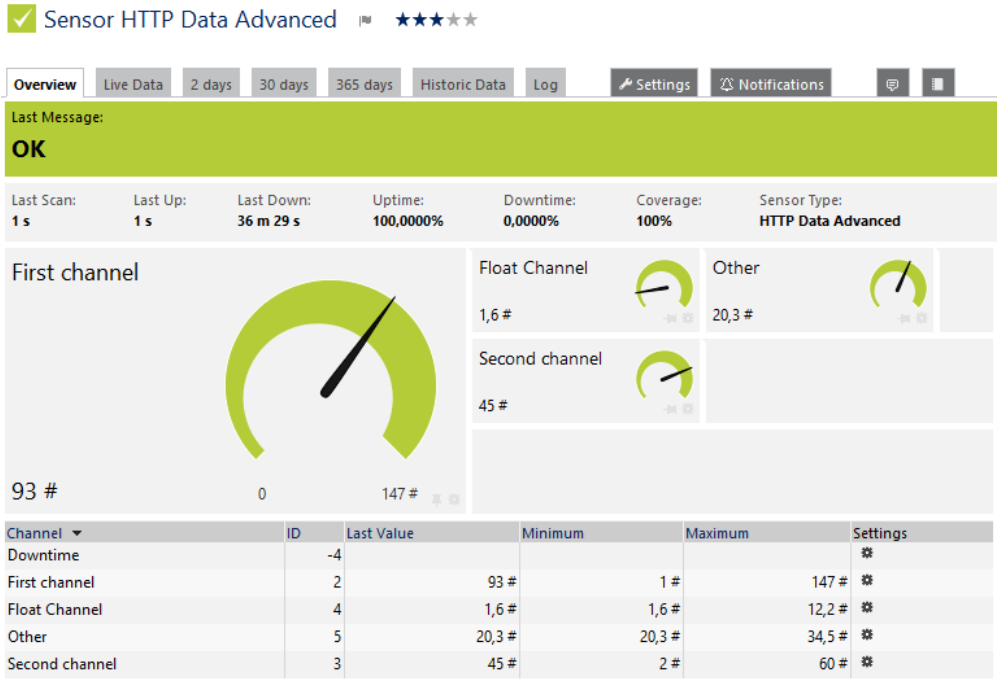
Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.50 HTTP Data Advanced Sensor

The HTTP Data Advanced sensor accesses a web server and retrieves XML or JSON encoded data. For details about the return value format, please see the **Application Programming Interface (API) Definition** 3174.

- The sensor can show values returned by the web server in multiple channels.



HTTP Data Advanced Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/http_data_advanced.png

Remarks

- The requested web server must return XML or JSON encoded data that matches the format as defined in the API documentation 3174 in section **Custom Sensors—Advanced Script and HTTP Data Sensors**.
- For best sensor performance, we recommend you specify the content type on the target server, which is application/xml or application/json.
- Knowledge Base: Which HTTP status code leads to which HTTP sensor status?
- This sensor type does not support Secure Remote Password (SRP) ciphers.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

HTTP SPECIFIC

Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).
URL	Enter the URL the sensor connects to. It has to be URL encoded!

HTTP SPECIFIC

	If you enter an absolute URL, the sensor uses this address independently from the **IP address/DNS name** setting of the device on which you create this sensor. You can enter an URL leading to a webpage (to measure the page source code's loading time), or enter the URL of an image or of another page asset to measure this element's availability and loading time. PRTG uses a smart URL replacement which allows you to use the parent device's IP address/DNS name setting as part of the URL. For more information, please see section **Smart URL Replacement** below.
Request Method	Choose an HTTP request method to determine how the sensor will request the given URL. ▪ **GET**: Request the website directly, like browsing the web. We recommend using this setting for a simple check of a web page. ▪ **POST**: Send post form data to the URL. If this setting is chosen, you must enter the data that will be sent in the **Postdata** field below. ▪ **HEAD**: Only request the HTTP header from the server; without the actual web page. Although this saves bandwidth since less data is transferred, it is not recommended because the measured request time is not the one experienced by your users and you might not be notified for slow results or timeouts.
Postdata	This field is only visible when you select the POST **Request Method** setting above. Enter the data part for the POST request here. No XML is allowed here!
Content Type	This setting is only visible when you select the POST **Request Method** setting above. Define the content type of a POST request. Choose between: ▪ **Default (application/x-www-form-urlencoded)**: This is the default content type used to encode the form data set for submission to the server. ▪ **Custom**: If you need another content type than default, enter this content type below.
Custom Content Type	This field is only visible when you select **Custom** above. Define the content type which is needed, for example, XML, JSON, HTTP.

HTTP SPECIFIC

Server Name Indication	Shows the Server Name Identification (SNI) that the sensor automatically determined from the host address of the parent device 360 or the target URL of the sensor. SNI has to be a Fully Qualified Domain Name (FQDN). Please ensure it matches the configuration of the target server. For details, see the Knowledge Base article My HTTP sensors fail to monitor websites which use SNI. What can I do?
SNI Inheritance	Define if you want to inherit the Server Name Identification (SNI) from the parent device. See the **Server Name Indication** setting above which SNI is determined. Choose between: ▪ **Inherit SNI from parent device**: The sensor determines the SNI from the host address of the parent device. ▪ **Do not inherit SNI from parent device**: The sensor determines the SNI from the target **URL** as defined in the settings of this sensor.

Result Handling	Define what the sensor will do with the data loaded at the given URL. Choose between: • **Discard HTML result**: Do not store the requested data. • **Store latest HTML result**: Store the last result of the requested data to the **Logs (Sensors)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File name: Result of Sensor [ID].txt. This is for debugging purposes, especially in combination with content checks. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, see section **Data Storage** 3226.

ADVANCED SENSOR DATA

Protocol Version	Define the HTTP protocol version that the sensor will use when connecting to the target URL. Choose between: ▪ **HTTP 1.0** ▪ **HTTP 1.1**: This is the default setting.
User Agent	Choose which user agent string the sensor will send when connecting to the target URL. Choose between:

ADVANCED SENSOR DATA

	▪ **Use PRTG's default string**: Do not enter a specific user agent, use the default setting. Usually, this is: Mozilla/5.0 (compatible; PRTG Network Monitor (www.paessler.com); Windows) ▪ **Use a custom string**: Use a custom user agent. Define below.
Custom User Agent	This field is only visible if you enable custom user agent above. Enter a string to be used as user agent when connecting to the URL specified above.
Use Custom HTTP Headers	Define if you want to send custom HTTP headers to the target URL. Choose between: ▪ **Do not use custom HTTP headers** ▪ **Use custom HTTP headers**
Custom HTTP Headers	This field is only available if you select using custom headers above. Enter a list of custom HTTP headers with theirs respective values that you want to transmit to the URL you define above, each pair in one line. The syntax of a header-value pair is header1:value1 The sensor does not support the header field names user-agent, content-length, host. Ensure the HTTP header statement is valid! Otherwise, the sensor request will not be successful.

AUTHENTICATION

Authentication	Define if the web page at the configured URL needs authentication. Choose between: ▪ **No authentication needed** ▪ **Web page needs authentication**
User	This field is only visible if you enable authentication above. Enter a username. Please enter a string.
Password	This field is only visible if you enable authentication above. Enter a password. Please enter a string.

AUTHENTICATION

Authentication Method

This field is only visible if enable authentication above. Select the authentication method the given URL is protected with. Choose between:

- **Basic access authentication (HTTP)**: Use simple HTTP authentication. This is the default setting and suitable for most cases.
  This authentication method transmits credentials as plain text.
- **Windows NT LAN Manager (NTLM)**: Use the Microsoft NTLM protocol for authentication. This is sometimes used in intranets for single sign-on.
- **Digest Access Authentication**: Use digest access authentication that applies a hash function to the password which is safer than basic access authentication.

We recommend that you use the default value.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.
- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

SENSOR DISPLAY

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

PROXY SETTINGS FOR HTTP SENSORS

HTTP Proxy Settings	The proxy settings determine how a sensor connects to a given URL. You can enter data for an HTTP proxy server that sensors will use when connecting via HTTP or HTTPS. This setting affects monitoring only and determines the behavior of HTTP sensors. To change proxy settings for the core server, please see **System Administration—Core & Probes** 2967. The **SSL Certificate Sensor** 2289 and the **SSL Security Check Sensor** 2299 do not support HTTP proxies, but you can configure connections via SOCKS proxies in their sensor settings.
Name	Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.
Port	Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.
User	If the proxy requires authentication, enter the username for the proxy login. Only basic authentication is available! Please enter a string or leave the field empty.
Password	If the proxy requires authentication, enter the password for the proxy login.

PROXY SETTINGS FOR HTTP SENSORS

Only basic authentication is available! Please enter a string or leave the field empty.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

Smart URL Replacement

Instead of entering a complete address in the URL field of an HTTP sensor, you can merely enter the protocol followed by colon and three slashes (that means you can enter either http:/// or https:/// or even a simple slash / as equivalent for http:///). PRTG will then fill in the parent device's **IP address** or **DNS name** in front of the third slash automatically. Whether this results in a valid URL or not, depends on the IP address or DNS name of the device where this HTTP sensor is created on. In combination with cloning devices, the smart URL replacement makes it easy to create many like devices.

For example, if you create a device with **DNS name** www.example.com and you put an HTTP sensor on it, you can provide values the following ways:

- Providing the value https:/// in the URL field, PRTG will automatically create the URL https://www.example.com/ from that.
- Using the value /help in the URL field, PRTG will automatically create and monitor the URL http://www.example.com/help
- It is also possible to provide a port number in the URL field which will be taken over by the device's DNS name and internally added, for example, http://:8080/

Smart URL replacement does not work for sensors running on the **Probe Device**.

More

Knowledge Base: Which HTTP status code leads to which HTTP sensor status?

- https://kb.paessler.com/en/topic/65731

Knowledge Base: My HTTP sensors fail to monitor websites which use SNI. What can I do?

- https://kb.paessler.com/en/topic/67398

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

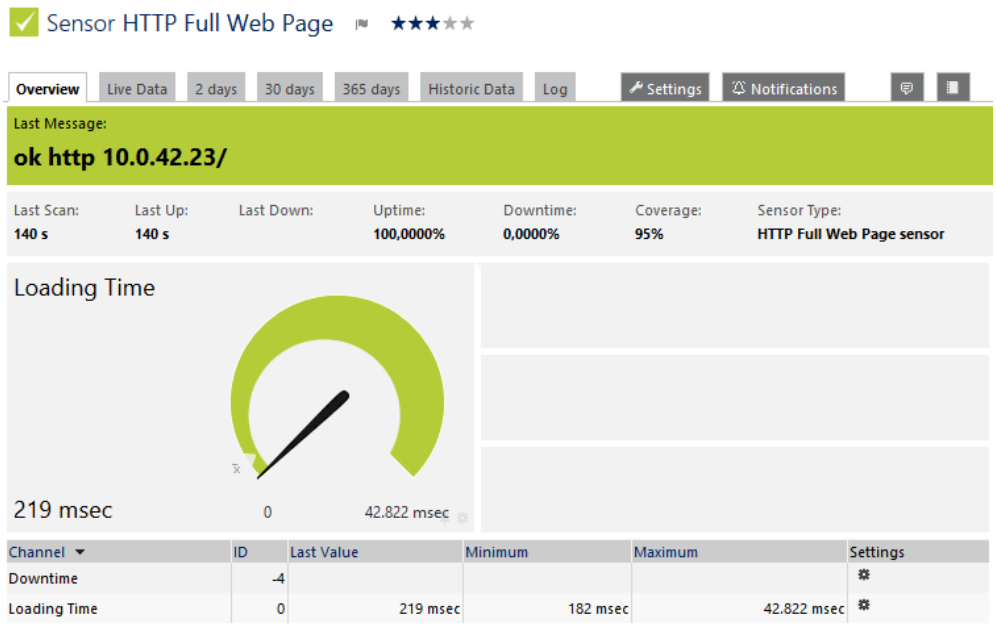
For more general information about settings, please see the **Object Settings** 188 section.

7.8.51 HTTP Full Web Page Sensor

The HTTP Full Web Page sensor monitors the full download time of a web page including assets such as images, etc. In the background, it opens the web page in a browser instance to perform the measurement. Links are not followed.

- This sensor shows the loading time of the full web page.

Be careful with this sensor, because it can generate considerable internet traffic if you use it with a low scanning interval!



HTTP Full Web Page Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/http_full_web_page.png

Remarks

- Supports Smart URL Replacement 927.
- Knowledge Base: What to do when I see a CreateUniqueTempDir() error message for my HTTP Full Webpage Sensor?
- Knowledge Base: HTTP Full Web Page sensor is unable to navigate. What can I do?
- Knowledge Base: How can I change the size of PhantomJS full web page screenshots?
- Knowledge Base: Which HTTP status code leads to which HTTP sensor status?
- This sensor type does not support Secure Remote Password (SRP) ciphers.
- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

FULL PAGE DOWNLOAD SETTINGS

Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).
URL	Enter the address of the web page that the sensor loads. It has to be URL encoded! If you enter an absolute URL, this address will be independent from the **IP address/DNS name** setting of the device this sensor is created on. PRTG uses a smart URL replacement which allows you to use the parent device's IP address/DNS name setting as part of the URL. For more information, please see section **Smart URL Replacement** below.
Browser Engine	Define which browser the sensor uses to load the web page. Choose between: ▪ **Chromium (recommended)**: Use the "WebKit" engine that is delivered with PRTG to perform the loading test. With each scanning interval, PRTG will load the URL defined above in an instance of "Chromium" and measure the time until the page is fully loaded. This is the recommended setting. ▪ **PhantomJS (Headless Webkit)**: Use the "PhantomJS" engine. This engine can have a high impact on your probe system's CPU and memory load, but there are additional options for result handling available (see below). ▪ **Internet Explorer**: With each scanning interval, the URL defined above is loaded in the background in an instance of Internet Explorer. PRTG uses the Internet Explorer of the system running the PRTG probe. For full functionality we strongly recommend you to install Internet Explorer 11 or higher on the system running the PRTG probe. The probe machine is either the local system (on every node, if on a cluster probe), or the system running the remote probe 3196 where the sensor is created. For all browser engines, the same proxy settings are used that are configured for the Windows user account that the PRTG probe is running on (this is usually the Windows local "system" user account, if not changed). These settings are accessible via the Internet Explorer of this system. If you want to use a proxy for this full web page sensor test, for example, please adjust the Internet Explorer's settings accordingly (on the computer running the probe; on all nodes, if in a cluster).
Security Context	Define the Windows user account that the sensor uses to run the browser engine. Choose between:

FULL PAGE DOWNLOAD SETTINGS

- **Use security context of probe service (default)**: Run the browser engine under the same Windows user account the PRTG probe is running on. By default, this is the local Windows "system" user account (if not manually changed).
- **Use Windows credentials of parent device**: Use the Windows user account defined in the settings of the parent device this sensor is created on. Please go to the sensor's parent device's settings to change the Windows credentials.
  When using the Chromium browser engine above, we recommended this setting here.

Result Handling

This setting is only visible if you select the PhantomJS engine above. This browser engine can render and store screenshots of the loaded web page. Choose between:

- **Discard HTML result (recommended)**: Do not store the requested web page.
- **Render and store a screenshot of most recent sensor result as JPG**: Render and store the last result of the web page to the **Logs (Sensors)** directory (on the remote system, when used on a remote probe; on the Master node, if in a cluster). This is for debugging purposes. The file will be overridden with each scanning interval. It will be named using the pattern Fullpage of Sensor (ID).jpg. For information on how to find the folder used for storage, please see **Data Storage** 3226 section.
- **Store and store screenshots of all sensor results as JPGs (requires lots of disk space)**: Render and store one new screenshot of the web page with each sensor scan, and store the pictures in the **Screenshots (Fullpage Sensor)** directory (on the remote system, when used on a remote probe). For information on how to find the folder used for storage, please see **Data Storage** 3226 section. This option can be used to create a visual history of the web page.
  Depending on the monitored website and the scanning interval of the sensor, this option can create a very high amount of data! Use with care and make sure you set appropriate data purging limits in the **System Administration—Core & Probes** 2972 settings.

If necessary, you can change the window size of the rendered screenshots. For details, see the Knowledge Base article How can I change the size of PhantomJS full web page screenshots?

Depending on the result handling method you choose, the sensor does not only store files in the screenshot directory, but there will also be files in an extra cache directory. If your disk on the probe system runs full, please also check this path (you might have to set folder options appropriately to see this directory):

FULL PAGE DOWNLOAD SETTINGS

C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5

Authentication

This setting is only visible if you select the **PhantomJS** engine above. Define if the monitored web page needs authentication for access. Choose between:

- **No authentication needed**: Access to the web page is granted without authentication.
- **Web page needs authentication**: PRTG automatically tries to use HTTP Basic authentication (BA) or Windows NT LAN Manager (NTLM) to access the web page with authentication. Enter the credentials below.
  Basic access authentication forwards the credentials in plain text!

User

This setting is only visible if you select the **PhantomJS** engine with authentication above. Enter the username for the web page.

Password

This setting is only visible if you select the **PhantomJS** engine with authentication above. Enter the password for the web page.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.
- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

SENSOR DISPLAY

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.

SCANNING INTERVAL

- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices** | **Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

Smart URL Replacement

Instead of entering a complete address in the URL field of an HTTP sensor, you can merely enter the protocol followed by colon and three slashes (that means you can enter either http:/// or https:/// or even a simple slash / as equivalent for http:///). PRTG will then fill in the parent device's **IP address** or **DNS name** in front of the third slash automatically. Whether this results in a valid URL or not, depends on the IP address or DNS name of the device where this HTTP sensor is created on. In combination with cloning devices, the smart URL replacement makes it easy to create many like devices.

For example, if you create a device with **DNS name** www.example.com and you put an HTTP sensor on it, you can provide values the following ways:

- Providing the value https:/// in the URL field, PRTG will automatically create the URL https://www.example.com/ from that.
- Using the value /help in the URL field, PRTG will automatically create and monitor the URL http://www.example.com/help
- It is also possible to provide a port number in the URL field which will be taken over by the device's DNS name and internally added, for example, http://:8080/

Smart URL replacement does not work for sensors running on the **Probe Device**.

More

Knowledge Base: Which HTTP status code leads to which HTTP sensor status?

- https://kb.paessler.com/en/topic/65731

Knowledge Base: What to do when I see a CreateUniqueTempDir() error message for my HTTP Full Webpage Sensor?

- https://kb.paessler.com/en/topic/40783

Knowledge Base: HTTP Full Web Page sensor is "unable to navigate". What can I do?

- https://kb.paessler.com/en/topic/59999

Knowledge Base: How can I change the size of PhantomJS full web page screenshots?

- https://kb.paessler.com/en/topic/60247

Knowledge Base: What is the difference between "HTTP" and "HTTP Full Web Page" Web Server sensors?

- https://kb.paessler.com/en/topic/943

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

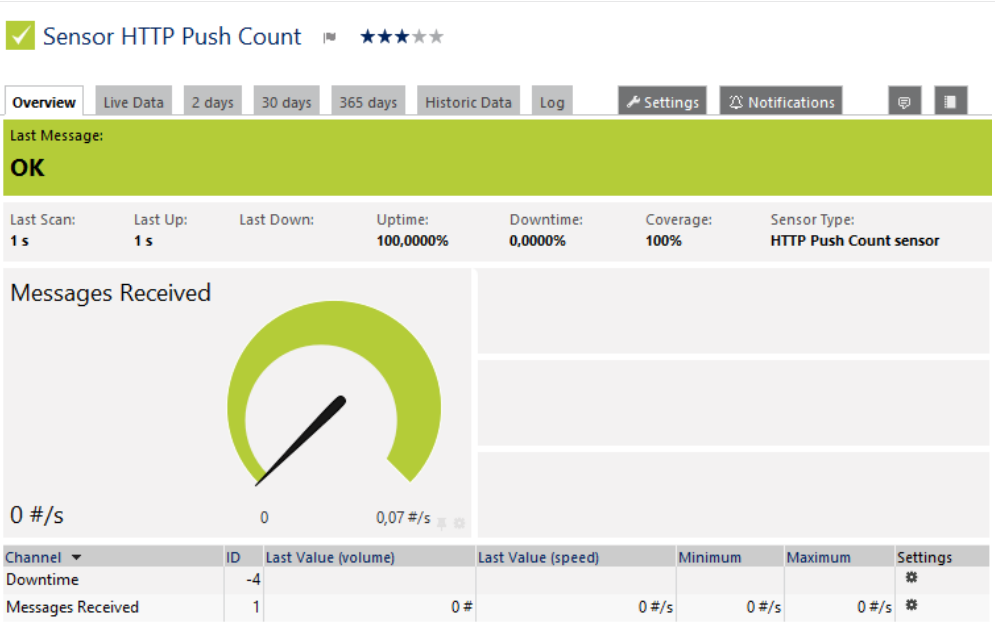
Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.52 HTTP Push Count Sensor

The HTTP Push Count sensor counts received messages that are pushed via a Hypertext Transfer Protocol (HTTP) request to PRTG. It provides a URL that you can use to push messages to the PRTG probe system via HTTP (insecure or TLS 1.2 encrypted).

- It shows the number of received messages per second.



HTTP Push Count Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/http_push_count.png

Remarks

- For details about the usage, please see manual section **HTTP Push Count Sensor—How to Use** 929.
- Knowledge Base: Which HTTP status code leads to which HTTP sensor status?
- This sensor type cannot be used in cluster mode. You can set it up on a local probe or remote probe only, not on a cluster probe.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

How to Use

This function is known as webhook. Basically, a webhook works like a push notification. Webhooks are usually triggered by some event (for example, a new comment to a blog post) and send according information to a specified URL. The HTTP Push Count sensor then displays the number of pushed and received messages.

Use the following URL to receive the HTTP requests of the webhook:

http://<probe_ip>**:**<port_number>**/**<token>

Replace the parameters <probe_ip>, <port_number>, and <token> with the corresponding values. You can define port number and identification token in the sensor settings. The probe IP is the IP address of the system your PRTG probe with the sensor is running on.

Example:

```
http://127.0.0.1:5050/XYZ123
```

You can use several sensors with the same port and identification token. In this case, the number of push messages will be shown in each of these sensors.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

HTTP PUSH

SSL Settings	Define the security of the incoming HTTP push requests. Choose between: ▪ **HTTP (unsafe)**: Send push messages to the PRTG probe system via insecure HTTP. ▪ **HTTPS (TLS 1.2 only)**: Send push messages to the PRTG probe system via secure HTTPS. The sensor only supports TLS 1.2 connections. It will use the SSL certificate that is delivered with PRTG or your own trusted SSL certificate 3228 that you have imported for the PRTG web server.
Port	This field is only visible if you choose HTTP above. Enter the number of the port on which this sensor listens for incoming HTTP requests. Default is **5050**.
SSL Port	This filed is only visible if you choose HTTPS above. Enter the number of the port on which this sensor listens for incoming HTTPS requests. Default is **5051**.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

HTTP PUSH

SSL Settings	Shows whether the sensor accepts push messages via HTTP or HTTPS. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Port	This field is only visible for sensors that accept push messages via HTTP. It shows the port number on which this sensor listens for incoming HTTP requests.

HTTP PUSH

	Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
SSL Port	This field is only visible for sensors that accept push messages via HTTPS. It shows the port number on which this sensor listens for incoming HTTPS requests. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Request Method	Select the request method of your webhook: ▪ **ANY**: Do not use any filter for the request method. ▪ **GET**: Choose this method if your webhook uses GET. ▪ **POST**: Choose this method if your webhook sends post form data. Postdata has to be **application/x-www-form-urlencoded** with the same parameters as for GET requests.
Identification Token	This is the token that is used to find the matching sensor for the incoming message. While you create the sensor, this token is {__guid__}. It is replaced with an automatically generated token after you have completed the sensor creation. If you want to use another identification token, you can edit it while or after sensor creation. ⓘ The token will not be replaced automatically if you change it already during sensor creation.
Incoming Request	Define what PRTG will do with the incoming messages. Choose between: ▪ **Discard request**: Do not store the pushed messages. ▪ **Write request to disk (Filename: "Request for Sensor [ID].txt")**: Store the last message received from the sensor to the **Logs (Sensor)** directory (on the Master node, if in a cluster). File name: Request for Sensor [ID].txt. This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see **Data Storage** 3226 section.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: Which HTTP status code leads to which HTTP sensor status?

- https://kb.paessler.com/en/topic/65731

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

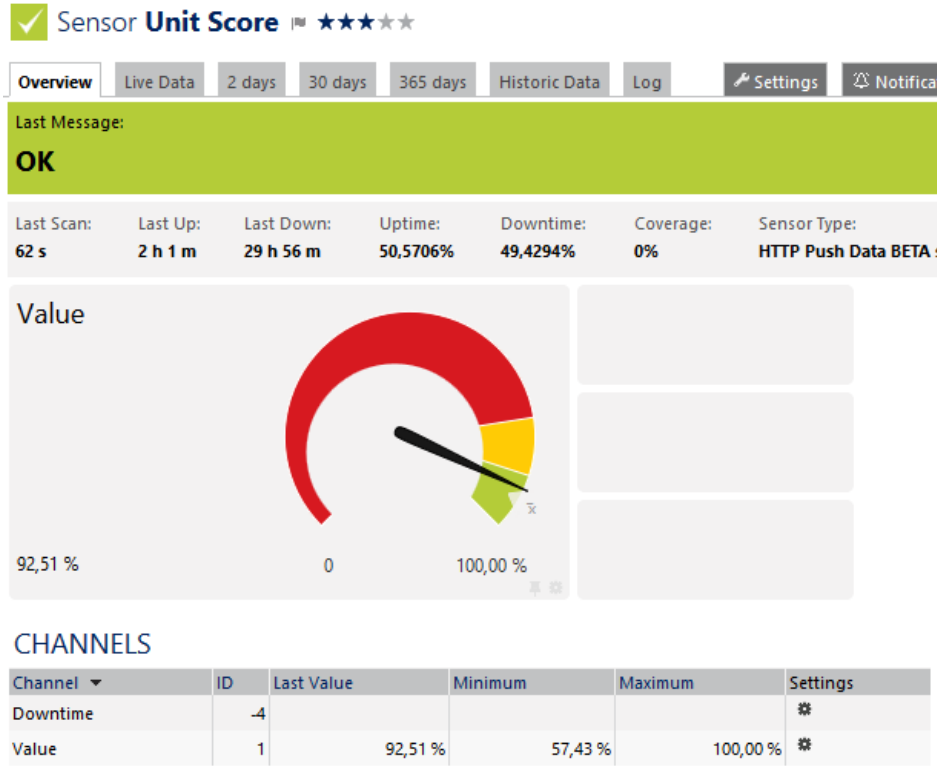
Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.53 HTTP Push Data Sensor

The HTTP Push Data sensor displays numerical values from received messages that are pushed via a Hypertext Transfer Protocol (HTTP) request to PRTG. It provides a URL that you can use to push messages to the PRTG probe system via HTTP (insecure or TLS 1.2 encrypted).

- The sensor shows the received value and an optional message in one channel.



HTTP Push Data Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/http_push_data.png

Remarks

- For details about the usage, please see manual section **HTTP Push Data Sensor—How to Use** 940.
- Knowledge Base: Which HTTP status code leads to which HTTP sensor status?
- This sensor type cannot be used in cluster mode. You can set it up on a local probe or remote probe only, not on a cluster probe.
- Currently, this sensor type is in beta status. The methods of operating can change at any time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.

BETA

- You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

How to Use

This function is known as webhook. Basically, a webhook works like a push notification. Webhooks are usually triggered by some event (for example, a new comment to a blog post) and send according information to a specified URL. The HTTP Push Data sensor then displays the data of pushed and received messages.

Use the following URL to receive the HTTP requests of the webhook:

http://<probe_ip>**:**<port_number>**/**<token>**?value=**<integer_or_float>**&text=**<text message>

Replace the parameters <probe_ip>, <port_number>, <token>, and <integer_or_float> with the corresponding values. The **&text** parameter is optional: You can omit it.

- You can define **port number** and **identification token** in the sensor settings.
- The **probe IP** is the IP address of the system on which your PRTG probe with this sensor is running on.
- The **value** can be an integer or a float value, depending on the data of your application; you have to set the value type accordingly in the sensor settings. This parameter will be the sensor value.
  If this parameter is missing, the sensor will show a **down** status.
- You can **optionally** add a custom text message by replacing the parameter <text message> with it. The text will be shown as sensor message. If there is no value but only a text, the text will be shown as error message.
  This text message has to be URL encoded (for example, the whitespaces in the sample URL below); most browsers achieve this automatically.

Example:

```
http://127.0.0.1:5050/XYZ123?value=0&text=this%20is%20a%20message
```

You can use several sensors with the same port and identification token. In this case, the data of push messages will be shown in each of these sensors.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

HTTP PUSH

SSL Settings	Define the security of the incoming HTTP push requests. Choose between: ▪ **HTTP (unsafe)**: Send push messages to the PRTG probe system via insecure HTTP. ▪ **HTTPS (TLS 1.2 only)**: Send push messages to the PRTG probe system via secure HTTPS. The sensor only supports TLS 1.2 connections. It will use the SSL certificate that is delivered with PRTG or your own trusted SSL certificate 3228 that you have imported for the PRTG web server.
Port	This field is only visible if you choose HTTP above. Enter the number of the port on which this sensor listens for incoming HTTP requests. Default is **5050**.
SSL Port	This filed is only visible if you choose HTTPS above. Enter the number of the port on which this sensor listens for incoming HTTPS requests. Default is **5051**.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	Enter one or more **Tags**, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

HTTP PUSH

SSL Settings	Shows whether the sensor accepts push messages via HTTP or HTTPS. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Port	This field is only visible for sensors that accept push messages via HTTP. It shows the port number on which this sensor listens for incoming HTTP requests. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
SSL Port	This field is only visible for sensors that accept push messages via HTTPS. It shows the port number on which this sensor listens for incoming HTTPS requests. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Request Method	Select the request method of your webhook: ▪ **ANY**: Do not use any filter for the request method. ▪ **GET**: Choose this method if your webhook uses GET.

HTTP PUSH

	▪ **POST**: Choose this method if your webhook sends post form data. Postdata has to be **application/x-www-form-urlencoded** with the same parameters as for GET requests.
Identification Token	This is the token that is used to find the matching sensor for the incoming message. While you create the sensor, this token is {__guid__}. It is replaced with an automatically generated token after you have completed the sensor creation. If you want to use another identification token, you can edit it while or after sensor creation. ⓘ The token will not be replaced automatically if you change it already during sensor creation.
Incoming Request	Define what PRTG will do with the incoming messages. Choose between: ▪ **Discard request**: Do not store the pushed messages. ▪ **Write request to disk (Filename: "Request for Sensor [ID].txt")**: Store the last message received from the sensor to the **Logs (Sensor)** directory (on the Master node, if in a cluster). File name: Request for Sensor [ID].txt. This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see **Data Storage** 3226 section.

HTTP PUSH DATA

No Incoming Data

Define which status 163 the sensor will attain if no push message has been received for at least two sensor scans. Choose between:

- **Ignore and keep last status (default)**: The sensor will remain in the status as defined by the last message received.
  The probe on which this sensor runs must be connected to keep the last status. If the probe is disconnected, the sensor will show the **Unknown** status. If the probe is connected again, the sensor does not automatically return from **Unknown** to the last status before the probe disconnect.
- **Switch to "Unknown" status**: The sensor will show an **Unknown** status if it has not received any message for at least two sensor scans.
- **Switch to "Error" after x minutes**: The sensor will show a **Down** status if it has not received any message within a defined time span. Define the time threshold below.

Time Threshold (Minutes)

This field is only visible if you select the error option above. Enter the time threshold in minutes after which the sensor status will show a **Down** status if it has not received a push message within this time span.

Please enter an integer value. The maximum threshold is **1440** minutes.

Value Type

Define which type the value of the received data has. If this setting does not match, the sensor will go into an **Down** status. Choose between:

- **Integer**
- **Float** (with dot "." as delimiter)

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

SENSOR DISPLAY

- **Show channels independently (default)**: Show an own graph for each channel.
- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: Which HTTP status code leads to which HTTP sensor status?

- https://kb.paessler.com/en/topic/65731

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

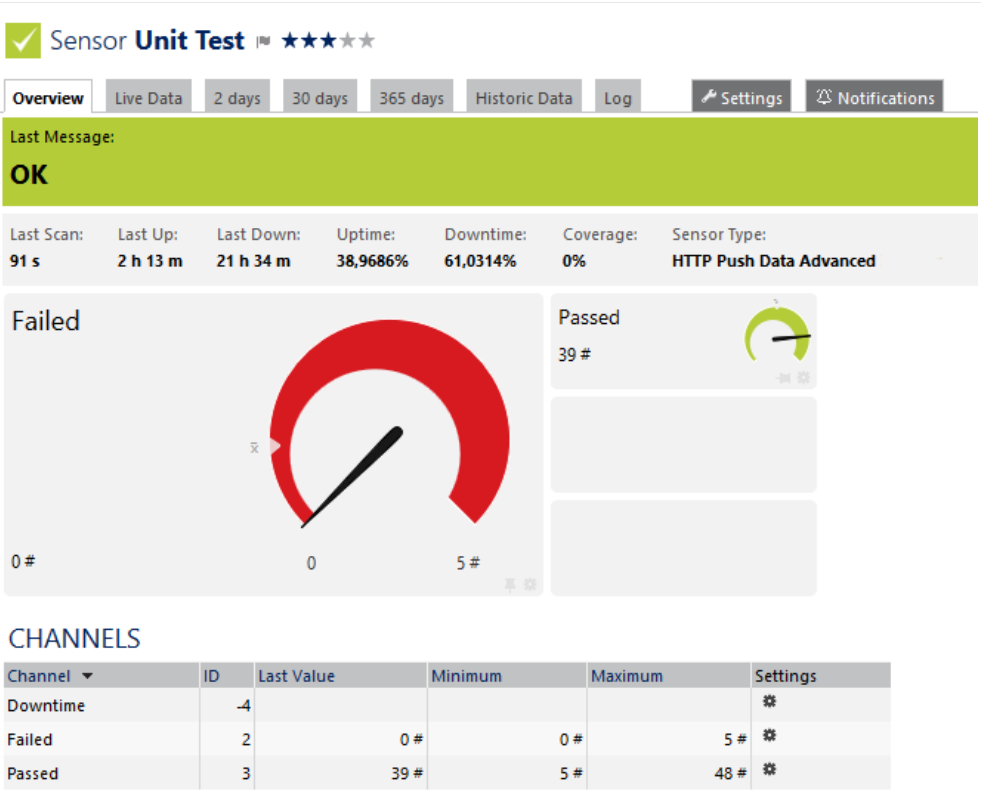
Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.54 HTTP Push Data Advanced Sensor

The HTTP Push Data Advanced sensor displays data from received messages that are pushed via a Hypertext Transfer Protocol (HTTP) request to PRTG. It provides a URL that you can use to push messages to the PRTG probe system via HTTP (insecure or TLS 1.2 encrypted).

- This sensor can show received values and a message encoded in valid XML or JSON in multiple channels.



HTTP Push Data Advanced Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/http_push_data_advanced.png

Remarks

- For details about the usage, please see manual section **HTTP Push Data Advanced Sensor—How to Use** 952.
- Knowledge Base: Which HTTP status code leads to which HTTP sensor status?
- This sensor type cannot be used in cluster mode. You can set it up on a local probe or remote probe only, not on a cluster probe.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

How to Use

This function is known as webhook. Basically, a webhook works like a push notification. Webhooks are usually triggered by some event (for example, a new comment to a blog post) and send according information to a specified URL. The HTTP Push Data Advanced sensor then displays the data of pushed and received messages.

The data that is pushed to this sensor must be valid XML or JSON. For details about the return value format please see the **Application Programming Interface (API) Definition**.

Use the following URLs to receive the HTTP requests of the webhook:

- **GET** requests: **http://**<probe_ip>**:**<port_number>**/**<token>**?content=**<valid XML_or_JSON>

  The XML encoded value of the content parameter has to match the format as defined in the API documentation in section **Custom Sensors—Advanced Script HTTP Data Sensors**.

- **POST** requests: **http://**<probe_ip>**:**<port_number>**/**<token>

  This HTTP request method sends the XML or JSON encoded HTTP body as POST data. The body has to match the format as defined in the API documentation in section **Custom Sensors—Advanced Script HTTP Data Sensors**. We strongly recommend the HTTP content type application/xml or application/json.

Replace the parameters <probe_ip>, <port_number>, <token> and <valid XML_or_JSON> (for GET requests) with the corresponding values:

- You can define **port number** and **identification token** in the sensor settings.
- The **probe IP** is the IP address of the system on which your PRTG probe with this sensor is running on.
- The content of GET requests has to be valid XML or JSON in the PRTG API format.
  The content has to be URL encoded (for example, the whitespaces in the sample URL below); most browsers achieve this automatically.

Minimum example for the GET method which returns one static channel value:

```
http://127.0.0.1:5050/XYZ123?content=<prtg><result><channel>MyChannel</channel><value>10</value></result><
```

By default, values within the <value> tags in the returned XML or JSON must be integers to be processed. If float values are returned, you have to explicitly define this value type according to the API documentation with <float> tags, otherwise the sensor will show **0** values in affected channels. Example:

```
http://127.0.0.1:5050/XYZ123?content=<prtg><result><channel>MyChannel</channel><value>10.45</value><float>
```

You can use several sensors with the same port and identification token. In this case, the data of push messages will be shown in each of these sensors.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

HTTP PUSH

SSL Settings	Define the security of the incoming HTTP push requests. Choose between: ▪ **HTTP (unsafe)**: Send push messages to the PRTG probe system via insecure HTTP. ▪ **HTTPS (TLS 1.2 only)**: Send push messages to the PRTG probe system via secure HTTPS. The sensor only supports TLS 1.2 connections. It will use the SSL certificate that is delivered with PRTG or your own trusted SSL certificate 3228 that you have imported for the PRTG web server.
Port	This field is only visible if you choose HTTP above. Enter the number of the port on which this sensor listens for incoming HTTP requests. Default is **5050**.
SSL Port	This filed is only visible if you choose HTTPS above. Enter the number of the port on which this sensor listens for incoming HTTPS requests. Default is **5051**.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

HTTP PUSH

SSL Settings	Shows whether the sensor accepts push messages via HTTP or HTTPS. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Port	This field is only visible for sensors that accept push messages via HTTP. It shows the port number on which this sensor listens for incoming HTTP requests. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
SSL Port	This field is only visible for sensors that accept push messages via HTTPS. It shows the port number on which this sensor listens for incoming HTTPS requests.

HTTP PUSH

Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Request Method

Select the request method of your webhook:

- **ANY**: Do not use any filter for the request method.
- **GET**: Choose this method if your webhook uses GET.
- **POST**: Choose this method if your webhook sends post form data. Postdata has to be **application/x-www-form-urlencoded** with the same parameters as for GET requests.

Identification Token

This is the token that is used to find the matching sensor for the incoming message. While you create the sensor, this token is {__guid__}. It is replaced with an automatically generated token after you have completed the sensor creation. If you want to use another identification token, you can edit it while or after sensor creation.

The token will not be replaced automatically if you change it already during sensor creation.

Incoming Request

Define what PRTG will do with the incoming messages. Choose between:

- **Discard request**: Do not store the pushed messages.
- **Write request to disk (Filename: "Request for Sensor [ID].txt")**: Store the last message received from the sensor to the **Logs (Sensor)** directory (on the Master node, if in a cluster). File name: Request for Sensor [ID].txt. This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see **Data Storage** 3226 section.

HTTP PUSH DATA

No Incoming Data

Define which status 163 the sensor will show if it has not received a push message for at least two sensor scans. Choose between:

HTTP PUSH DATA

- **Ignore and keep last status (default)**: The sensor remains in the status as defined by the last message that the sensor received.
  The probe on which this sensor runs must be connected to keep the last status. If the probe is disconnected, the sensor will show the **Unknown** status. If the probe is connected again, the sensor does not automatically return from **Unknown** to the last status before the probe disconnect.
- **Switch to "Unknown" status**: The sensor will show an **Unknown** status if it has not received any message for at least two sensor scans.
- **Switch to "Error" after x minutes**: The sensor will show a **Down** status if it has not received any message within a defined time span. Define the time threshold below.

Time Threshold (Minutes)

This field is only visible if you select the error option above. Enter a time threshold in minutes. If this time elapses, the sensor will show a **Down** status if it has not received a push message within this time span.

Please enter an integer value. The maximum threshold is **1440** minutes.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.
- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

SENSOR DISPLAY

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.

SCANNING INTERVAL

- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.
	Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:
	▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices** | **Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: Which HTTP status code leads to which HTTP sensor status?

- https://kb.paessler.com/en/topic/65731

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

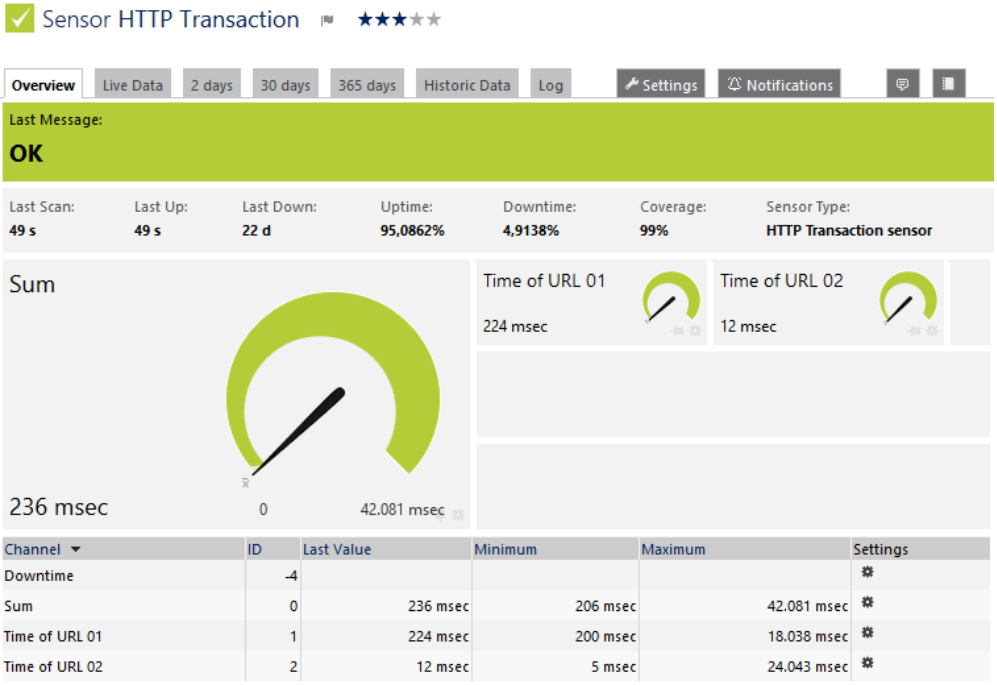
Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.55 HTTP Transaction Sensor

The HTTP Transaction sensor monitors an interactive website, such as a web shop, by performing a transaction using a set of Hypertext Transfer Protocol (HTTP) URLs. The sensor monitors whether logins or shopping carts work properly.

- It shows the loading time of single URLs and of the complete transaction.



HTTP Transaction Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/http_transaction.png

Remarks

- Supports Smart URL Replacement 974.
- Knowledge Base: Configuration Tips for HTTP Transaction Sensors
- Knowledge Base: Which user agent should I use in the HTTP Advanced sensor's settings?
- Knowledge Base: Which HTTP status code leads to which HTTP sensor status?
- This sensor type does not support Secure Remote Password (SRP) ciphers.
- If you need to use SRP ciphers, please choose the "compatibility mode" in the sensor settings below.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

HTTP SPECIFIC

Timeout (Sec.)	Enter a timeout in seconds for all HTTP requests. If the complete transaction takes longer than this value defines, the sensor cancels the request and shows an according error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).
Single URL Timeout (Sec.)	Enter a timeout in seconds for one single HTTP request. If the reply of any single request takes longer than this value defines, the sensor cancels the transaction and shows an according error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).

HTTP ENGINE

Monitoring Engine	If you encounter unexpected errors with the standard method that is used to monitor a URL, try to use the compatibility mode which is based on .NET. Choose between: ▪ **Default/High Performance (recommended)**: This is the default monitoring method for this sensor type. ▪ **Alternate/Compatibility Mode**: Try this method as an alternative for websites that do not work with the default approach. Using the compatibility mode, this sensor executes an external exe. Because of this, this method needs more resources, but it can be helpful in particular cases. ⓘ If you select the compatibility mode, the options for the SSL method will be slightly different. You can also check for trusted certificates. Please see below. ⚠ When using the Compatibility Mode, **Smart URL Replacement** will not work, so this sensor will not use the **IP Address/DNS value** of the parent device automatically then.

SSL SPECIFIC (WHEN USING COMPATIBILITY MODE)

SSL Method	When using the compatibility mode, the SSL specific settings are a bit different to the default (automatically used) SSL settings. You can choose between: ▪ **SSL V3** ▪ **TLS V1**

SSL SPECIFIC (WHEN USING COMPATIBILITY MODE)

	▪ **SSL V3 or TLS V1**: This is the default setting.
Check SSL Certificates	Specify if the sensor will check the certificate of the monitored URL. Choose between: ▪ **Do not check used certificates**: Do not consider the certificates of the monitored web pages. This the default setting. ▪ **Check if the used certificates are trusted**: Inspect the certificates. If the certificate of the server is not trusted, the sensor shows a **Down** status and displays a corresponding message.

This sensor type implicitly supports Server Name Identification (SNI), an extension to the TLS protocol.

ADVANCED SENSOR DATA

Limit Download (kb)	Enter a maximum amount of data that is transferred per every single request. If you set content checks below, please be aware that the sensor can only check the content downloaded within this limit for certain search expressions.
Cookie Management	Select if cookies are used for the transaction. Choose between: • **Use cookies (recommended)**: Allow cookies to be set and read during the transaction cycle. • **Ignore cookies**: Do not allow cookies. Use this option if you want to test the transaction without the use of cookies. We recommend that you use the default value.
User Agent	Choose which user agent string the sensor sends when connecting to the defined URLs. Choose between: ▪ **Use PRTG's Default String**: Do not enter a specific user agent, use the default setting. Usually, this is: Mozilla/5.0 (compatible; PRTG Network Monitor (www.paessler.com); Windows) ▪ **Use a Custom String**: Use a custom user agent. Define below.
Custom User Agent	This field is only visible if you enable the **Use a Custom String** option above. Enter a string that the sensor uses as user agent when connecting to the URL specified above.

ADVANCED SENSOR DATA

Result Handling	Define what PRTG will do with the web page loaded at the given URL. Choose between: • **Discard HTML result**: Do not store the requested web page. • **Store latest HTML result**: Store the last result of the requested web page to the **Logs (Sensors)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File name: Result of Sensor [ID].txt. This is for debugging purposes, especially in combination with content checks. The file will be overwritten with each scanning interval. For information on how to find the folder used for storage, see section **Data Storage** 3226.

AUTHENTICATION

Authentication	Define if the web page at the configured URL needs authentication. Choose between: ▪ **No authentication needed** ▪ **Web page needs authentication**
User	This field is only visible if you enable authentication above. Enter a username. Please enter a string.
Password	This field is only visible if you enable authentication above. Enter a password. Please enter a string.
Authentication Method	This field is only visible if enable authentication above. Select the authentication method the given URL is protected with. Choose between: ▪ **Basic access authentication (HTTP)**: Use simple HTTP authentication. This is the default setting and suitable for most cases. This authentication method transmits credentials as plain text. ▪ **Windows NT LAN Manager (NTLM)**: Use the Microsoft NTLM protocol for authentication. This is sometimes used in intranets for single sign-on.

AUTHENTICATION

- **Digest Access Authentication**: Use digest access authentication that applies a hash function to the password which is safer than basic access authentication.

We recommend that you use the default value.

TRANSACTION URL

You can define up to 10 different transaction URLs which will all be called in a row. Only if the complete transaction can be completed, the sensor will show an **Up** status 163. Using this mechanism you can set up an extended monitoring with multiple URLs. Please enter settings for at least one transaction URL. You can use as many steps as needed and disable the other steps.

Transaction Step #x

This setting is available for URL #2 through #10. Define if you want to use this step for your transaction check. Choose between:

- **Disable step #x**: Do not use this step. Choose this option if you do not need all 10 steps for your transaction check.
- **Enable step #x**: Enable this step. Further options will be viewed, as described below.

URL

Please enter the URL the sensor will connect to. It has to be URL encoded! If you enter an absolute URL, this address will be independent from the **IP address/DNS name** setting of the device this sensor is created on. PRTG uses a smart URL replacement which allows you to use the parent device's IP address/DNS name setting as part of the URL. For more information, please see section **Smart URL Replacement** below.

Request Method

The request method determines how the given URL is requested.

- **GET**: Request the website directly, like browsing the web. We recommend using this setting for a simple check of a web page.
- **POST**: Send post form data to the URL. If this setting is chosen, you must enter the data that will be sent in the **Postdata** field below.
- **HEAD**: Only request the HTTP header from the server; without the actual web page. Although this saves bandwidth since less data is transferred, it is not recommended because the measured request time is not the one experienced by your users and you might not be notified for slow results or timeouts.

TRANSACTION URL

Postdata	This field is only active when POST is selected in the **Request Method** setting above. Please enter the data part for the post request here. No XML is allowed here!
Check For Existing Key Words (Positive)	Define whether the result at the configured URL will be checked for keywords. Choose between: ▪ **Disable**: Do not search for keywords. ▪ **Enable key word check (positive)**: In the result returned at the URL, check if a key word exists. The content check is only intended for HTML websites and might not work with other target URLs.
Response Must Include	Define which string must be part of the web at the given URL. If the data does not include this string, the sensor will show an error status and display this string along with the affected URL in the sensor message. Please enter a string. Only simple text search is available here. The characters * and ? work here as placeholder, whereas * stands for no or any number of characters and ? stands for exactly one character (as known from Windows search). This behavior cannot be disabled, so the literal search for these characters is not possible.
Check For Existing Key Words (Negative)	Define whether the the result at the configured URL will be checked for keywords. Choose between: ▪ **Disable**: Do not search for keywords. ▪ **Enable key word check (negative)**: In the result returned at the URL, check if a key word does not exist. The content check is only intended for HTML websites and might not work with other target URLs.
Response Must Not Include	Define which string must not be part of the web at the given URL. If the data does include this string, the sensor will show an error status and display this string along with the affected URL in the sensor message. Please enter a string. Only simple text search is available here. The characters * and ? work here as placeholder, whereas * stands for no or any number of characters and ? stands for exactly one character (as known from Windows search). This behavior cannot be disabled, so the literal search for these characters is not possible.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

PROXY SETTINGS FOR HTTP SENSORS

HTTP Proxy Settings	The proxy settings determine how a sensor connects to a given URL. You can enter data for an HTTP proxy server that sensors will use when connecting via HTTP or HTTPS. This setting affects monitoring only and determines the behavior of HTTP sensors. To change proxy settings for the core server, please see **System Administration—Core & Probes** 2967.

PROXY SETTINGS FOR HTTP SENSORS

The SSL Certificate Sensor 2289 and the SSL Security Check Sensor 2299 do not support HTTP proxies, but you can configure connections via SOCKS proxies in their sensor settings.

Name	Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.
Port	Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.
User	If the proxy requires authentication, enter the username for the proxy login. Only basic authentication is available! Please enter a string or leave the field empty.
Password	If the proxy requires authentication, enter the password for the proxy login. Only basic authentication is available! Please enter a string or leave the field empty.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.

SCANNING INTERVAL

- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

Smart URL Replacement

Instead of entering a complete address in the URL field of an HTTP sensor, you can merely enter the protocol followed by colon and three slashes (that means you can enter either http:/// or https:/// or even a simple slash / as equivalent for http:///). PRTG will then fill in the parent device's **IP address** or **DNS name** in front of the third slash automatically. Whether this results in a valid URL or not, depends on the IP address or DNS name of the device where this HTTP sensor is created on. In combination with cloning devices, the smart URL replacement makes it easy to create many like devices.

For example, if you create a device with **DNS name** www.example.com and you put an HTTP sensor on it, you can provide values the following ways:

- Providing the value https:/// in the URL field, PRTG will automatically create the URL https://www.example.com/ from that.
- Using the value /help in the URL field, PRTG will automatically create and monitor the URL http://www.example.com/help
- It is also possible to provide a port number in the URL field which will be taken over by the device's DNS name and internally added, for example, http://:8080/

Smart URL replacement does not work for sensors running on the **Probe Device**.

More

Knowledge Base: Which HTTP status code leads to which HTTP sensor status?

- https://kb.paessler.com/en/topic/65731

Knowledge Base: Configuration Tips for HTTP Transaction Sensors needed

- https://kb.paessler.com/en/topic/443

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

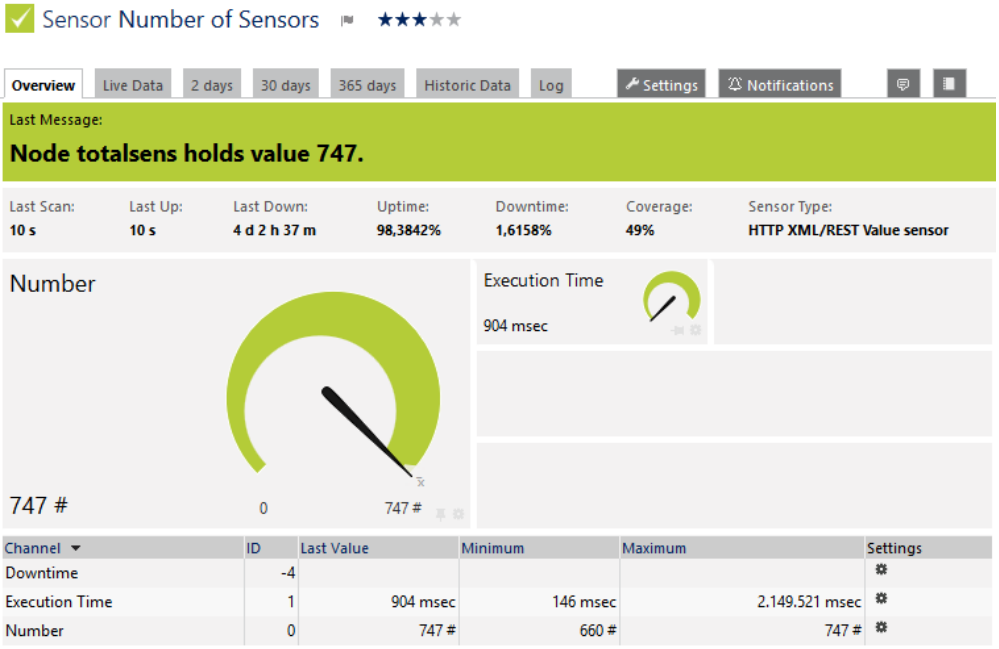
Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.56 HTTP XML/REST Value Sensor

The HTTP XML/REST Value sensor retrieves an XML file from a given URL and parses it.

- It can show the value of one defined XML node.



HTTP XML/REST Value Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/http_xmlrest_value.png

Remarks

- Requires 977 .NET 4.0 or higher on the probe system. If the sensor shows the error PE087, please additionally install .NET 3.5 on the probe system.
- This sensor can monitor only one single node in an XML file and shows the value in one channel. If you need to monitor more than one node of an XML document, please add the sensor for each target node anew.
- Supports Smart URL Replacement 988.
- We recommend Windows 2012 R2 on the probe system for best performance of this sensor.
- Knowledge Base: HTTP XML/REST Value Sensor: FAQ
- Knowledge Base: Which HTTP status code leads to which HTTP sensor status?
- This sensor type does not support Secure Remote Password (SRP) ciphers.
- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.

Requirement: .NET Framework

This sensor type requires the Microsoft .NET Framework to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the remote probe 3196. If the framework is missing, you cannot create this sensor.

Required .NET version (with latest updates): .NET 4.0 (Client Profile is sufficient), .NET 4.5, or .NET 4.6.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/60543

Limited to 50 Sensor Channels

PRTG does not support more than 50 sensor channels officially. Depending on the data used with this sensor type, you might exceed the maximum number of supported sensor channels. In this case, PRTG will try to display all sensor channels. However, please be aware that you will experience limited usability and performance.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SENSOR SETTINGS

Channel Name	Enter a name for the channel that will display the value at the given URL.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SETTINGS

URL	Enter the URL that returns the XML file. It has to be URL encoded! If you enter an absolute URL, the sensor uses this address independently from the **IP Address/DNS Name** setting of the device on which you create this sensor. PRTG uses a smart URL replacement that allows you to use the parent device's IP address/DNS name setting as part of the URL. For more information, please see section **Smart URL Replacement** 988 below.
XML Node (and optional property)	Enter the name of the node that this sensor checks, or enter a node name and a property name to check a property value. To obtain a value from nested tags, enter the tag names separated by a slash symbol, for example, use myTag/myTagInside as XML node value. ⓘ You can also check values in JavaScript Object Notation (JSON) notation. Please see **Checking JSON** 987 section below.

SENSOR SETTINGS

	You can try using XPath syntax here but it does not work in all cases and we do not provide any technical support for XPath issues. For further documentation about XPath, please see **More** 976 section below.
HTTP Username	If the URL requires authentication, enter the username. Please enter a string or leave the field empty.
HTTP Password	If the URL requires authentication, enter the password. Please enter a string or leave the field empty.
Sensor Value	Define what value this sensor shows. Choose between: ▪ **Use the value of the selected XML node**: Return the value that the sensor finds at the specified XML node. If this is non-numeric, the sensor shows 0. ▪ **Use the number of occurrences of the selected XML node or its children/siblings**: Return the number of occurrences found. Define further below.
Count XML Nodes	This setting is only visible if you enable the return number option above. Define which count the sensor shows. Choose between: ▪ **Occurrences of the selected XML node**: Return how often the defined XML node occurs at the defined URL. ▪ **Child nodes of the selected XML node**: Return the number of child nodes that exist below the node at the defined URL. ▪ **Sibling nodes of the selected XML node**: Return the number of sibling nodes that exist next to the node at the defined URL.
Namespaces	Define whether namespaces in the XML document are used or not. Choose between: ▪ **Use Namespaces**: Process the value you enter in the **XML Node (and optional property)** field including possibly existing namespace information. ▪ **Remove Namespaces**: Ignore namespace information in the XML document and process the value you enter in the **XML Node (and optional property)** field as node names only. For more information see **About Namespaces** 988 section below.
Content Type in Header	Define what to include in the header of the request sent to the URL defined above. Choose between: ▪ **Enable (recommended)**: This works for most web servers and is the recommended setting.

SENSOR SETTINGS

- **Disable**: Only very few web servers cannot handle this content type and need this setting. Try this if you get an error message with the enabled option.
- **Custom**: You can use a custom content type.

Custom Content Type

This field is only visible when you enable the **Custom** option above. Enter a custom content type like text/xml or text/html.

HTTP Headers

Optionally enter a list of custom HTTP headers with theirs respective values that you want to transmit to the URL you define above. The syntax of a list with header-value pairs is header1:value1|header2:value2|...|headerx:valuex

The sensor does not accept header field names that include a dash (-) character. If you want to use such an HTTP header, please leave out the dash of the name. For example, enter ContentType:value instead of Content-Type:value.

Example: From:johnqpublic@example.com|AcceptLanguage:en-us

Ensure that the HTTP header statement is valid! Otherwise, the sensor request will not be successful.

Characters to Remove

This field is only visible if you enable the **Use the value of the selected XML node** option above. Optionally enter a string that the sensor removes from the returned XML value. Use this to remove any unwanted characters from the result, for example, a thousands separator from numeric values. Please enter a string or leave the field empty.

Decimal Delimiter

This setting is only visible if you enable the **Use the value of the selected XML node** option above. If the sensor value of the selected XML node is of the type float, you can define any character here which is handled as the decimal delimiter. Enter one character or leave the field empty.

Custom Message

Optionally enter a custom sensor message. Use %1 as a placeholder to automatically fill in the returned XML value. Please enter a string or leave the field empty.

SSLv3 Connection

Define if you want to allow SSLv3 only for connections to the URL configured above. Choose between:

- **Use SSLv3 if available**
- **Force usage of SSLv3**

SENSOR SETTINGS

The force method does not work when the requested URL uses forward secrecy. For details, see this Knowledge Base article: My HTTP sensors could not create an SSL secure channel and are down. What can I do?

If Channel Value Changes

Define what this sensor will do when the sensor value changes. You can choose between:

- **Ignore changes (default)**: The sensor takes no action on change.
- **Trigger 'change' notification**: The sensor sends an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification 2791 whenever the sensor value changes.

The change notification for this sensor can only be triggered if the returned value is a numerical value. Strings are not supported by this option and cannot trigger a notification.

Unit String

Enter a string that the sensor will add to the retrieved values as a unit description. This is for display purposes only.

DEBUG OPTIONS

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result**: Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section **Data Storage** 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

Checking JSON

With the **XML Node (and optional property)** field you can also check values that are returned in JavaScript Object Notation (JSON) notation under the defined URL.

Example

A JSON notated section may look like the following:

```
{
  "test": "Hello World",
  "object": {
    "value": "content",
    "AnotherValue": "AnotherContent"
  },
  "arraytest": [
    "one",
    "two"
  ]
}
```

Depending on your entries in the **XML Node** field, the sensor will process the respective values:

Entry in Sensor's "XML Node" Field (from Example Above)	Processed Value (from Example Above)
test	Hello World
object/value	content
object/AnotherValue	AnotherContent
object	contentAnotherContent
arraytest[1]	one
arraytest[2]	two

The sensor converts whitespaces in JSON keys into underscores (_). So, for example, if you look for the node "some node" in the JSON, you need to enter "some_node" into the node field. If you count the number of nodes (for example, "some_node"), both "some node" and "some_node" would be counted if they appear in the JSON.

If a key exists more than once in the JSON, the value of the first appearance is returned (no difference between whitespace and underscore).

About Namespaces

In an XML document, tags may use namespaces.

Example

A namespace notated section may look like the following:

```
<myNamespace:myNode>
  some information
</myNamespace:myNode>
```

If you set this sensor to **Use Namespaces** (this is the default setting), it will expect the full node name, including the namespace information, in the **XML Node (and optional property)** field. In the example above, this would be myNamespace:myNode.

If your node names are unique even without the namespace information, you can simplify the settings by setting this sensor to **Remove Namespaces**. The sensor will then expect the node name only in the **XML Node (and optional property)** field. In the example above, this would be myNode.

Smart URL Replacement

Instead of entering a complete address in the URL field of an HTTP sensor, you can merely enter the protocol followed by colon and three slashes (that means you can enter either http:/// or https:/// or even a simple slash / as equivalent for http:///). PRTG will then fill in the parent device's **IP address** or **DNS name** in front of the third slash automatically. Whether this results in a valid URL or not, depends on the IP address or DNS name of the device where this HTTP sensor is created on. In combination with cloning devices, the smart URL replacement makes it easy to create many like devices.

For example, if you create a device with **DNS name** www.example.com and you put an HTTP sensor on it, you can provide values the following ways:

- Providing the value https:/// in the URL field, PRTG will automatically create the URL https://www.example.com/ from that.
- Using the value /help in the URL field, PRTG will automatically create and monitor the URL http://www.example.com/help

- It is also possible to provide a port number in the URL field which will be taken over by the device's DNS name and internally added, for example, http://:8080/

Smart URL replacement does not work for sensors running on the **Probe Device**.

More

Knowledge Base: Which HTTP status code leads to which HTTP sensor status?

- https://kb.paessler.com/en/topic/65731

Knowledge Base: Is there a tool available that can help me building queries for the XML/Rest Sensor?

- https://kb.paessler.com/en/topic/48783

Knowledge Base: How do I extract values from XML nodes (with nested tags) using PRTG's XML/Rest Value Sensor?

- https://kb.paessler.com/en/topic/43223

Knowledge Base: How can I use XPath with PRTG's XML/Rest Value Sensor?

- https://kb.paessler.com/en/topic/26393

Knowledge Base: HTTP XML/REST Value Sensor shows protocol violation. What can I do?

- https://kb.paessler.com/en/topic/26793

Knowledge Base: Why does my HTTP XML/REST Value Sensor return a 404 error?

- https://kb.paessler.com/en/topic/46503

Knowledge Base: My HTTP sensors could not create an SSL secure channel and are down. What can I do?

- https://kb.paessler.com/en/topic/61045

Knowledge Base: For which sensor types do you recommend Windows Server 2012 R2 and why?

- https://kb.paessler.com/en/topic/64331

Knowledge Base: Which .NET version does PRTG require?

- https://kb.paessler.com/en/topic/60543

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

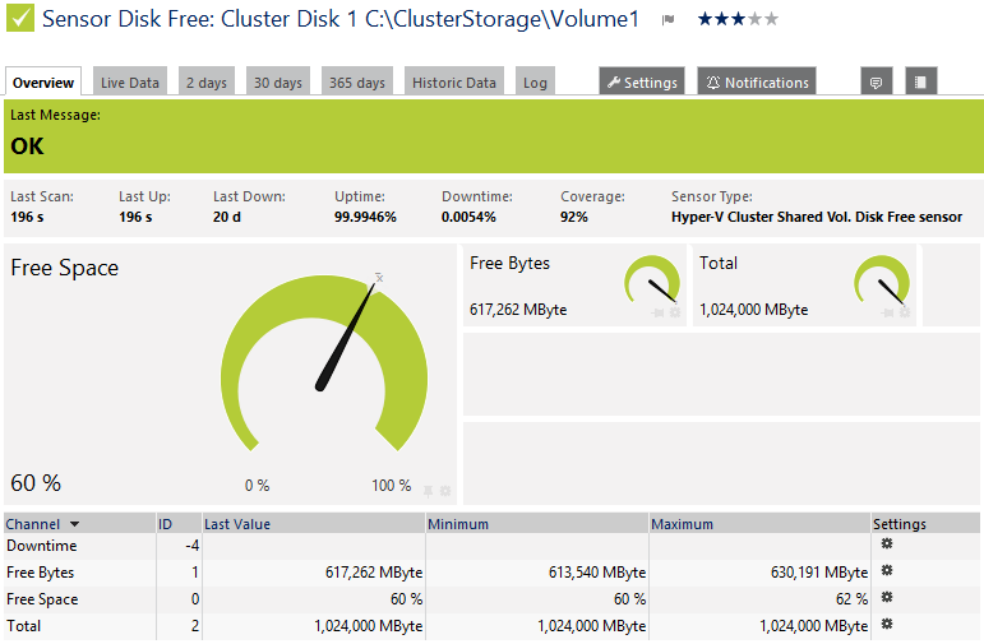
For more general information about settings, please see the **Object Settings** 188 section.

7.8.57 Hyper-V Cluster Shared Volume Disk Free Sensor

The Hyper-V Cluster Shared Volume Disk Free sensor monitors a Microsoft Hyper-V cluster shared volume via PowerShell.

It can show the following:

- Available disk space in percent
- Available disk space in bytes
- Total disk space



Hyper-V Cluster Shared Volume Disk Free Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/Hyper_V_Cluster_Shared_Volume_Disk_Free.png

Remarks

- Requires 992 Remote PowerShell on the target device.
- Requires 992 WSFC PowerShell Interface on the target device.
- Requires 992 .NET 4.0 or higher on the probe system.
- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- The parent device for this sensor must be a Windows server running Hyper-V.
- Knowledge Base: Why don't my Hyper-V sensors work after changing names?
- Knowledge Base: PowerShell Sensors: FAQ

- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Requirement: Remote PowerShell

The Hyper-V Cluster Shared Volume Disk Free sensor uses PowerShell commands. To monitor devices with this sensor **Remote PowerShell** has to be enabled.

In larger environments, the default memory limit for the remote shell might be insufficient and you might see the error message The WSMan provider host process did not return a proper response. In this case, increase the memory limit for Remote PowerShell. For detailed information, please see the Knowledge Base article How can I increase memory for Remote PowerShell?

Requirement: WSFC PowerShell Interface

This sensor type needs the **WSFC (Windows Server Failover Clustering) PowerShell Interface** to be installed on the target machine. You can list all modules in the PowerShell console with the command **Get-Module -ListAvailable**. Here **FailoverClusters** has to appear. Under Windows 2008 and 2012 the interface is part of the VMM Administrator Console, or the VMM 2012 Management Console.

The interface is available everywhere the WSFC feature is installed: Windows Server 2008 R2 (SP1) Full and Core (not installed by default); Microsoft Hyper-V Server 2008 R2 (SP1); Remote Server Administration Tools (RSAT) for Windows 7 (SP1).

Requirement: .NET Framework

This sensor type requires the Microsoft .NET Framework to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the remote probe 3196. If the framework is missing, you cannot create this sensor.

Required .NET version (with latest updates): .NET 4.0 (Client Profile is sufficient), .NET 4.5, or .NET 4.6.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/60543

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the disks you want to monitor. PRTG creates one sensor for each disk you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

DISK FREE SETTINGS

Disk	Select the disks you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items. Ensure the resource name of your disks do not contain unsupported characters, especially avoid the hash (#) sign. We recommend to not rename resource disk name once you have set up monitoring. For detailed information, please see the Knowledge Base article Why don't my Hyper-V sensors work after changing names?

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	Enter one or more **Tags**, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DISK FREE SETTINGS

Disk	Shows the name of the disk. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section **Data Storage**. You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: Why don't my Hyper-V sensors work after changing names?

- https://kb.paessler.com/en/topic/15533

Knowledge Base: How do I enable and use remote commands in Windows PowerShell?

- https://kb.paessler.com/en/topic/44453

Knowledge Base: My Powershell sensor returns an error message. What can I do?

- https://kb.paessler.com/en/topic/59473

Knowledge Base: "No Logon Servers Available" when Using PowerShell Sensors

- https://kb.paessler.com/en/topic/59745

Knowledge Base: How can I increase memory for Remote PowerShell?

- https://kb.paessler.com/en/topic/61922

Knowledge Base: Which .NET version does PRTG require?

- https://kb.paessler.com/en/topic/60543

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

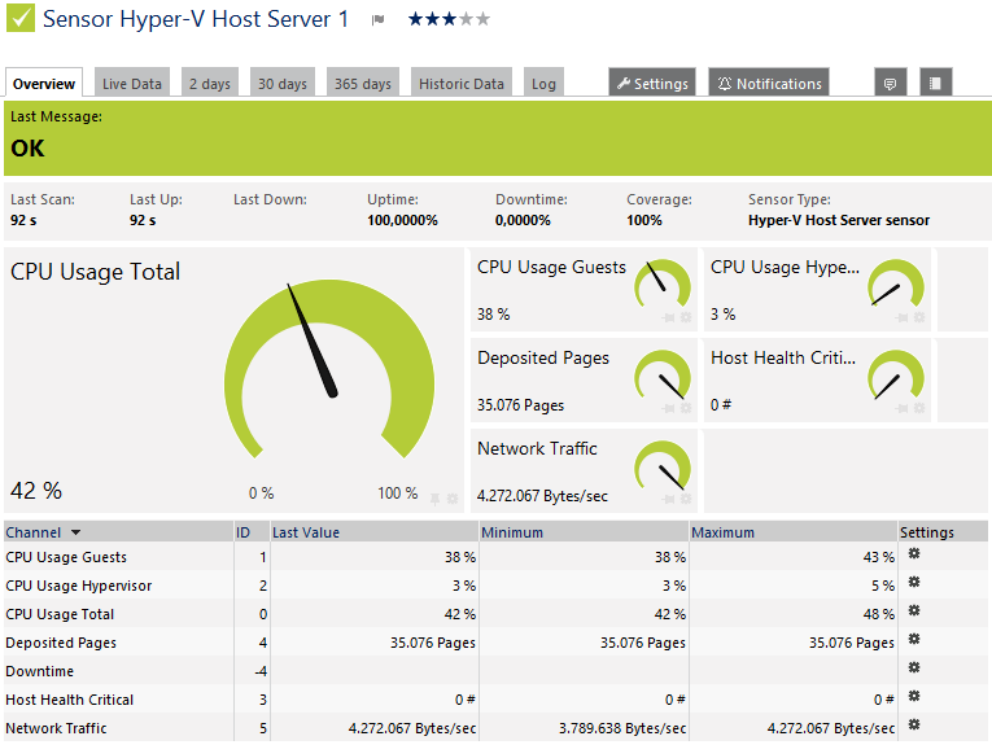
For more general information about settings, please see the **Object Settings** 188 section.

7.8.58 Hyper-V Host Server Sensor

The Hyper-V Host Server sensor monitors a Microsoft Hyper-V host server via Windows Management Instrumentation (WMI) or Windows Performance Counters, as configured in the "Windows Compatibility Options" of the parent device.

It can show the following:

- CPU usage in percent of guests, hypervisor, total
- Number of host health critical values
- Number of deposited pages
- Network traffic: Sums up the total bytes per second (received and sent) on all ports of your virtual switch.



Hyper-V Host Server Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/hyper_v_host_server.png

Remarks

- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- Requires Windows Server 2008 or later on the probe system.
- Requires the Remote Registry Windows service to be running on the target computer.

- Uses a hybrid approach 1002 with Windows Performance Counters and WMI as fallback to query data. Please stay below 200 WMI sensors per probe!
- The parent device for this sensor must be a Windows server running Hyper-V.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Requirement: Windows Credentials

Requires credentials for Windows systems to be defined for the device you want to use the sensor on. In the parent device's 365 **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. Otherwise, a connection via Performance Counters will not be possible. However, WMI connections may still work.

Hybrid Approach: Performance Counters and WMI

By default, this sensor type uses Windows Management Instrumentation (WMI) to request monitoring data. You can change the default behavior to a hybrid approach in the **Windows Compatibility Options** of the parent device's settings 372 on which you create this sensor: if you choose this option, the sensor will first try to query data via Windows Performance Counters and use WMI as a fallback if Performance Counters are not available. When running in fallback mode, the sensor will re-try to connect via Performance Counters after 24 hours.

Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per probe 111. Above this number, please consider using multiple **Remote Probes** 3196 for load balancing.

For a general introduction to the technology behind WMI, please see **Monitoring via WMI** 3092 section.

Requirement: Windows Version

In order for this sensor to work with Windows Performance Counters, please make sure a Windows version 2008 or later is installed on the computer running the PRTG probe: This is either on the local system (on every node, if on a cluster probe), or on the system running a remote probe 3196.

Requirement: Remote Registry Service

In order for this sensor to work with Windows Performance Counters, please make sure the Remote Registry Windows service is running on the target computer. If you fail to do so, a connection via Performance Counters will not be possible. However, WMI connections may still work.

To enable the service, please log in to the respective computer and open the services manager (for example, via services.msc). In the list, find the respective service and set its Start Type to Automatic.

Add Sensor

The **Add Sensor** dialog appears when you manually [288] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** [360] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree [151], as well as in alarms [190], logs [198], notifications [2829], reports [2862], maps [2885], libraries [2845], and tickets [200].
Parent Tags	Shows **Tags** [124] that this sensor inherits [124] from its parent device, group, and probe [118]. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** [124], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited [124] from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DEBUG OPTIONS

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result**: Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section Data Storage 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.
- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings 2782 settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. ⓘ Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

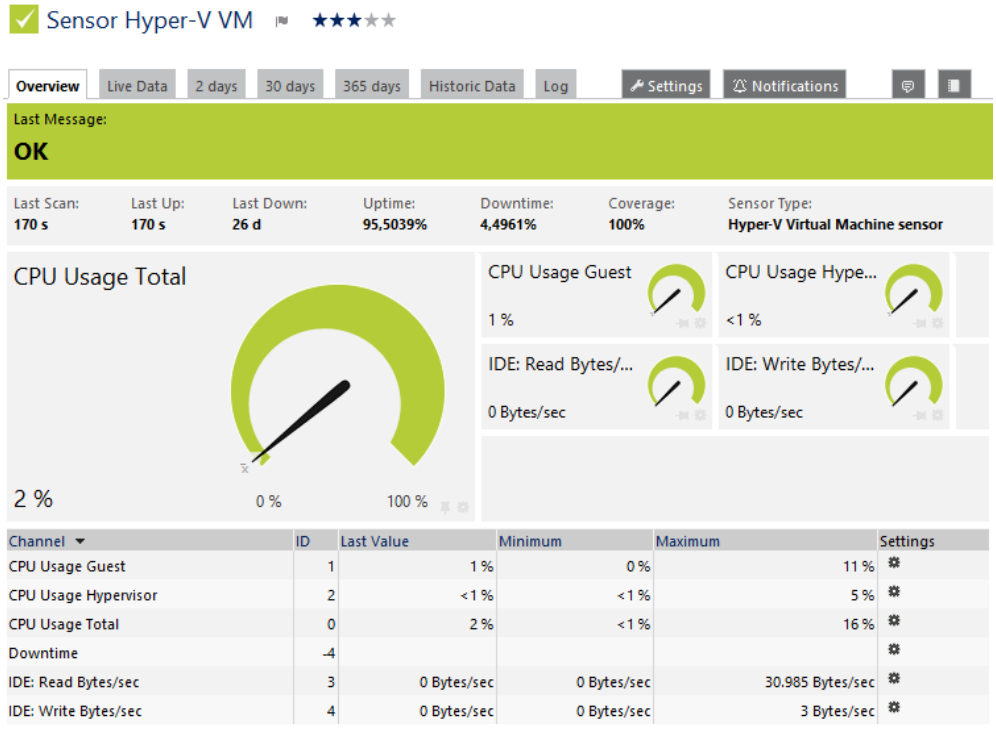
7.8.59 Hyper-V Virtual Machine Sensor

The Hyper-V Virtual Machine sensor monitors a virtual machine running on a Microsoft Hyper-V host server via Windows Management Instrumentation (WMI) or Windows Performance Counters, as configured in the "Windows Compatibility Options" of the parent device.

It can show the following:

- CPU usage in percent of guests, hypervisor, total
- IDE disk read speed (bytes per second)
- IDE disk write speed (bytes per second)

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Hyper-V Virtual Machine Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/hyper_v_virtual_machine.png

Remarks

- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- Requires Windows Server 2008 or later on the probe system.
- Requires the Remote Registry Windows service to be running on the target computer.

- Uses a hybrid approach 1010 with Windows Performance Counters and WMI as fallback to query data. Please stay below 200 WMI sensors per probe!
- The parent device for this sensor must be a Hyper-V server or a System Center Virtual Machine Manager (SCVMM).
- We recommend using System Center Virtual Machine Manager (SCVMM) as parent device, because this way PRTG will continue to monitor your virtual machines also when they change the physical host using Live Migration.
- To monitor a virtual machine with this sensor, disable User Account Control (UAC) in the control panel of the Windows operating system which is running on this virtual machine. Otherwise, the sensor might switch into a **Down** status with the error message "The virtual machine is not running or is powered off".
- Knowledge Base: Why don't my Hyper-V sensors work after changing names?

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Requirement: Windows Credentials

Requires credentials for Windows systems to be defined for the device you want to use the sensor on. In the parent device's 365 **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. Otherwise, a connection via Performance Counters will not be possible. However, WMI connections may still work.

Hybrid Approach: Performance Counters and WMI

By default, this sensor type uses Windows Management Instrumentation (WMI) to request monitoring data. You can change the default behavior to a hybrid approach in the **Windows Compatibility Options** of the parent device's settings 372 on which you create this sensor: if you choose this option, the sensor will first try to query data via Windows Performance Counters and use WMI as a fallback if Performance Counters are not available. When running in fallback mode, the sensor will re-try to connect via Performance Counters after 24 hours.

Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per probe 111. Above this number, please consider using multiple **Remote Probes** 3196 for load balancing.

For a general introduction to the technology behind WMI, please see **Monitoring via WMI** 3092 section.

Requirement: Windows Version

In order for this sensor to work with Windows Performance Counters, please make sure a Windows version 2008 or later is installed on the computer running the PRTG probe: This is either on the local system (on every node, if on a cluster probe), or on the system running a remote probe 3196.

Requirement: Remote Registry Service

In order for this sensor to work with Windows Performance Counters, please make sure the Remote Registry Windows service is running on the target computer. If you fail to do so, a connection via Performance Counters will not be possible. However, WMI connections may still work.

To enable the service, please log in to the respective computer and open the services manager (for example, via services.msc). In the list, find the respective service and set its Start Type to Automatic.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the virtual machines you want to monitor. PRTG creates one sensor for each VM you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

VIRTUAL MACHINE SETTINGS

Virtual Machine	Select the virtual machines (VMs) you want to add a sensor for, including the ones that are not running. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items. Ensure the name of your VMs do not contain unsupported characters, especially avoid the hash (#) sign. We recommend to not rename virtual machines once you have set up monitoring. For detailed information, please see the Knowledge Base article Why don't my Hyper-V sensors work after changing names?

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

VIRTUAL MACHINE SETTINGS

GUID	Shows the Globally Unique Identifier (GUID) of the virtual machine that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

VIRTUAL MACHINE SETTINGS

Name	Shows the name of the virtual machine that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Description	Shows information about the virtual machine. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Powered Off VMs	Define how to react to a virtual machine that is powered off. Choose between: • **Alarm when powered off**: The sensor will change to a **Down** 163 status if the virtual machine is powered off. Note: While in Down status, a sensor does not record any data in any of its channels. • **Ignore powered off state**: The sensor will not change to a **Down** status if the virtual machine is powered off. It will report zero values instead.
Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section **Data Storage** 3226. You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: Why don't my Hyper-V sensors work after changing names?

- https://kb.paessler.com/en/topic/15533

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.60 Hyper-V Virtual Network Adapter Sensor

The Hyper-V Network Adapter sensor monitors virtual network adapters running on a Microsoft Hyper-V host server via Windows Management Instrumentation (WMI) or Windows Performance Counters, as configured in the "Windows Compatibility Options" of the parent device.

It can show the following:

- Sent, received, and totally transferred bytes
- Sent and received packets per second
- Sent and received broadcast packets per second
- Sent and received directed packets per second
- Sent and received multicast packets per second

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

Channel	ID	Last Value	Minimum	Maximum	Settings
Broadcast Packets Received	0	21 /sec	21 /sec	21 /sec	
Broadcast Packets Sent	1	0,02 /sec	0,02 /sec	0,02 /sec	
Bytes	4	2 KByte	2 KByte	2 KByte	
Bytes Received	2	2 KByte	2 KByte	2 KByte	
Bytes Sent	3	< 0,01 KByte	< 0,01 KByte	< 0,01 KByte	
Directed Packets Received	5	0,03 /sec	0,03 /sec	0,03 /sec	
Directed Packets Sent	6	0,03 /sec	0,03 /sec	0,03 /sec	
Downtime	-4				
Multicast Packets Received	7	5 /sec	5 /sec	5 /sec	
Multicast Packets Sent	8	0 /sec	0 /sec	0 /sec	
Packets	11	26 /sec	26 /sec	26 /sec	
Packets Received	9	26 /sec	26 /sec	26 /sec	
Packets Sent	10	0,05 /sec	0,05 /sec	0,05 /sec	

Hyper-V Virtual Network Adapter Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/hyper_v_virtual_network_adapter.png

Remarks

- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- Requires 1022 Windows Server 2008 or later on the probe system.
- Requires 1022 the Remote Registry Windows service to be running on the target computer.
- Uses a hybrid approach 1022 with Windows Performance Counters and WMI as fallback to query data. Please stay below 200 WMI sensors per probe!
- The parent device for this sensor must be a Hyper-V server.
- Knowledge Base: Why don't my Hyper-V sensors work after changing names?

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Requirement: Windows Credentials

Requires credentials for Windows systems to be defined for the device you want to use the sensor on. In the parent device's 365 **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. Otherwise, a connection via Performance Counters will not be possible. However, WMI connections may still work.

Hybrid Approach: Performance Counters and WMI

By default, this sensor type uses Windows Management Instrumentation (WMI) to request monitoring data. You can change the default behavior to a hybrid approach in the **Windows Compatibility Options** of the parent device's settings 372 on which you create this sensor: if you choose this option, the sensor will first try to query data via Windows Performance Counters and use WMI as a fallback if Performance Counters are not available. When running in fallback mode, the sensor will re-try to connect via Performance Counters after 24 hours.

Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per probe 111. Above this number, please consider using multiple **Remote Probes** 3196 for load balancing.

For a general introduction to the technology behind WMI, please see **Monitoring via WMI** 3092 section.

Requirement: Windows Version

In order for this sensor to work with Windows Performance Counters, please make sure a Windows version 2008 or later is installed on the computer running the PRTG probe: This is either on the local system (on every node, if on a cluster probe), or on the system running a remote probe 3196.

Requirement: Remote Registry Service

In order for this sensor to work with Windows Performance Counters, please make sure the Remote Registry Windows service is running on the target computer. If you fail to do so, a connection via Performance Counters will not be possible. However, WMI connections may still work.

To enable the service, please log in to the respective computer and open the services manager (for example, via services.msc). In the list, find the respective service and set its Start Type to Automatic.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the network adapters you want to monitor. PRTG creates one sensor for each adapter you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

VIRTUAL MACHINE SETTINGS

Hyper-V Virtual Network Adapter	Select the virtual network adapters you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items. We recommend you do not rename virtual machines once you have set up monitoring. Renaming them will also change the internal virtual network adapter names, so monitoring might be interrupted. For detailed information about virtual machine naming, please see the Knowledge Base article Why don't my Hyper-V sensors work after changing names?

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

HYPER-V VIRTUAL NETWORK ADAPTER SETTINGS

Virtual Network Adapter	Shows the name of the virtual network adapter monitored by this sensor. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section **Data Storage** 3226.

HYPER-V VIRTUAL NETWORK ADAPTER SETTINGS

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply. If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply. If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: Why don't my Hyper-V Virtual Machine sensors work after changing names?

- https://kb.paessler.com/en/topic/15533

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

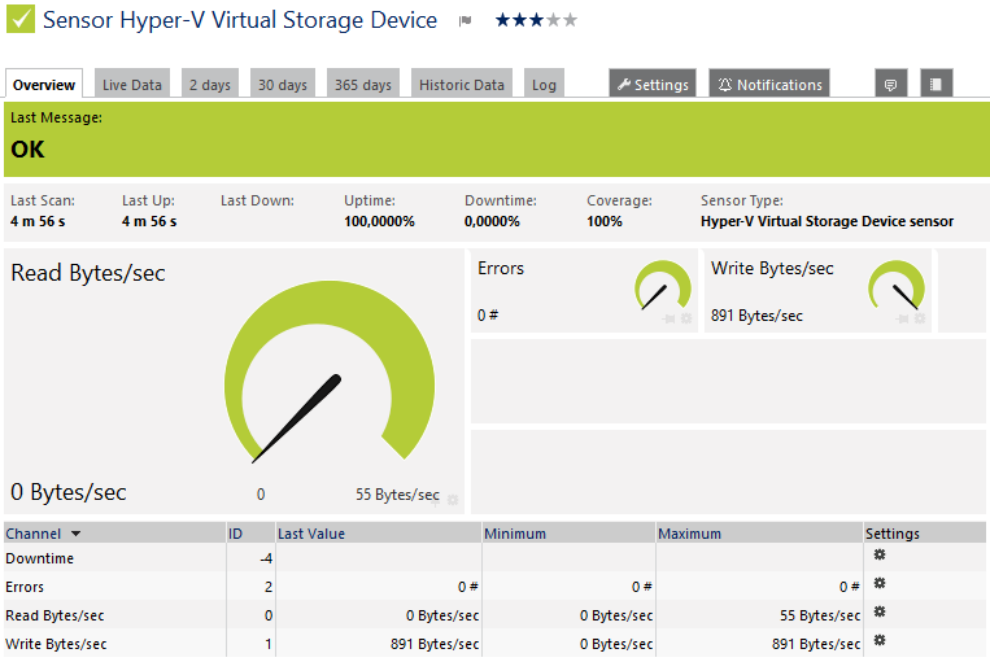
7.8.61 Hyper-V Virtual Storage Device Sensor

The Hyper-V Virtual Storage sensor monitors a virtual storage device running on a Microsoft Hyper-V host server via Windows Management Instrumentation (WMI) or Windows Performance Counters, as configured in the "Windows Compatibility Options" of the parent device.

It can show the following:

- Read speed in bytes per second
- Write speed in bytes per second
- Number of errors

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Hyper-V Virtual Storage Device Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/hyper_v_virtual_storage_device.png

Remarks

- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- Requires 1032 Windows Server 2008 or later on the probe system.
- Requires 1032 the Remote Registry Windows service to be running on the target computer.
- Uses a hybrid approach 1032 with Windows Performance Counters and WMI as fallback to query data. Please stay below 200 WMI sensors per probe!
- The parent device for this sensor must be a Hyper-V server.

- This sensor does not support Live Migration.
- Knowledge Base: Why don't my Hyper-V sensors work after changing names?

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Requirement: Windows Credentials

Requires credentials for Windows systems to be defined for the device you want to use the sensor on. In the parent device's 365 **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. Otherwise, a connection via Performance Counters will not be possible. However, WMI connections may still work.

Hybrid Approach: Performance Counters and WMI

By default, this sensor type uses Windows Management Instrumentation (WMI) to request monitoring data. You can change the default behavior to a hybrid approach in the **Windows Compatibility Options** of the parent device's settings 372 on which you create this sensor: if you choose this option, the sensor will first try to query data via Windows Performance Counters and use WMI as a fallback if Performance Counters are not available. When running in fallback mode, the sensor will re-try to connect via Performance Counters after 24 hours.

Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per probe 111. Above this number, please consider using multiple **Remote Probes** 3196 for load balancing.

For a general introduction to the technology behind WMI, please see **Monitoring via WMI** 3092 section.

Requirement: Windows Version

In order for this sensor to work with Windows Performance Counters, please make sure a Windows version 2008 or later is installed on the computer running the PRTG probe: This is either on the local system (on every node, if on a cluster probe), or on the system running a remote probe 3196.

Requirement: Remote Registry Service

In order for this sensor to work with Windows Performance Counters, please make sure the Remote Registry Windows service is running on the target computer. If you fail to do so, a connection via Performance Counters will not be possible. However, WMI connections may still work.

To enable the service, please log in to the respective computer and open the services manager (for example, via services.msc). In the list, find the respective service and set its Start Type to Automatic.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the storage devices you want to monitor. PRTG creates one sensor for each storage you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

HYPER-V VIRTUAL STORAGE DEVICE SETTINGS

Virtual Storage Device	Select the virtual storage devices you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.

BASIC SENSOR SETTINGS

Parent Tags	Shows **Tags** [124] that this sensor inherits [124] from its parent device, group, and probe [118]. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** [124], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited [124] from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

HYPER-V VIRTUAL STORAGE DEVICE SETTINGS

Virtual Storage Device	Shows the unique identifier of the device that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section **Data Storage** [3226]. You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

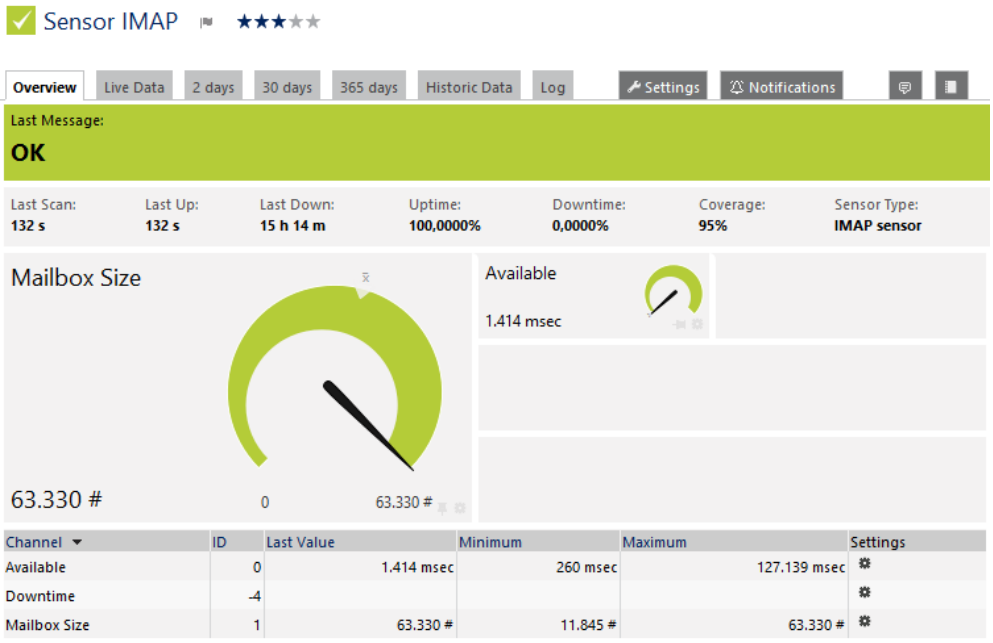
For more general information about settings, please see the **Object Settings** 188 section.

7.8.62 IMAP Sensor

The IMAP sensor monitors an email server using Internet Message Access Protocol (IMAP).

It can show the following:

- Response time of the email server
- Number of emails in the defined mailbox
- It can also check the content of emails for certain key words. This way, you can use this sensor to monitor backup solutions via emails that are sent out by these solutions. For more information, see the Knowledge Base article How can I monitor my backup software to be sure backup succeeded last night?



IMAP Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/imap.png

Remarks

- If you use content checks, we recommend using a dedicated IMAP account that is only checked by PRTG. Editing existing mails in the mailbox of the monitored IMAP account can lead to false alarms or malfunctions of this sensor type.
- This sensor type might not work properly when monitoring subfolders of mailboxes. If it has to check subsequent emails with identical subjects, later on incoming emails might not be recognized.
- This sensor type does not support Secure Remote Password (SRP) ciphers.
- Knowledge Base: My IMAP sensor does not process HTML emails correctly using regex. What can I do?

- Knowledge Base: How can I monitor my backup software to be sure backup succeeded last night?
- Knowledge Base: Can I analyze multipart emails using the PRTG IMAP sensor?
- Knowledge Base: My IMAP sensor does not find emails when I check for message date. What can I do?

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

CONNECTIVITY

Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).
Port	Enter the number of the port that the sensor uses to connect via IMAP. For non-secure connections, usually port 143 is used. For SSL connections it is usually port 993. The actual setting depends on the server you are connecting to. Please enter an integer value. We recommend that you use the default value. If you do not get a connection, please try another port number.
Security	Define the security level for the sensor connection. Choose between: ▪ **Use Transport-Level Security if available using StartTLS (default)**: Choose this option to try to connect to the server using TLS and StartTLS. If the server does not support this, the sensor will try to connect without encryption. ▪ **Use Transport-Level Security if available**: Choose this option to try to connect to the server using TLS. If the server does not support this, the sensor will try to connect without encryption. ▪ **Enforce Transport-Level Security using StartTLS**: Choose this option to try connecting to the server using TLS and StartTLS. If the server does not support this, the sensor will show a **Down** status 163. ▪ **Enforce Transport-Level Security**: Choose this option to try to connect to the server using TLS. If the server does not support this, the sensor will show a **Down** status 163. If the sensor connects to a server via StartTLS, the connection is established unencrypted first. After the connection is established, the sensor sends a certain command (StartTLS) over the unencrypted connection to negotiate a secure connection via the SSL/TLS protocol. If the sensor uses TLS without StartTLS, the negotiation of a secure connection happens immediately (implicitly) so that no commands are sent in unencrypted plain text. If there is no secure connection possible, no communication will take place.

AUTHENTICATION

Username	Enter a username for IMAP authentication. Please enter a string.
Password	Enter a password for IMAP authentication. Please enter a string.
Mailbox Name	Enter the name of the mailbox (for example, the name of the IMAP folder) that the sensor will check. Default value is **Inbox**. Unless you set a last message date check below, the sensor will always look at all emails contained in the mailbox. Ensure you do not manually edit emails in this mailbox with another email client because this can result in malfunctions of this sensor's email identification.

SENSOR BEHAVIOR

General Behavior	This sensor can additionally check the content of all incoming emails. Choose between: ▪ **Check connectivity only, do not process emails (default)**: Only check availability of the IMAP server and check if a login is successful. Do not process any emails in the IMAP email account. ▪ **Count emails in this mailbox**: Count the emails in the defined mailbox. ▪ **Process emails in this mailbox**: Log in to the IMAP email account and check the emails which it contains. Define further options below.
Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section Data Storage 3226. You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

FILTER EMAILS IN INBOX

This settings section is only visible if you choose to process the emails in the mailbox.

Only Include Emails with Matching "From"	Define if you want to check the "From" field of the emails. Choose between: ▪ **Do not check (default)**: Do not process this field in emails. ▪ **Check using string search**: Process this field in emails using simple string search. ▪ **Check using regular expression**: Process this field in emails using a regular expression. For more information about syntax, please see the **Regular Expressions** 3193 section. When using a search, the sensor will scan all emails from the newest to the oldest. The sensor finishes the scan with the first match! This means that after it has found a match in one email, the sensor will not perform any further checks in older emails.
Search for	This field is only visible if you enable a "from" check above. Enter a search string using the method defined above.
Only Include Emails with Matching "Subject"	Define if you want to check the "Subject" field of the emails. Choose between: ▪ **Do not check (default)**: Do not process the subject of emails. ▪ **Check using string search**: Process the subject of emails using simple string search. ▪ **Check using regular expression**: Process the subject of emails using a regular expression. For more information about syntax, please see the **Regular Expressions** 3193 section. When using a search, the sensor will scan all emails from the newest to the oldest. The sensor finishes the scan with the first match! This means that after it has found a match in one email, the sensor will not perform any further checks in older emails.
Search for	This field is only visible if you enable a "subject" check above. Enter a search string using the method defined above.
Only Include Emails with Matching Email Body	Define if you want to check the email body of the emails. Choose between: ▪ **Do not check (default)**: Do not process the email body.

FILTER EMAILS IN INBOX

	▪ **Check using string search**: Process the email body using simple string search. ▪ **Check using regular expression**: Process the email body using a regular expression. For more information about syntax, please see the **Regular Expressions** 3193 section. When using a search, the sensor will scan all emails from the newest to the oldest. The sensor finishes the scan with the first match! This means that after it has found a match in one email, the sensor will not perform any further checks in older emails.
Search for	This field is only visible if you enable checking the email body above. Enter a search string using the method defined above.
Only Include Recent Emails	Define if you want to check all emails in the mailbox, or only mails that were received within the last few hours. Choose between: ▪ **Do not check message age (default)**: Always check all emails that the mailbox contains. ▪ **Emails must be younger than**: Only check emails that were received in the last few hours. Define below.
Maximum Age in Hours	This field is only visible if you enable the message age check above. Enter the maximum age in hours. The sensor will only process emails that are younger. Please enter an integer value.
If No Email Matches the Above Filters	Define which status 163 the sensor will show if it does not find any email in the mailbox that matches the defined filters. Choose between: ▪ **Set sensor to "Up" status (default)** ▪ **Set sensor to "Warning" status** ▪ **Set sensor to "Down" status**
Message	This field is only visible if you define a **Warning** or **Down** status as no matching behavior above. Define the message that the sensor will show if it did not find any matching emails together with a **Warning** or **Down** status as you define above.

VALIDATE LATEST EMAIL

This settings section is only visible if you choose to process the emails in the mailbox.

The sensor will only validate the latest email that matches the filters above! If the sensor does not find a matching email, it will not perform any email validation.

For the Latest Email that Matches, Set Sensor to "Warning" Status	Define in which cases the sensor will show a **Warning** status 163. Choose between: ▪ **Never (default)**: Never set this sensor to a **Warning** status based on email content. ▪ **Always**: Always set this sensor to a **Warning** status in case any emails could be identified. ▪ **If subject contains**: Set the sensor to **Warning** if the subject of the found email contains the search text you define below. ▪ **If subject does not contain**: Set the sensor to **Warning** if the subject of the found email does not contain the search text you define below. ▪ **If email body contains**: Set the sensor to **Warning** if the body of the found email contains the search text you define below. ▪ **If email body does not contain**: Set the sensor to **Warning** if the body of the found email does not contain the search text you define below.
Check Method	This setting is only visible if you select an if condition above. Define how you want to check for the above condition. Choose between: ▪ **String search**: Check the email subject or body using simple string search. ▪ **Regular expression**: Check the email subject or body using a regular expression. For more information about syntax, please see **Regular Expressions** 3193 section.
Search Text	This setting is only visible if you select an if condition above. Enter a search string using the method defined above.
Warning Message	This setting is only visible if you select a warning condition above. Define the message that the sensor will show for a **Warning** status 163.
Based on Message Age, Set Sensor to "Warning" Status	Define if you want to check the age of the latest matching email in the mailbox. Choose between: ▪ **Never (default)**: Do not check the age of the email.

VALIDATE LATEST EMAIL

	▪ **If email is older than**: Set the sensor to **Warning** status if the found email is older than you define below.
Message Age in Hours	This field is only visible if you enable the message age check above. Enter the maximum age in hours. If the processed email is older, the sensor will show a **Warning** status. Please enter an integer value. Ensure you do not manually edit emails in this mailbox with another email client because this can result in malfunctions of the message age check.
For the Latest Email that Matches, Set Sensor to "Down" Status	Define in which cases the sensor will show a **Down** status 163. Choose between: ▪ **Never (default)**: Never set this sensor to a **Down** status based on email content. ▪ **Always**: Always set this sensor to a **Down** status in case any emails could be identified. ▪ **If subject contains**: Set the sensor to **Down** if the subject of the found email contains the search text you define below. ▪ **If subject does not contain**: Set the sensor to **Down** if the subject of the found email does not contain the search text you define below. ▪ **If email body contains**: Set the sensor to **Down** if the body of the found email contains the search text you define below. ▪ **If email body does not contain**: Set the sensor to **Down** if the body of the found email does not contain the search text you define below.
Check Method	This setting is only visible if you select an if condition above. Define how you want to check for the above condition. Choose between: ▪ **String search**: Check the email subject or body using simple string search. ▪ **Regular expression**: Check the email subject or body using a regular expression. For more information about syntax, please see **Regular Expressions** 3193 section.
Search Text	This setting is only visible if you enable an if condition above. Enter a search string using the method defined above.

VALIDATE LATEST EMAIL

Error Message	This setting is only visible if you select a down condition above. Define the message that the sensor will show for a **Down** status 163.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply. If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply. If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: How can I monitor my backup software to be sure backup succeeded last night?

- https://kb.paessler.com/en/topic/47023

Knowledge Base: My IMAP sensor does not process HTML emails correctly using regex. What can I do?

- https://kb.paessler.com/en/topic/61019

Knowledge Base: Can I analyze multipart emails using the PRTG IMAP sensor?

- https://kb.paessler.com/en/topic/63532

Knowledge Base: My IMAP sensor does not find emails when I check for message date. What can I do?

- https://kb.paessler.com/en/topic/69811

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

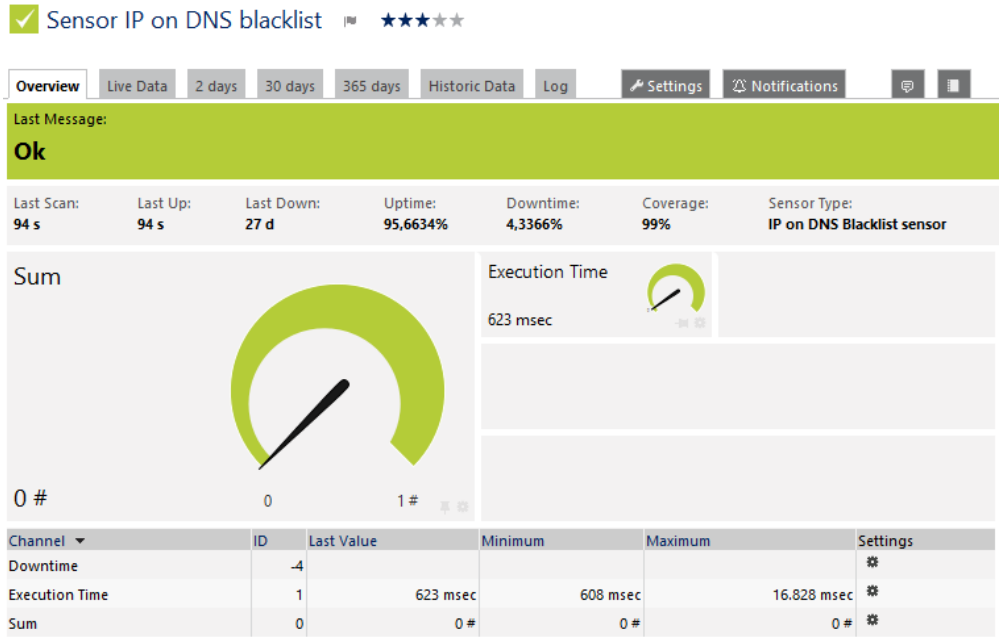
Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.63 IP on DNS Blacklist Sensor

The IP on DNS Blacklist sensor checks if the IP address of its parent device is listed on specific blacklist servers.

- The sensor shows the number of blacklist hits it can find.



IP on DNS Blacklist Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/ip_on_dns_blacklist.png

Remarks

- If a DNS name is used as hostname of the parent device, PRTG will resolve it to an IP address before querying blacklist servers.
- During normal operation, there should be 0 hits and the sensor should show a green **Up** status 163. If the sensor can find the IP address on at least one of the blacklist servers, it will show a yellow **Warning** status by default. You can set additional thresholds in the Sensor Channels Settings 2782.
- Requires 1055 .NET 4.0 or higher on the probe system. If the sensor shows the error PE087, please additionally install .NET 3.5 on the probe system.
- We recommend Windows 2012 R2 on the probe system for best performance of this sensor.
- Knowledge Base: Is there a list of anti spam black list servers?
- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.

Requirement: .NET Framework

This sensor type requires the Microsoft .NET Framework to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the remote probe 3196. If the framework is missing, you cannot create this sensor.

Required .NET version (with latest updates): .NET 4.0 (Client Profile is sufficient), .NET 4.5, or .NET 4.6.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/60543

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

BASIC SENSOR SETTINGS

	You can add additional tags to the sensor if you like. Other tags are automatically inherited[124] from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SETTINGS

Blacklist Servers	Define the blacklist servers that the sensor uses for the check. You can enter a comma separated list. Default is bl.spamcop.net. For a list of servers, please see this Knowledge Base article: Is there a list of anti spam black list servers? With each scanning interval, PRTG will query all servers in the list! We recommend you do not enter more than 10 servers to make sure the check can be completed within the scanning interval of this sensor. If you use too many blacklist servers, the sensor will show the error message Timeout (code: PE018).

DEBUG OPTIONS

Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section **Data Storage**[3226].

DEBUG OPTIONS

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply. If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply. If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: Is there a list of anti spam black list servers?

- https://kb.paessler.com/en/topic/37633

Knowledge Base: For which sensor types do you recommend Windows Server 2012 R2 and why?

- https://kb.paessler.com/en/topic/64331

Knowledge Base: Which .NET version does PRTG require?

- https://kb.paessler.com/en/topic/60543

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

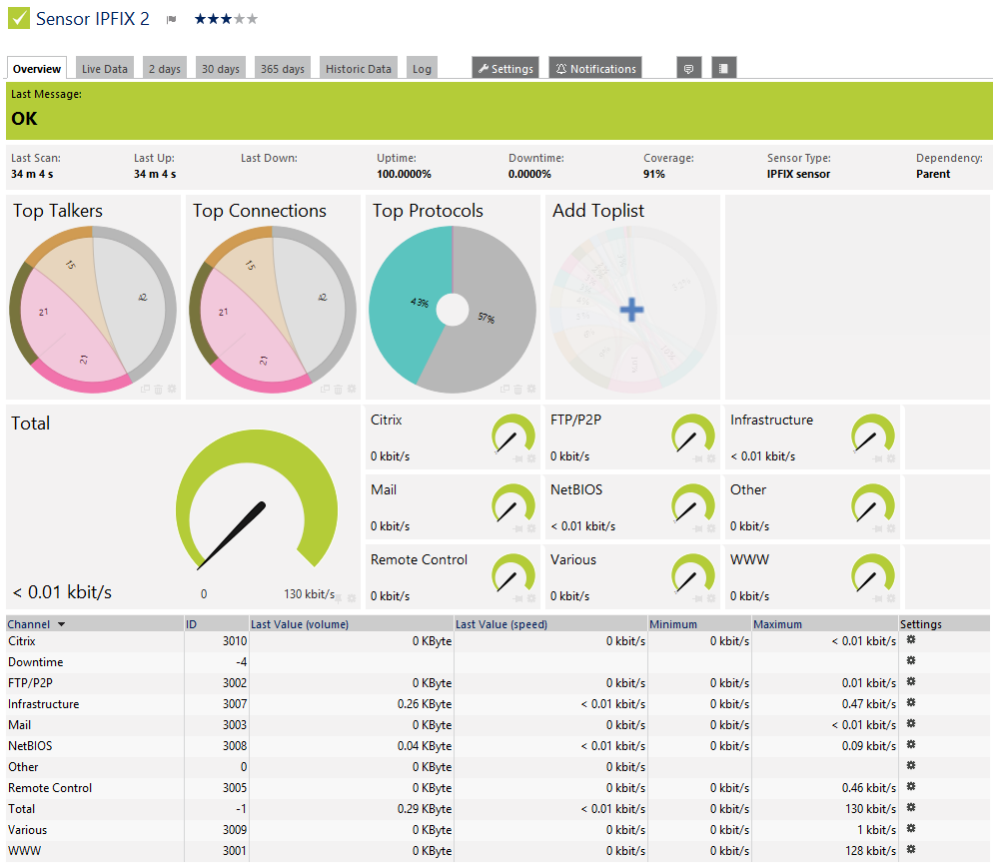
7.8.64 IPFIX Sensor

The IPFIX sensor receives traffic data from an IPFIX (Internet Protocol Flow Information Export) compatible device and shows traffic by type. There are several filter options available to divide traffic into different channels. Ensure your device supports IPFIX when using this sensor.

This sensor can show the following traffic types in kbit per second:

- Chat (IRC, AIM)
- Citrix
- FTP/P2P (file transfer)
- Infrastructure (network services: DHCP, DNS, Ident, ICMP, SNMP)
- Mail (mail traffic: IMAP, POP3, SMTP)
- NetBIOS
- Remote control (RDP, SSH, Telnet, VNC)
- WWW (web traffic: HTTP, HTTPS)
- Total traffic
- Other protocols (other UDP and TCP traffic)

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



IPFIX Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/ipfix.png

Remarks

- You have to enable IPFIX export on the device for this sensor to work. The device must send the flow data stream to the IP address of the PRTG probe system on which the sensor is set up (either a local or remote probe).
- This sensor type cannot be used in cluster mode. You can set it up on a local probe or remote probe only, not on a cluster probe.
- Knowledge Base: How can I change the default groups and channels for xFlow and Packet Sniffer sensors?
- Knowledge Base: What is the Active Flow Timeout in Flow sensors?
- For a general introduction to the technology behind flow monitoring, please see manual section **Monitoring Bandwidth via Flows** 3099.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

IPFIX SPECIFIC SETTINGS

Receive IPFIX Packets on UDP Port	Enter the UDP port number on which the flow packets are received. It must match the one you have configured in the IPFIX export options of your hardware router device. Please enter an integer value.
Sender IP	Enter the IP address of the sending device you want to receive the IPFIX data from. Enter an IP address to receive data from a specific device only, or leave the field empty to receive data from any device on the specified port.
Receive IPFIX Packets on IP	Select the IP address(es) on which PRTG listens to IPFIX packets. The list of IP addresses shown here is specific to your setup. To select an IP address, add a check mark in front of the respective line or in the top level box to select all. The IP address selected here must match the one configured in the IPFIX export options of your hardware router device.
Active Flow Timeout (Minutes)	Enter a time span in minutes after which new flow data must be received. If the timeout is reached and no new data is received, the sensor may switch to an **Unknown** status. Please enter an integer value. We recommend you set this one minute longer than the respective timeout configured in your hardware router device. For more details about this setting, please see this Knowledge Base article: What is the Active Flow Timeout in Flow sensors? If you set this value too low, flow information might be lost!
Sampling Mode	Define if you want to use the sampling mode. This setting must accord to the setting in the flow exporter. Choose between: ▪ **Off**: The standard flow will be used. ▪ **On**: Switch into sampling mode and specify the sampling rate below.
Sampling Rate	This field is only visible when sampling mode is **On** above. Enter a number that matches the sampling rate in your exporter device. If the number is different, monitoring results will be incorrect. Please enter an integer value.
Log Stream Data to Disk (for Debugging)	Define if you want the probe to write a logfile of the stream and packet data to the data folder (see **Data Storage** 3226). Choose between: ▪ **None (recommended)**: Do not write additional logfiles. Recommended for normal use cases.

IPFIX SPECIFIC SETTINGS

- **Only for the 'Other' channel**: Only write logfiles of data that is not filtered otherwise and therefore accounted to the default **Other** channel.
- **All stream data**: Write logfiles for all data received.

Use with caution! When enabled, huge data files can be created. Please use for a short time and for debugging purposes only.

CHANNEL CONFIGURATION

Channel Selection

Define the categories the sensor accounts the traffic to. There are different groups of traffic available. Choose between:

- **Web**: Internet web traffic.
- **File Transfer**: Traffic caused by FTP.
- **Mail**: Internet mail traffic.
- **Chat**: Traffic caused by chat and instant messaging.
- **Remote Control**: Traffic caused by remote control applications, such as RDP, SSH, Telnet, and VNC.
- **Infrastructure**: Traffic caused by network services, such as DHCP, DNS, Ident, ICMP, and SNMP.
- **NetBIOS**: Traffic caused by NetBIOS communication.
- **Citrix**: Traffic caused by Citrix applications.
- **Other Protocols**: Traffic caused by various other protocols via UDP and TCP.

For each traffic group, you can select how many channels will be used for each group, that is, how detailed the sensor divides the traffic. For each group, choose between:

- **No**: Do not account traffic of this group in its own channel. All traffic of this group is accounted to the default channel named **Other**.
- **Yes**: Count all traffic of this group and summarize it into one channel.

CHANNEL CONFIGURATION

- **Detail**: Count all traffic of this group and further divide it into different channels. The traffic appears in several channels as shown in the **Content** column.
  Extensive use of this option can cause load problems on your probe system. We recommend setting specific, well-chosen filters for the data you really want to analyze.

You can change the default configuration for groups and channels. For details, please see this Knowledge Base article: How can I change the default groups and channels for xFlow and Packet Sniffer sensors?

FILTERING

Include Filter	Define if you want to filter any traffic. If you leave this field empty, all traffic will be included. To include specific traffic only, define filters using a special syntax. For detailed information, please see **Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors** 3175 section.
Exclude Filter	First, the filters defined in the **Include Filter** field are considered. From this subset, you can explicitly exclude traffic, using the same syntax. For detailed information, please see **Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors** 3175 section.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

PRIMARY TOPLIST

Primary Toplist	Define which will be your primary toplist. It will be shown in maps when adding a toplist object. Choose from: ▪ **Top Talkers** ▪ **Top Connections** ▪ **Top Protocols** ▪ [Any custom toplists you have added]

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

Toplists

For all flow and packet sniffer sensors there are **Toplists** available on the **Overview** tab of a sensor's detail page. Using toplists, you can review traffic data of small time periods in great detail. For more information, please see **Toplists** 2806 section.

More

Paessler Website: Paessler NetFlow Testers

- https://www.paessler.com/tools/netflowtester

Knowledge Base: How can I change the default groups and channels for xFlow and Packet Sniffer sensors?

- https://kb.paessler.com/en/topic/60203

Knowledge Base: What is the Active Flow Timeout in Flow sensors?

- https://kb.paessler.com/en/topic/66485

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

Related Topics

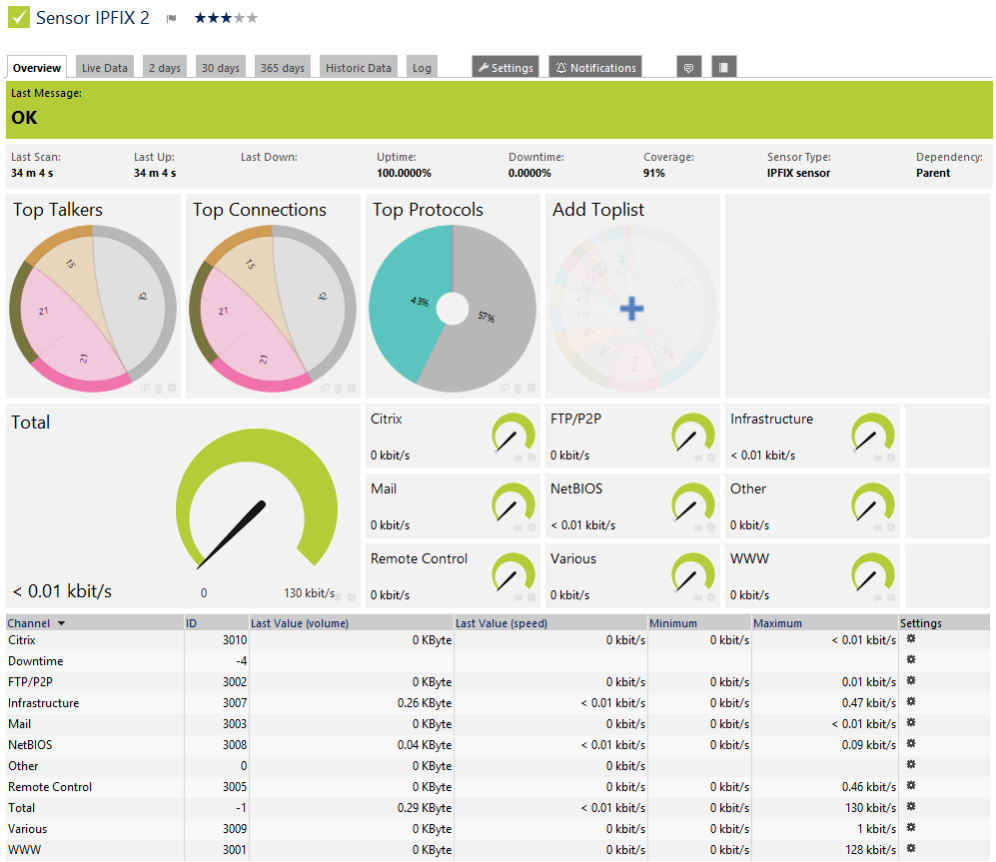
- **Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors** 3175
- **Channel Defintions for xFlow, IPFIX, and Packet Sniffer Sensors** 3180

7.8.65 IPFIX (Custom) Sensor

The IPFIX (Custom) sensor receives traffic data from an IPFIX (Internet Protocol Flow Information Export) compatible device and shows the traffic by type. In this custom sensor, you can define your own channel definitions to divide traffic into different channels. Ensure your device supports IPFIX when using this sensor.

- This sensor can show traffic by type individually according to your needs.

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



IPFIX Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/ipfix.png

Remarks

- In order for this sensor to work, you have to enable IPFIX export on the device. The device must send the flow data stream to the IP address of the PRTG probe system on which the sensor is set up (either a local or remote probe).
- This sensor type cannot be used in cluster mode. You can set it up on a local probe or remote probe only, not on a cluster probe.
- Knowledge Base: What is the Active Flow Timeout in Flow sensors?

- This sensor does not support more than 50 channels[1076] officially.
- For a general introduction to the technology behind flow monitoring, please see manual section **Monitoring Bandwidth via Flows**[3099].

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Limited to 50 Sensor Channels

PRTG does not support more than 50 sensor channels officially. Depending on the data used with this sensor type, you might exceed the maximum number of supported sensor channels. In this case, PRTG will try to display all sensor channels. However, please be aware that you will experience limited usability and performance.

Add Sensor

The **Add Sensor** dialog appears when you manually[288] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings**[360] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree[151], as well as in alarms[190], logs[198], notifications[2829], reports[2862], maps[2885], libraries[2845], and tickets[200].
Parent Tags	Shows **Tags**[124] that this sensor inherits[124] from its parent device, group, and probe[118]. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags**[124], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

BASIC SENSOR SETTINGS

	You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

IPFIX SPECIFIC SETTINGS

Receive IPFIX Packets on UDP Port	Enter the UDP port number on which the flow packets are received. It must match the one configured in the IPFIX export options of your hardware router device. Please enter an integer value.
Sender IP	Enter the IP address of the sending device you want to receive the IPFIX data from. Enter an IP address to receive data from a specific device only, or leave the field empty to receive data from any device on the specified port.
Receive IPFIX Packets on IP	Select the IP address(es) on which PRTG listens to IPFIX packets. The list of IP addresses shown here is specific to your setup. To select an IP address, add a check mark in front of the respective line. The IP address selected here must match the one configured in the IPFIX export options of your hardware router device.
Active Flow Timeout (Minutes)	Enter a time span in minutes after which new flow data must be received. If the timeout is reached and no new data is received, the sensor may switch to an **Unknown** status. Please enter an integer value. We recommend you set this one minute longer than the respective timeout configured in your hardware router device. For more details about this setting, please see this Knowledge Base article: What is the Active Flow Timeout in Flow sensors? If you set this value too low, flow information might be lost!
Sampling Mode	Define if you want to use the sampling mode. This setting must accord to the setting in the flow exporter. Choose between: ▪ **Off**: The standard flow will be used. ▪ **On**: Switch into sampling mode and specify the sampling rate below.

IPFIX SPECIFIC SETTINGS

Sampling Rate	This field is only visible when sampling mode is **On** above. Enter a number that matches the sampling rate in your device. If the number is different, monitoring results will be incorrect. Please enter an integer value.
Channel Definition	Please enter a channel definition to divide the traffic into different channels. Write each definition in one line. For detailed information, please see **Channel Definitions for xFlow and Packet Sniffer Sensors** 3180 section. All traffic for which no channel is defined will be accounted to the default channel named **Other**. Extensive use of many filters can cause load problems on your probe system. We recommend defining specific, well-chosen filters for the data you really want to analyze.
Log Stream Data to Disk (for Debugging)	Define if you want the probe to write a logfile of the stream and packet data to the data folder (see **Data Storage** 3226). Choose between: ▪ **None (recommended)**: Do not write additional logfiles. Recommended for normal use cases. ▪ **Only for the 'Other' channel**: Only write logfiles of data that is not filtered otherwise and therefore accounted to the default **Other** channel. ▪ **All stream data**: Write logfiles for all data received. Use with caution! When enabled, huge data files can be created. Please use for a short time and for debugging purposes only.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

FILTERING

Include Filter	Define if you want to filter any traffic. If you leave this field empty, all traffic will be included. To include specific traffic only, define filters using a special syntax. For detailed information, please see **Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors** 3175 section.
Exclude Filter	First, the filters defined in the **Include Filter** field are considered. From this subset, you can explicitly exclude traffic, using the same syntax. For detailed information, please see **Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors** 3175 section.

PRIMARY TOPLIST

Primary Toplist	Define which will be your primary toplist. It will be shown in maps when adding a toplist object. Choose from: ▪ **Top Talkers** ▪ **Top Connections** ▪ **Top Protocols** ▪ [Any custom toplists you have added]

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. ⓘ Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

Toplists

For all flow and packet sniffer sensors there are **Toplists** available on the **Overview** tab of a sensor's detail page. Using toplists, you can review traffic data of small time periods in great detail. For more information, please see **Toplists** 2806 section.

More

Paessler Website: Paessler NetFlow Testers

- https://www.paessler.com/tools/netflowtester

Knowledge Base: How can I change the default groups and channels for xFlow and Packet Sniffer sensors?

- https://kb.paessler.com/en/topic/60203

Knowledge Base: What is the Active Flow Timeout in Flow sensors?

- https://kb.paessler.com/en/topic/66485

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

Related Topics

- **Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors** 3175
- **Channel Defintions for xFlow, IPFIX, and Packet Sniffer Sensors** 3180

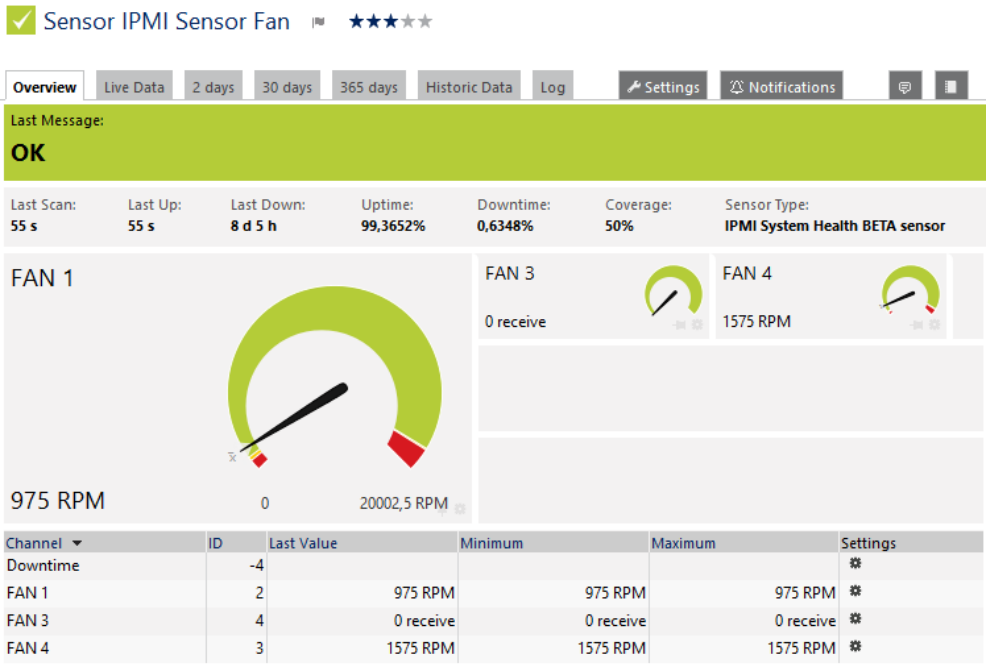
7.8.66 IPMI System Health Sensor

The IPMI System Health sensor monitors the status of a system via the Intelligent Platform Management Interface (IPMI).

It can show the following:

- Temperatures of, for example, the system or the peripheral temperature.
- Fan rotation per minute
- Voltages
- Status of a power supply

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



IPMI System Health Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/ipmi_system_health.png

Remarks

- You have to explicitly specify the credentials of the IPMI in the sensor settings.
- Requires 1086 .NET 4.0 or higher on the probe system.
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.

- This sensor type has predefined limits for several metrics. You can change these limits individually in the channel settings. For detailed information about channel limits, please refer to the manual section **Sensor Channels Settings** 2782.
- Currently, this sensor type is in beta status. The methods of operating can change at any time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Requirement: .NET Framework

This sensor type requires the Microsoft .NET Framework to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the remote probe 3196. If the framework is missing, you cannot create this sensor.

Required .NET version (with latest updates): .NET 4.0 (Client Profile is sufficient), .NET 4.5, or .NET 4.6.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/60543

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Before you can actually add this sensor, PRTG will ask you to provide your credentials for the Intelligent Platform Management Interface (IPMI) in the add sensor dialog 288. Enter the **Username** and the **Password** in the respective fields.

Select the metrics you want to monitor. PRTG will create one sensor for each metric you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

IPMI SPECIFIC

Group	Select the measurements you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

IPMI CREDENTIALS

Username	Enter the username for the Intelligent Platform Management Interface (IPMI). If not changed yet, this field shows the username that you defined during sensor creation.
Password	Enter the password for the Intelligent Platform Management Interface (IPMI). If not changed yet, this field shows the encrypted password that you defined the sensor creation.

IPMI SPECIFIC

Group	Shows the metric that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Logfile Results	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section **Data Storage** 3226. You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

SENSOR DISPLAY

	You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

SCANNING INTERVAL

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: Which .NET version does PRTG require?

- https://kb.paessler.com/en/topic/60543

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

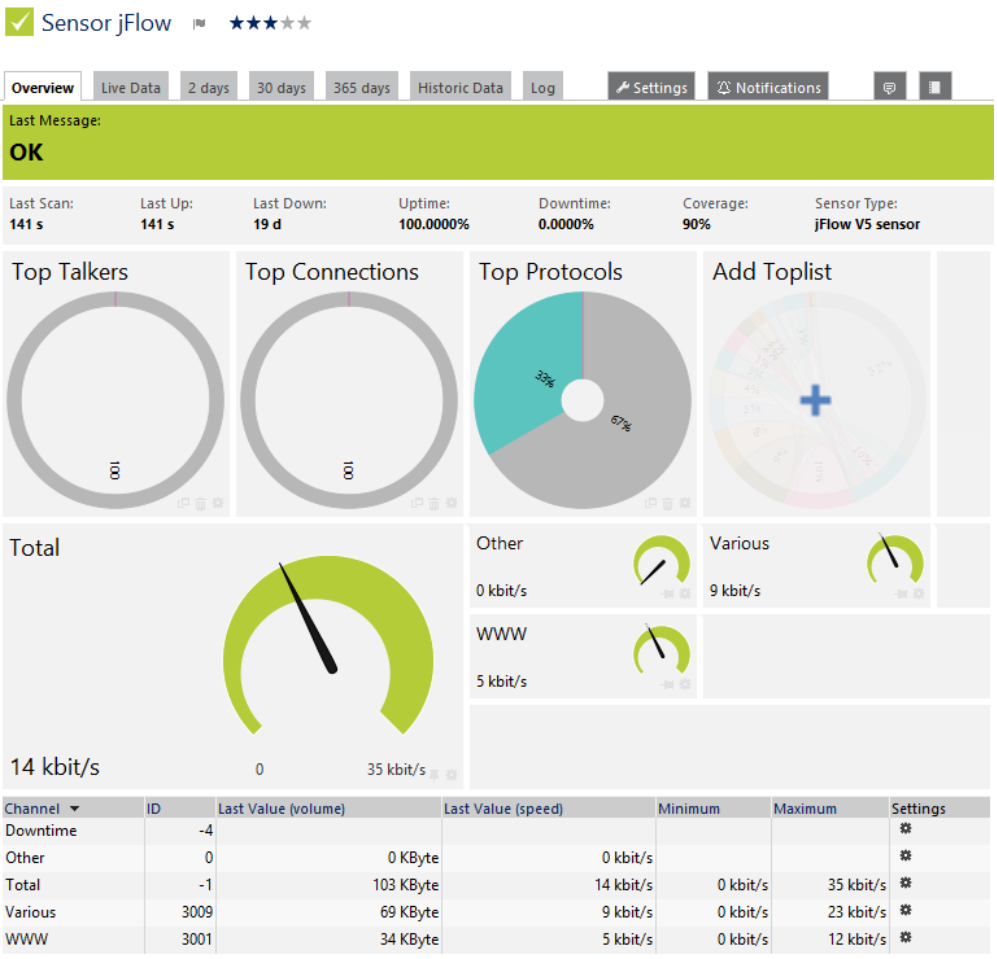
7.8.67 jFlow V5 Sensor

The jFlow V5 sensor receives traffic data from a jFlow V5 compatible device and shows the traffic by type. On your hardware device, ensure it matches jFlow V5! There are several filter options available to divide traffic into different channels.

This sensor can show the following traffic types in kbit per second:

- Chat (IRC, AIM)
- Citrix
- FTP/P2P (file transfer)
- Infrastructure (network services: DHCP, DNS, Ident, ICMP, SNMP)
- Mail (mail traffic: IMAP, POP3, SMTP)
- NetBIOS
- Remote control (RDP, SSH, Telnet, VNC)
- WWW (web traffic: HTTP, HTTPS)
- Total traffic
- Other protocols (other UDP and TCP traffic)

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



jFlow V5 Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/jflow_v5.png

Remarks

- You have to enable jFlow export of the respective version on the monitored device for this sensor to work. The device must send the flow data stream to the IP address of the PRTG probe system on which the sensor is set up (either a local or remote probe).
- This sensor type cannot be used in cluster mode. You can set it up on a local probe or remote probe only, not on a cluster probe.
- Knowledge Base: What is the Active Flow Timeout in Flow sensors?
- For a general introduction to the technology behind flow monitoring, please see manual section **Monitoring Bandwidth via Flows** 3099.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

JFLOW V5 SPECIFIC SETTINGS

Receive jFlow Packets on UDP Port	Enter the UDP port number on which PRTG receives the flow packets. It must match the one you have configured in the jFlow export options of your hardware router device. Please enter an integer value. When you configure the export, please make sure you select the appropriate jFlow version for this sensor.
Sender IP	Enter the IP address of the sending device you want to receive the jFlow from. Enter an IP address to receive data from a specific device only, or leave the field empty to receive data from any device on the specified port.
Receive jFlow Packets on IP	Select the IP address(es) on which PRTG listens to jFlow packets. The list of IP addresses you see here is specific to your setup. To select an IP address, add a check mark in front of the respective line. You can also select and deselect all items by using the check box in the table head. The IP address you select here must match the one you configured in the jFlow export options of your hardware router device. When you configure the export, please make sure you select the appropriate jFlow version for this sensor.
Active Flow Timeout (Minutes)	Enter a time span in minutes after which the sensor must have received new flow data. If the timeout is reached and no new data came in, the sensor may switch to an **Unknown** status. Please enter an integer value. We recommend you set this one minute longer than the respective timeout configured in your hardware router device. For more details about this setting, please see this Knowledge Base article: What is the Active Flow Timeout in Flow sensors? If you set this value too low, flow information might be lost!
Sampling Mode	Define if you want to use the sampling mode. This setting must accord to the setting in the flow exporter. Choose between: ▪ **Off**: The standard flow will be used. ▪ **On**: Switch into sampling mode and specify the sampling rate below.
Sampling Rate	This field is only visible when sampling mode is **On** above. Enter a number that matches the sampling rate in your exporter device. If the number is different, monitoring results will be incorrect. Please enter an integer value.

JFLOW V5 SPECIFIC SETTINGS

Log Stream Data to Disk (for Debugging)

Define if you want the probe to write a logfile of the stream and packet data to the data folder (see **Data Storage** 3226). Choose between:

- **None (recommended)**: Do not write additional logfiles. Recommended for normal use cases.
- **Only for the 'Other' channel**: Only write logfiles of data that is not filtered otherwise and therefore accounted to the default **Other** channel.
- **All stream data**: Write logfiles for all data received.

Use with caution! When enabled, huge data files can be created. Please use for a short time and for debugging purposes only.

CHANNEL CONFIGURATION

Channel Selection

Define the categories the sensor accounts the traffic to. There are different groups of traffic available. Choose between:

- **Web**: Internet web traffic.
- **File Transfer**: Traffic caused by FTP.
- **Mail**: Internet mail traffic.
- **Chat**: Traffic caused by chat and instant messaging.
- **Remote Control**: Traffic caused by remote control applications, such as RDP, SSH, Telnet, and VNC.
- **Infrastructure**: Traffic caused by network services, such as DHCP, DNS, Ident, ICMP, and SNMP.
- **NetBIOS**: Traffic caused by NetBIOS communication.
- **Citrix**: Traffic caused by Citrix applications.
- **Other Protocols**: Traffic caused by various other protocols via UDP and TCP.

For each traffic group, you can select how many channels will be used for each group, that is, how detailed the sensor divides the traffic. For each group, choose between:

- **No**: Do not account traffic of this group in its own channel. All traffic of this group is accounted to the default channel named **Other**.

CHANNEL CONFIGURATION

- **Yes**: Count all traffic of this group and summarize it into one channel.
- **Detail**: Count all traffic of this group and further divide it into different channels. The traffic appears in several channels as shown in the **Content** column.
  Extensive use of this option can cause load problems on your probe system. We recommend setting specific, well-chosen filters for the data you really want to analyze.

You can change the default configuration for groups and channels. For details, please see this Knowledge Base article: How can I change the default groups and channels for xFlow and Packet Sniffer sensors?

FILTERING

Include Filter	Define if you want to filter any traffic. If you leave this field empty, all traffic will be included. To include specific traffic only, define filters using a special syntax. For detailed information, please see **Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors** 3175 section.
Exclude Filter	First, the filters defined in the **Include Filter** field are considered. From this subset, you can explicitly exclude traffic, using the same syntax. For detailed information, please see **Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors** 3175 section.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

PRIMARY TOPLIST

Primary Toplist	Define which will be your primary toplist. It will be shown in maps when adding a toplist object. Choose from: ▪ **Top Talkers** ▪ **Top Connections** ▪ **Top Protocols** ▪ [Any custom toplists you have added]

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

Toplists

For all flow and packet sniffer sensors there are **Toplists** available on the **Overview** tab of a sensor's detail page. Using toplists, you can review traffic data of small time periods in great detail. For more information, please see **Toplists** 2806 section.

More

Knowledge Base: Where is the volume line in graphs?

- https://kb.paessler.com/en/topic/61272

Knowledge Base: What is the Active Flow Timeout in Flow sensors?

- https://kb.paessler.com/en/topic/66485

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

Related Topics

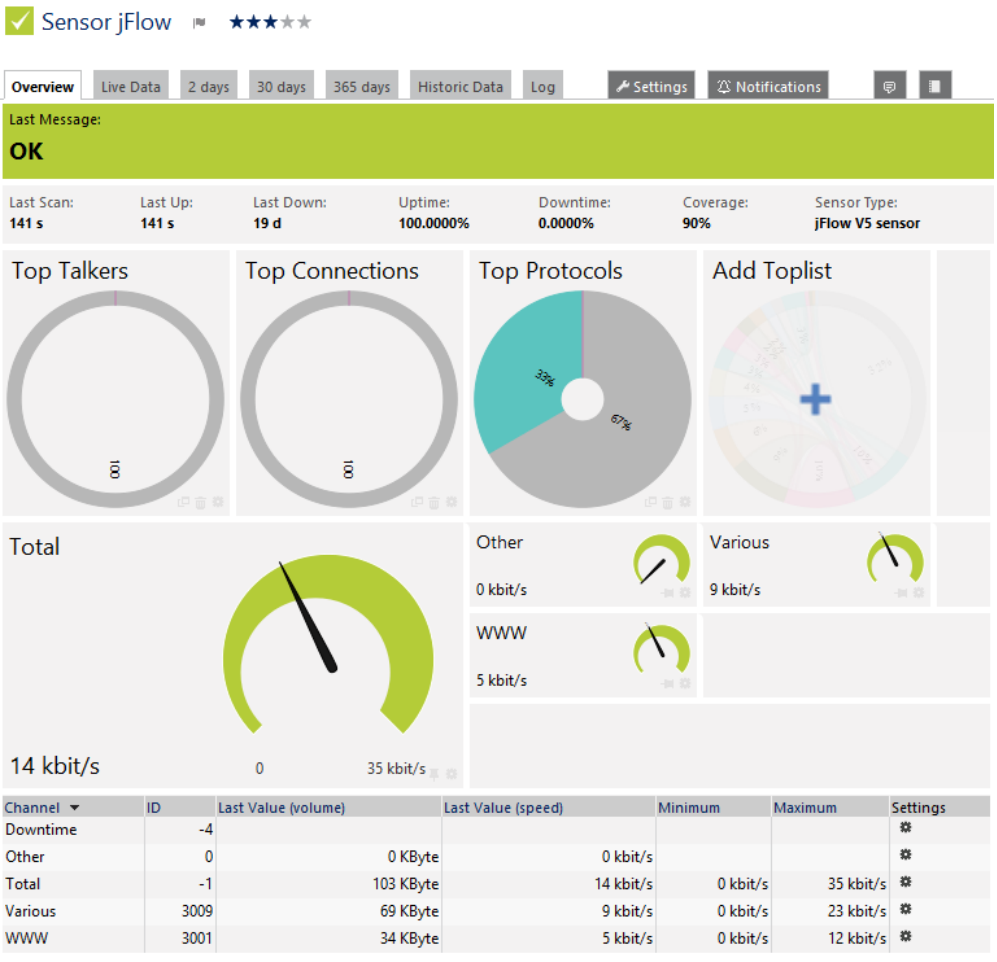
- **Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors** 3175
- **Channel Defintions for xFlow, IPFIX, and Packet Sniffer Sensors** 3180

7.8.68 jFlow V5 (Custom) Sensor

The jFlow V5 (Custom) sensor receives traffic data from a jFlow V5 compatible device and shows the traffic by type. On your hardware device, please make sure it matches jFlow V5! In this custom sensor, you can define your own channel definitions to divide traffic into different channels.

- This sensor can show traffic by type individually according to your needs.

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



jFlow V5 Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/jflow_v5.png

Remarks

- You have to enable jFlow export of the respective version on the monitored device for this sensor to work. The device must send the flow data stream to the IP address of the PRTG probe system on which the sensor is set up (either a local or remote probe).

- This sensor type cannot be used in cluster mode. You can set it up on a local probe or remote probe only, not on a cluster probe.
- Knowledge Base: What is the Active Flow Timeout in Flow sensors?
- This sensor does not support more than 50 channels 1108 officially.
- For a general introduction to the technology behind flow monitoring, please see manual section **Monitoring Bandwidth via Flows** 3099.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Limited to 50 Sensor Channels

PRTG does not support more than 50 sensor channels officially. Depending on the data used with this sensor type, you might exceed the maximum number of supported sensor channels. In this case, PRTG will try to display all sensor channels. However, please be aware that you will experience limited usability and performance.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	Enter one or more **Tags**, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

JFLOW SPECIFIC SETTINGS

Receive jFlow Packets on UDP Port	Enter the UDP port number on which PRTG receives the flow packets. It must match the one you have configured in the jFlow export options of your hardware router device. Please enter an integer value. When you configure the export, please make sure you select the appropriate jFlow version for this sensor.
Sender IP	Enter the IP address of the sending device you want to receive the jFlow from. Enter an IP address to receive data from a specific device only, or leave the field empty to receive data from any device on the specified port.
Receive jFlow Packets on IP	Select the IP address(es) on which PRTG listens to jFlow packets. The list of IP addresses you see here is specific to your setup. To select an IP address, add a check mark in front of the respective line. You can also select and deselect all items by using the check box in the table head. The IP address you select here must match the one you configured in the jFlow export options of your hardware router device. When you configure the export, please make sure you select the appropriate jFlow version for this sensor.

JFLOW SPECIFIC SETTINGS

Active Flow Timeout (Minutes)	Enter a time span in minutes after which the sensor must have received new flow data. If the timeout is reached and no new data came in, the sensor may switch to an **Unknown** status. Please enter an integer value. We recommend you set this one minute longer than the respective timeout configured in your hardware router device. For more details about this setting, please see this Knowledge Base article: What is the Active Flow Timeout in Flow sensors? If you set this value too low, flow information might be lost!
Sampling Mode	Define if you want to use the sampling mode. This setting must accord to the setting in the flow exporter. Choose between: ▪ **Off**: The standard flow will be used. ▪ **On**: Switch into sampling mode and specify the sampling rate below.
Sampling Rate	This field is only visible when sampling mode is **On** above. Enter a number that matches the sampling rate in your exporter device. If the number is different, monitoring results will be incorrect. Please enter an integer value.
Channel Definition	Please enter a channel definition to divide the traffic into different channels. Write each definition in one line. For detailed information, please see **Channel Defintions for xFlow and Packet Sniffer Sensors** 3180 section. All traffic for which no channel is defined will be accounted to the default channel named **Other**. Extensive use of many filters can cause load problems on your probe system. We recommend defining specific, well-chosen filters for the data you really want to analyze.
Log Stream Data to Disk (for Debugging)	Define if you want the probe to write a logfile of the stream and packet data to the data folder (see **Data Storage** 3226). Choose between: ▪ **None (recommended)**: Do not write additional logfiles. Recommended for normal use cases. ▪ **Only for the 'Other' channel**: Only write logfiles of data that is not filtered otherwise and therefore accounted to the default **Other** channel. ▪ **All stream data**: Write logfiles for all data received.

JFLOW SPECIFIC SETTINGS

Use with caution! When enabled, huge data files can be created. Please use for a short time and for debugging purposes only.

FILTERING

Include Filter

Define if you want to filter any traffic. If you leave this field empty, all traffic will be included. To include specific traffic only, define filters using a special syntax. For detailed information, please see **Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors** 3175 section.

Exclude Filter

First, the filters defined in the **Include Filter** field are considered. From this subset, you can explicitly exclude traffic, using the same syntax. For detailed information, please see **Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors** 3175 section.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.
- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

SENSOR DISPLAY

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

PRIMARY TOPLIST

Primary Toplist	Define which will be your primary toplist. It will be shown in maps when adding a toplist object. Choose from: ▪ **Top Talkers** ▪ **Top Connections** ▪ **Top Protocols** ▪ [Any custom toplists you have added]

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

Toplists

For all flow and packet sniffer sensors there are **Toplists** available on the **Overview** tab of a sensor's detail page. Using toplists, you can review traffic data of small time periods in great detail. For more information, please see **Toplists** 2806 section.

More

Knowledge Base: Where is the volume line in graphs?

- https://kb.paessler.com/en/topic/61272

Knowledge Base: What is the Active Flow Timeout in Flow sensors?

- https://kb.paessler.com/en/topic/66485

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

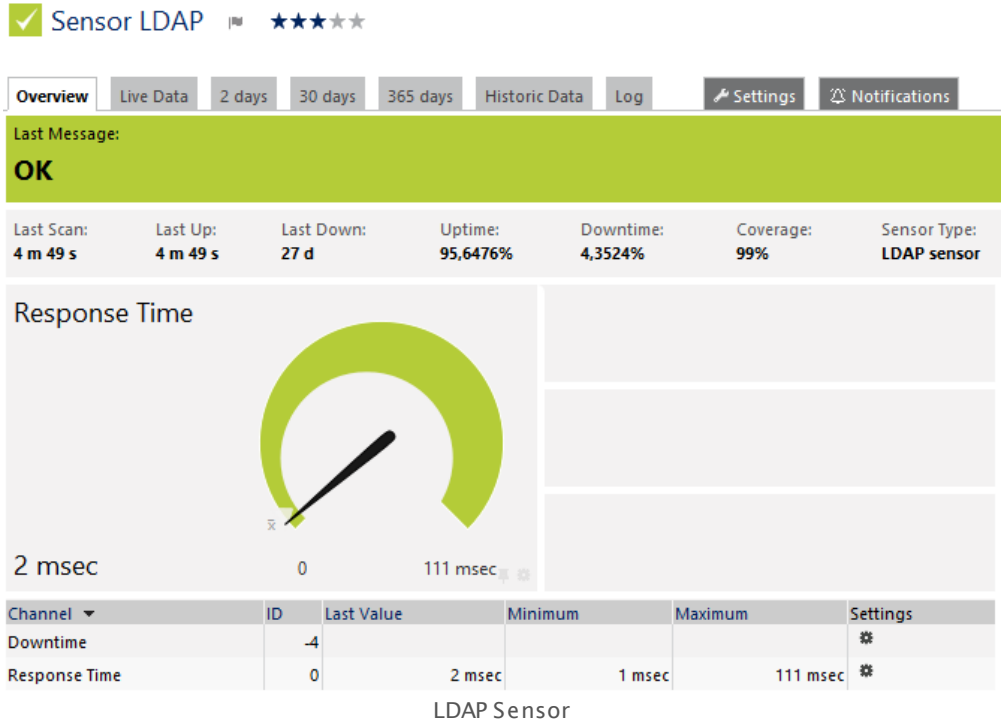
Related Topics

- **Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors** 3175
- **Channel Defintions for xFlow, IPFIX, and Packet Sniffer Sensors** 3180

7.8.69 LDAP Sensor

The LDAP sensor monitors directory services using Lightweight Directory Access Protocol (LDAP), connecting to the server trying a "bind". If the server does not respond or authentication fails, it will show an error message.

- The sensor shows the response time of the server.



LDAP Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/ldap.png

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

LDAP SPECIFIC

Port	Enter the LDAP port number, usually port 389 for unencrypted connections. Please enter an integer value.
Distinguished Name	Enter the Distinguished Name (DN) you want to authenticate to the LDAP server. Usually, this is the information for the user you want to authenticate with. For example, use the format **cn=Manager,dc=my-domain,dc=com** for a DN on an OpenLDAP server.
Password	Enter the password for the entered Distinguished Name.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

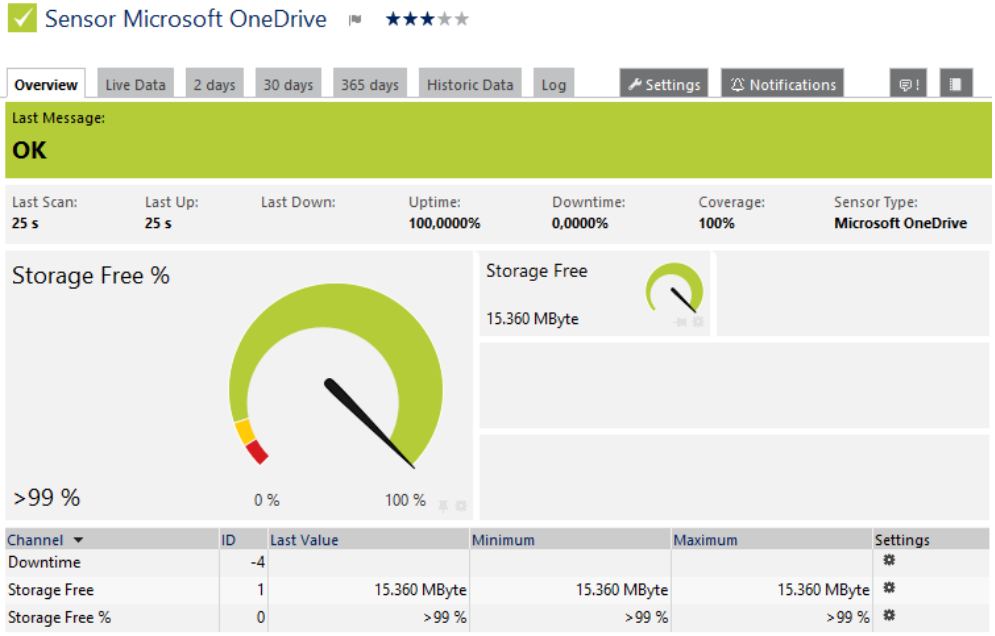
Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.70 Microsoft OneDrive Sensor

The Microsoft OneDrive sensor monitors a Microsoft OneDrive Personal account using the OneDrive Application Programming Interface (API) and OAuth2. It shows the following:

- Free storage in bytes and percent



Microsoft OneDrive Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/microsoft_onedrive.png

Remarks

- The minimum scanning interval for this sensor type is **30 minutes**.
- For details about OAuth2 authentication, please see manual section Authentication Using OAuth2 1133.
- This sensor type only supports OneDrive Personal, it does not work with OneDrive Business.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

PRTG requires OAuth2 authorization before you can actually add this sensor type. Provide the requested credentials in the appearing window.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

MICROSOFT CREDENTIALS

This sensor type uses OAuth2 authentication to get access to your Microsoft account. For details about the authentication approach, please see section **Authentication Using OAuth2** 1133.

OAuth URL	Click the button **Get Access Code** to connect this sensor to your Microsoft account using OAuth2. This is necessary to allow the sensor to query data from OneDrive. A new browser window appears. Please follow the steps there and confirm the permission for PRTG to connect to your OneDrive account. OneDrive forwards you to an empty page after completing the authorization process. Copy the complete **URL** of this empty page and paste it into the **OAuth Code** field below.
OAuth Code	Paste the complete **URL** from the address bar of your browser on the empty page to which OneDrive forwards you. The empty page appears after completing the authorization process for PRTG at your OneDrive account. Click **OK** to define the sensor settings 840. It is mandatory to connect this sensor to your OneDrive account to create this sensor. Please complete the OAuth approach first to get the OAuth code.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.

BASIC SENSOR SETTINGS

Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

MICROSOFT CREDENTIALS

OAuth Code	Shows the authorization code that the sensor uses to get access to your OneDrive account. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. ⓘ You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.

SCANNING INTERVAL

- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

This sensor type has a fixed minimum scanning interval for performance reasons. You cannot run the sensor in shorter intervals than this minimum interval. Consequently, shorter scanning intervals as defined in **System Administration—Monitoring** 2955 are not available for this sensor.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

Authentication Using OAuth2

This sensor type uses the OAuth2 security protocol to access the account from which you want to retrieve and monitor data. OAuth2 enables you to grant access to the target account without sharing your password with PRTG. The authorization approach of PRTG using OAuth2 works as follows.

1. **Authorization Request**
   First, you have to request authorization for this sensor to access service resources from your account. For this purpose you are asked to get an access code for this sensor in the **Add Sensor** dialog. Click the **Get Access Code** button to start the authorization process using OAuth2. A new browser window will open on the authorization server of the target service.

2. **Verifying Identity**
   This new window contains a login form for your account that you want to monitor. Log in to your account using your credentials for this service to authenticate your identity. This is a common login to your account on the target server so PRTG will not see your password. The service will forward you to the authorization page and asks you to permit PRTG to access the data in your account.
   If you are already logged in to the service with a user account, you do not have to enter credentials in this step and get directly to the access permission page.

3. **Authorizing PRTG**
   Permit PRTG to access information on your account. Note that this permission holds only for this specific sensor, not for other sensors of this type or PRTG as a whole. For each sensor of this type you add, you have to confirm the access permission anew. You can change the account permissions at any time in your account at the target service.

4. **Getting Authorization Code**
   Permitting PRTG to access your account data forwards you to a page where the service provides an **authorization code**. Copy this code and switch back to the **Add Sensor** dialog in PRTG.
   The code is only valid a short period of time and expires after a few minutes. You can use a particular code only once.

5. **Providing Authorization Code**
   Paste the authorization code into the **OAuth Code** field and complete the **Add Sensor** dialog. You do not have to go through further configuration steps manually. The sensor will accomplish the following steps automatically.

6. **Requesting Access Token**
   After receiving the authorization code, PRTG will request an access token from the API of the target service. For this purpose, PRTG transmits the authorization code together with several authentication details. The API checks if the authorization is valid and returns the access token to PRTG. Access token are specific for one account and one application (here: PRTG). The authorization process to read data from your account is now complete.

7. **Retrieving Data**
   The sensor transmits the access token with each sensor scan in the defined scanning interval to authenticate with your account. It is not necessary to use the original account credentials anew. The used tokens will refresh automatically from time to time.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

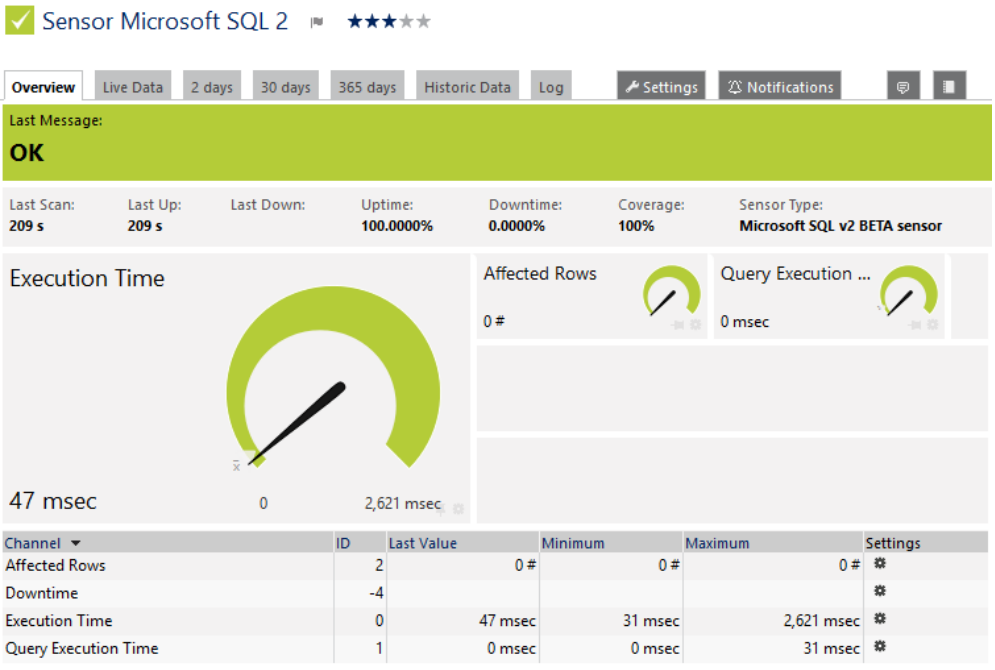
For more general information about settings, please see the **Object Settings** 188 section.

7.8.71 Microsoft SQL v2 Sensor

The Microsoft SQL v2 sensor monitors a database on a Microsoft SQL server and executes a defined query.

It can show the following:

- Execution time of the whole request (including connection buildup, query execution, transaction handling, disconnection)
- Execution time of the given query
- Number of rows which were addressed by the query (including select statements if you process data tables)
- It can also process the data table and show defined values in individual channels.



Microsoft SQL v2 Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/microsoft_sql_v2.png

Remarks

- Requires 1136 .NET 4.0 on the probe system.
- Define credentials, custom port (if required), and timeout in settings section **Credentials for Database Management Systems** 370 of the parent device, or in the settings of a group or probe above.
- PRTG Manual: **Monitoring Databases** 3120 (includes an example 3121 for channel value selection)
- Knowledge Base: How to setup the SQL v2 sensors in PRTG? Is there a guide?

- Knowledge Base: How can I monitor strings from an SQL database and show a sensor status depending on it?
- Knowledge Base: How can I monitor error tables in SQL databases?
- Your SQL query must be stored in a file on the system of the probe the sensor is created on. If you use it on a remote probe, store the file on the system running the remote probe. In a cluster setup, copy the file to every cluster node.
- Save the SQL script with the query into the **\Custom Sensors\sql\mssql** subfolder of your PRTG installation. See manual section **Data Storage** 3226 for more information about how to find this path.
- This sensor type supports Microsoft SQL server 2005 or later.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Requirement: .NET Framework

This sensor type requires the Microsoft .NET Framework to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the remote probe 3196. If the framework is missing, you cannot create this sensor.

Required .NET version (with latest updates): .NET 4.0 (Client Profile is sufficient), .NET 4.5, or .NET 4.6.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/60543

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DATABASE SPECIFIC

Database	Enter the name of the SQL database to which the sensor connects. For example, such a database's name could be MyDatabase. This is a logical entity on the database server where database objects like tables or stored procedures exist.
SQL Server Instance	Define if you want to use an instance name for the database connection. Choose between: ▪ **No instance name required (default)**: Use the default instance for the connection. ▪ **Use instance name**: Use a named instance that you can specify below.
Instance Name	This field is only visible if you enable instance name usage above. Enter the named instance you want to monitor.
Encryption	Define encryption usage for the database connection. Choose between:

DATABASE SPECIFIC

- **Use server defaults (default)**: The database connection is only encrypted if enforced by the database server.
- **Enforce encryption but do not validate server certificate**: Choose this option to make sure the database connection is encrypted.
- **Enforce encryption and validate server certificate**: Choose this option to force encryption and to validate the database server certificate. This approach provides highest security, for example, it helps prevent "man in the middle" attacks.
  The sensor validates the certificate only if the database server enforces encryption!

DATA

SQL Query File

Select an SQL script file that includes a valid SQL statement to execute on the server. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

The script will be executed with every scanning interval. The list contains SQL scripts from the database management system specific **\Custom Sensors\sql** subfolder of your PRTG installation. Store your script there. If used on a remote probe, the file must be stored on the system running the remote probe. If used on a cluster probe, you must store the file on all servers running a cluster node!

For more information on how to find this path, please see **Data Storage** 3226 section. By default, there is the demo script **Demo Serveruptime.sql** available that you can use to monitor the uptime of the target server.

For example, a correct expression in the file could be: SELECT AVG (UnitPrice) FROM Products. If you want to use transactions, separate the individual steps with semicolons ";".

Please be aware that with each request, the full result set will be transferred, so use filters and limits in your query.

You can use the following placeholders in your query file to have them replaced by an input parameter:

- Microsoft SQL, MySQL, PostgreSQL: **@prtg**
- Oracle SQL: **:prtg**

DATA

	▪ ADO SQL: **?** (question mark) This is useful if you have various SQL sensors with queries that differ in only one parameter.
Use Input Parameter	Define if you want to pass a parameter to your SQL query file. This will replace the placeholder %prtg (Microsoft SQL, MySQL, PostgreSQL), or :prtg (Oracle SQL), or ? (ADO SQL) in the SQL query. Choose between: ▪ **Don't use input parameter (default)**: Execute the SQL query file without using placeholders. ▪ **Use input parameter**: Execute an SQL query file that contains a placeholder. Provide the parameter you want to use in the query below.
Input Parameter	This field is only visible if you choose **Use input parameter** above. Enter the parameter you want to pass to the SQL query file. This parameter replaces the placeholder %prtg or :prtg or ? in the SQL query. You can also use PRTG placeholders for custom sensors (command line parameters) as input parameter, for example, %sensorid or %deviceid. For details, see **Application Programming Interface (API) Definition** 3174. Provide strings as they are and do not surround them with quotation marks. PRTG will correctly insert string parameters into the query automatically.
Use Transaction	Define if you want to use transactions and if they will affect the database content. Choose between: ▪ **Don't use transaction (default)**: No transactions will be executed. ▪ **Use transaction and always rollback**: Choose this option to ensure that no data in the database will be changed by the query. In the SQL query file, separate the single steps of the transaction with semicolons. ▪ **Use transaction and commit on success**: Choose this option to perform changes on the database with the query. The changes will only apply if all execution steps succeed without any errors. In the SQL query file, separate the single steps of the transaction with semicolons.
Data Processing	Define if you want to process data from the database. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew. Choose between:

DATA

	▪ **Just execute the query**: If you select this option, the sensor will only show information about the number of affected rows and the execution time of the query. Affected rows are rows that were changed somehow with the query (for example, created, deleted, edited). ▪ **Count table rows**: Choose this option if you perform a SELECT statement and want to monitor how many rows of the data table this statement returns. ▪ **Process data table**: Select this option to read and analyze the queried data table. If you select this option, the sensor will count rows with SELECT statements as well.
Handle DBNull in Channel Values as	This setting is only visible if you select **Process data table** above. Define the sensor behavior if DBNull is returned by the query. Choose between: ▪ **Error**: The sensor will show a **Down** status if DBNull is reported. ▪ **Number 0**: The sensor will recognize the result DBNull as a valid value and interpret it as the number 0.
Select Channel Value by	This setting is only visible if you select **Process data table** above. Define how the desired cell in the database table will be selected. This is necessary to configure the cells that will be used in the sensor channels. Choose between: ▪ **Column number**: The channel value will be determined by using the value in row 0 of the column whose number you specify below. ▪ **Column name**: The channel value will be determined by using the value in row 0 of the column whose name you specify below. ▪ **Row number**: The channel value will be determined by using the value in column 0 of the row whose number you specify below. ▪ **Key value pair**: The channel value will be determined by searching in column 0 for the key you specify below and returning the value in column 1 of the same row where the key value was found. The option you choose here also defines the method to optionally determine a value for the sensor message. For details, see setting **Use Data Table Value in Sensor Message** below. Please see manual section **Monitoring Databases** 3120 for an example 3121 for channel value selection.

DATA

Sensor Channel #x	This setting is only visible if you select **Process data table** above. You can define up to 10 different channels for the data processing of this sensor. You have to define at least one data channel if you process the data table, so you will see all available settings for Channel #1 without enabling it manually. For all other possible channels, choose between: ▪ **Disable**: This channel will not be added to the sensor. ▪ **Enable**: This channel will be added to the sensor. Define the settings as described above. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Sensor Channel #x Name	This setting is only visible if you select **Process data table** above. Enter a unique name for the channel. Please enter a string. Channels will be generated dynamically with this name as identifier. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Sensor Channel #x Column Number	This setting is only visible if you select **Column number** above. Provide the number of the column which will be used to determine the channel value in row 0. Please enter an integer value.
Sensor Channel #x Column Name	This setting is only visible if you select **Column number** above. Provide the name of the column which will be used to determine the channel value in row 0. Please enter a string.
Sensor Channel #x Row Number	This setting is only visible if you select **Row number** above. Provide the number of the row which will be used to determine the channel value in column 0. Please enter an integer value.
Sensor Channel #x Key	This setting is only visible if you select **Key value pair** above. Provide the key to search for in column 0 of the data table. The value in column 1 of the same row where the key value was found will be used to determine the channel value. Please enter a string.
Sensor Channel #x Mode	This setting is only visible if you select **Process data table** above. Define how to display the determined value in the channel. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew. Choose between: ▪ **Absolute (recommended)**: Shows the value as the sensor retrieves it from the data table.

DATA

	▪ **Difference**: The sensor calculates and shows the difference between the last and the current value returned from the data table.
Sensor Channel #x Unit	This setting is only visible if you select **Process data table** above. Define the unit of the channel value. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew. Choose between: ▪ BytesBandwidth ▪ BytesMemory ▪ BytesDisk ▪ Temperature ▪ Percent ▪ TimeResponse ▪ TimeSeconds ▪ TimeHours ▪ Count ▪ CPU ▪ BytesFile ▪ SpeedDisk ▪ SpeedNet ▪ Custom ▪ Value Lookup For more information about the available units, please refer to the PRTG **Application Programming Interface (API) Definition** 3174 for custom sensors. To use lookups 3183 with this channel, choose **Value Lookup** and select your lookup file below. Do not use **Custom** for using lookups with this sensor!
Sensor Channel #x Custom Unit	This setting is only visible if you select **Custom** above. Define a unit for the channel value. Please enter a string.
Sensor Channel #x Value Lookup	This settings is only visible if you select **Value Lookup** above. Select a lookup 3183 file that you want to use with this channel.

DATA

Use Data Table Value in Sensor Message	This setting is only visible if you select **Process data table** above. Define if the sensor message will show a value from the data table. Choose between: ▪ **Disable**: Do not use a custom sensor message. ▪ **Enable**: Define a custom sensor message with a defined value of the data table. Define the value selection below. The method to determine a value for the sensor message is defined in setting **Select Channel Value by** above.
Sensor Message Column Number	This setting is only visible if you select **Column number** and **Use Data Table Value in Sensor Message** above. Enter the number of a column. The sensor message will show the value in row 0 of this column. Please enter an integer value. ⓘ Columns and rows start with index 0.
Sensor Message Column Name	This setting is only visible if you select **Column name** and **Use Data Table Value in Sensor Message** above. Enter the name of a column. The sensor message will show the value in row 0 of this column. Please enter a string. ⓘ Columns and rows start with index 0.
Sensor Message Row Number	This setting is only visible if you select **Row number** and **Use Data Table Value in Sensor Message** above. Enter the number of a row. The sensor message will show value in column 0 of this row. Please enter an integer value. ⓘ Columns and rows start with index 0.
Sensor Message Key	This setting is only visible if you select **Key value pair** and **Use Data Table Value in Sensor Message** above. Enter a key to search for in column 0 of the data table. The sensor message will show the value in column 1 of the row where the key has been found. Please enter a string. ⓘ Columns and rows start with index 0.
Sensor Message	This setting is only visible if you select **Use Data Table Value in Sensor Message** above. Define the sensor message. Please enter a string. Use the placeholder {0} at the position where the value will be added. Example: **The message is {0}**

DATA

If Sensor Message Changes

Define what this sensor will do when the sensor value changes. You can choose between:

- **Ignore changes (default)**: The sensor takes no action on change.
- **Trigger 'change' notification**: The sensor sends an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification 2791 whenever the sensor value changes.

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result**: Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section **Data Storage** 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.

SCANNING INTERVAL

- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. ⓘ To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: How to setup the SQL v2 sensors in PRTG? Is there a guide?

- https://kb.paessler.com/en/topic/70618

Knowledge Base: How can I monitor strings from an SQL database and show a sensor status depending on it?

- https://kb.paessler.com/en/topic/63259

Knowledge Base: How do I monitor the size of a Microsoft SQL server database?

- https://kb.paessler.com/en/topic/18183

Knowledge Base: How can I monitor error tables in SQL databases?

- https://kb.paessler.com/en/topic/70774

Knowledge Base: Which .NET version does PRTG require?

- https://kb.paessler.com/en/topic/60543

PRTG Manual:

- **Monitoring Databases** 3120

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

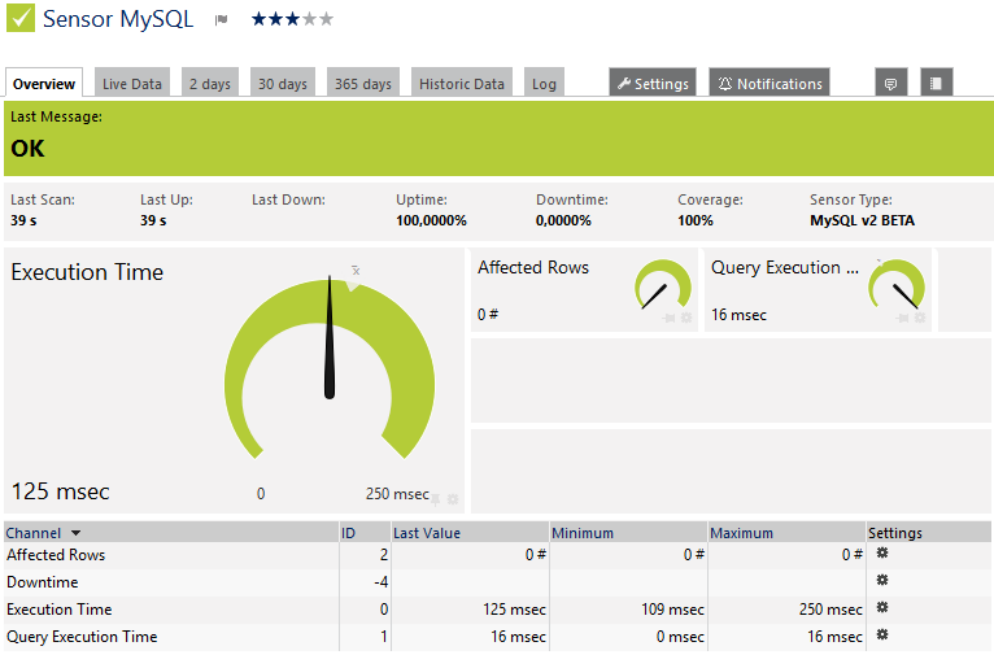
For more general information about settings, please see the **Object Settings** 188 section.

7.8.72 MySQL v2 Sensor

The MySQL v2 sensor monitors a database on a MySQL server and executes a defined query.

It can show the following:

- Execution time of the whole request (including connection buildup, query execution, transaction handling, disconnection)
- Execution time of a given query
- Number of rows which were addressed by the query (including select statements if you process data tables)
- It can also process the data table and show defined values in individual channels.



MySQL v2 Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/mysql.png

Remarks

- Requires 1136 .NET 4.0 on the probe system.
- Define credentials, custom port (if required), and timeout in settings section **Credentials for Database Management Systems** 370 of the parent device, or in the settings of a group or probe above.
- PRTG Manual: **Monitoring Databases** 3120 (includes an example 3121 for channel value selection)
- Knowledge Base: How to setup the SQL v2 sensors in PRTG? Is there a guide?
- Knowledge Base: How can I monitor strings from an SQL database and show a sensor status depending on it?

- Knowledge Base: How can I monitor error tables in SQL databases?
- Your SQL query must be stored in a file on the system of the probe the sensor is created on. If you use it on a remote probe, store the file on the system running the remote probe. In a cluster setup, copy the file to every cluster node.
- Save the SQL script with the query into the **\Custom Sensors\sql\mysql** subfolder of your PRTG installation. See manual section **Data Storage** 3226 for more information about how to find this path.
- This sensor type supports MySQL server version 5.0 or later and might also work with previous versions.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Requirement: .NET Framework

This sensor type requires the Microsoft .NET Framework to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the remote probe 3196. If the framework is missing, you cannot create this sensor.

Required .NET version (with latest updates): .NET 4.0 (Client Profile is sufficient), .NET 4.5, or .NET 4.6.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/60543

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DATABASE SPECIFIC

Database	Enter the name of the MySQL database to which the sensor connects. For example, such a database's name could be MyDatabase. This is a logical entity on the database server where database objects like tables or stored procedures exist. The database name of a MySQL server also reflects a physical directory structure where your database objects are stored. Enter the appropriate string which is the same as you would supply when invoking the mysql.exe admin tool (with the command line switch -p) or after the login with mysql.exe with the command use.

DATA

SQL Query File	Select an SQL script file that includes a valid SQL statement to execute on the server. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew. The script will be executed with every scanning interval. The list contains SQL scripts from the database management system specific **\Custom Sensors\sql** subfolder of your PRTG installation. Store your script there. If used on a remote probe, the file must be stored on the system running the remote probe. If used on a cluster probe, you must store the file on all servers running a cluster node! For more information on how to find this path, please see **Data Storage** 3226 section. By default, there is the demo script **Demo Serveruptime.sql** available that you can use to monitor the uptime of the target server. For example, a correct expression in the file could be: SELECT AVG (UnitPrice) FROM Products. If you want to use transactions, separate the individual steps with semicolons ";". Please be aware that with each request, the full result set will be transferred, so use filters and limits in your query. You can use the following placeholders in your query file to have them replaced by an input parameter: ▪ Microsoft SQL, MySQL, PostgreSQL: **@prtg** ▪ Oracle SQL: **:prtg** ▪ ADO SQL: **?** (question mark) This is useful if you have various SQL sensors with queries that differ in only one parameter.
Use Input Parameter	Define if you want to pass a parameter to your SQL query file. This will replace the placeholder %prtg (Microsoft SQL, MySQL, PostgreSQL), or :prtg (Oracle SQL), or ? (ADO SQL) in the SQL query. Choose between: ▪ **Don't use input parameter (default)**: Execute the SQL query file without using placeholders. ▪ **Use input parameter**: Execute an SQL query file that contains a placeholder. Provide the parameter you want to use in the query below.
Input Parameter	This field is only visible if you choose **Use input parameter** above. Enter the parameter you want to pass to the SQL query file. This parameter replaces the placeholder %prtg or :prtg or ? in the SQL query.

DATA

	You can also use PRTG placeholders for custom sensors (command line parameters) as input parameter, for example, %sensorid or %deviceid. For details, see **Application Programming Interface (API) Definition** 3174. Provide strings as they are and do not surround them with quotation marks. PRTG will correctly insert string parameters into the query automatically.
Use Transaction	Define if you want to use transactions and if they will affect the database content. Choose between: ▪ **Don't use transaction (default)**: No transactions will be executed. ▪ **Use transaction and always rollback**: Choose this option to ensure that no data in the database will be changed by the query. In the SQL query file, separate the single steps of the transaction with semicolons. ▪ **Use transaction and commit on success**: Choose this option to perform changes on the database with the query. The changes will only apply if all execution steps succeed without any errors. In the SQL query file, separate the single steps of the transaction with semicolons.
Data Processing	Define if you want to process data from the database. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew. Choose between: ▪ **Just execute the query**: If you select this option, the sensor will only show information about the number of affected rows and the execution time of the query. Affected rows are rows that were changed somehow with the query (for example, created, deleted, edited). ▪ **Count table rows**: Choose this option if you perform a SELECT statement and want to monitor how many rows of the data table this statement returns. ▪ **Process data table**: Select this option to read and analyze the queried data table. If you select this option, the sensor will count rows with SELECT statements as well.
Handle DBNull in Channel Values as	This setting is only visible if you select **Process data table** above. Define the sensor behavior if DBNull is returned by the query. Choose between: ▪ **Error**: The sensor will show a **Down** status if DBNull is reported. ▪ **Number 0**: The sensor will recognize the result DBNull as a valid value and interpret it as the number 0.

DATA

Select Channel Value by	This setting is only visible if you select **Process data table** above. Define how the desired cell in the database table will be selected. This is necessary to configure the cells that will be used in the sensor channels. Choose between: ▪ **Column number**: The channel value will be determined by using the value in row 0 of the column whose number you specify below. ▪ **Column name**: The channel value will be determined by using the value in row 0 of the column whose name you specify below. ▪ **Row number**: The channel value will be determined by using the value in column 0 of the row whose number you specify below. ▪ **Key value pair**: The channel value will be determined by searching in column 0 for the key you specify below and returning the value in column 1 of the same row where the key value was found. The option you choose here also defines the method to optionally determine a value for the sensor message. For details, see setting **Use Data Table Value in Sensor Message** below. Please see manual section **Monitoring Databases** 3120 for an example 3121 for channel value selection.
Sensor Channel #x	This setting is only visible if you select **Process data table** above. You can define up to 10 different channels for the data processing of this sensor. You have to define at least one data channel if you process the data table, so you will see all available settings for Channel #1 without enabling it manually. For all other possible channels, choose between: ▪ **Disable**: This channel will not be added to the sensor. ▪ **Enable**: This channel will be added to the sensor. Define the settings as described above. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Sensor Channel #x Name	This setting is only visible if you select **Process data table** above. Enter a unique name for the channel. Please enter a string. Channels will be generated dynamically with this name as identifier. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

DATA

Sensor Channel #x Column Number	This setting is only visible if you select **Column number** above. Provide the number of the column which will be used to determine the channel value in row 0. Please enter an integer value.
Sensor Channel #x Column Name	This setting is only visible if you select **Column number** above. Provide the name of the column which will be used to determine the channel value in row 0. Please enter a string.
Sensor Channel #x Row Number	This setting is only visible if you select **Row number** above. Provide the number of the row which will be used to determine the channel value in column 0. Please enter an integer value.
Sensor Channel #x Key	This setting is only visible if you select **Key value pair** above. Provide the key to search for in column 0 of the data table. The value in column 1 of the same row where the key value was found will be used to determine the channel value. Please enter a string.
Sensor Channel #x Mode	This setting is only visible if you select **Process data table** above. Define how to display the determined value in the channel. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew. Choose between: ▪ **Absolute (recommended)**: Shows the value as the sensor retrieves it from the data table. ▪ **Difference**: The sensor calculates and shows the difference between the last and the current value returned from the data table.
Sensor Channel #x Unit	This setting is only visible if you select **Process data table** above. Define the unit of the channel value. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew. Choose between: ▪ BytesBandwidth ▪ BytesMemory ▪ BytesDisk ▪ Temperature ▪ Percent ▪ TimeResponse ▪ TimeSeconds ▪ TimeHours

DATA

- Count
- CPU
- BytesFile
- SpeedDisk
- SpeedNet
- Custom
- Value Lookup

For more information about the available units, please refer to the PRTG Application Programming Interface (API) Definition 3174 for custom sensors.

To use lookups 3183 with this channel, choose **Value Lookup** and select your lookup file below. Do not use **Custom** for using lookups with this sensor!

Sensor Channel #x Custom Unit

This setting is only visible if you select **Custom** above. Define a unit for the channel value. Please enter a string.

Sensor Channel #x Value Lookup

This settings is only visible if you select **Value Lookup** above. Select a lookup 3183 file that you want to use with this channel.

Use Data Table Value in Sensor Message

This setting is only visible if you select **Process data table** above. Define if the sensor message will show a value from the data table. Choose between:

- **Disable**: Do not use a custom sensor message.
- **Enable**: Define a custom sensor message with a defined value of the data table. Define the value selection below.

The method to determine a value for the sensor message is defined in setting **Select Channel Value by** above.

Sensor Message Column Number

This setting is only visible if you select **Column number** and **Use Data Table Value in Sensor Message** above. Enter the number of a column. The sensor message will show the value in row 0 of this column. Please enter an integer value.

Columns and rows start with index 0.

Sensor Message Column Name

This setting is only visible if you select **Column name** and **Use Data Table Value in Sensor Message** above. Enter the name of a column. The sensor message will show the value in row 0 of this column. Please enter a string.

DATA

Columns and rows start with index 0.

Sensor Message Row Number

This setting is only visible if you select **Row number** and **Use Data Table Value in Sensor Message** above. Enter the number of a row. The sensor message will show value in column 0 of this row. Please enter an integer value.

Columns and rows start with index 0.

Sensor Message Key

This setting is only visible if you select **Key value pair** and **Use Data Table Value in Sensor Message** above. Enter a key to search for in column 0 of the data table. The sensor message will show the value in column 1 of the row where the key has been found. Please enter a string.

Columns and rows start with index 0.

Sensor Message

This setting is only visible if you select **Use Data Table Value in Sensor Message** above. Define the sensor message. Please enter a string. Use the placeholder {0} at the position where the value will be added.

Example: **The message is {0}**

If Sensor Message Changes

Define what this sensor will do when the sensor value changes. You can choose between:

- **Ignore changes (default)**: The sensor takes no action on change.
- **Trigger 'change' notification**: The sensor sends an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification 2791 whenever the sensor value changes.

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result**: Do not store the sensor result.

DATA

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section Data Storage 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: How to setup the SQL v2 sensors in PRTG? Is there a guide?

- https://kb.paessler.com/en/topic/70618

Knowledge Base: How can I monitor strings from an SQL database and show a sensor status depending on it?

- https://kb.paessler.com/en/topic/63259

Knowledge Base: How do I monitor the size of a Microsoft SQL server database?

- https://kb.paessler.com/en/topic/18183

Knowledge Base: How can I monitor error tables in SQL databases?

- https://kb.paessler.com/en/topic/70774

Knowledge Base: Which .NET version does PRTG require?

- https://kb.paessler.com/en/topic/60543

PRTG Manual:

- **Monitoring Databases** 3120

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

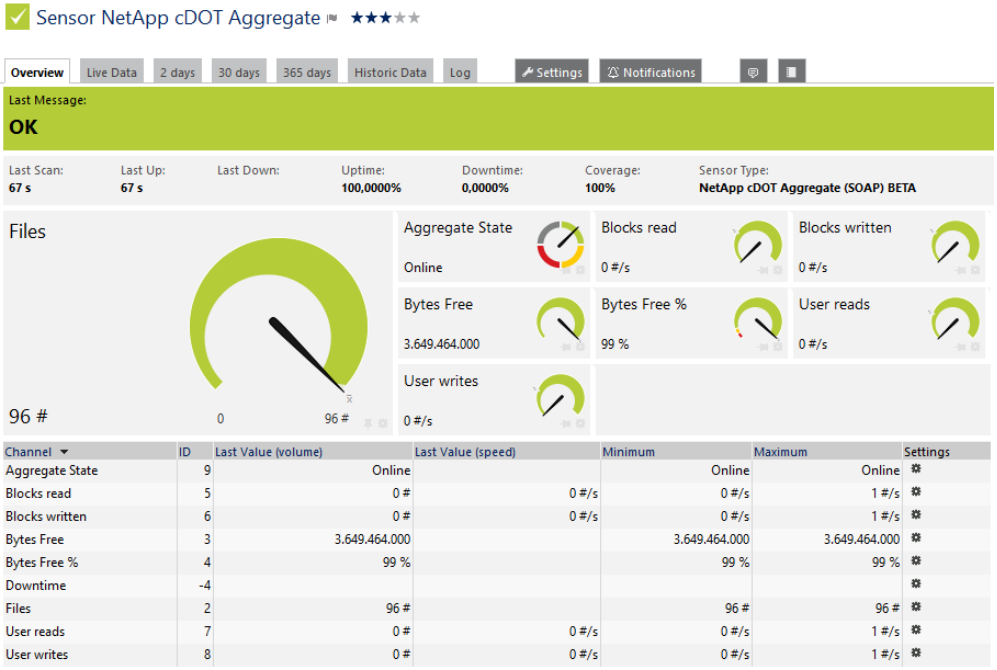
Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.73 NetApp cDOT Aggregate (SOAP) Sensor

The NetApp cDOT Aggregate (SOAP) sensor monitors a NetApp clustered Data ONTAP (cDOT) storage aggregate accessing the cDOT web Application Programming Interface (API) via Simple Object Access Protocol (SOAP). It can show the following:

- Number of files on the aggregate
- Status of the aggregate (online, restrict, offline)
- Read and written blocks per second
- User reads and writes per seconds
- Free bytes in total and percent



NetApp cDOT Aggregate (SOAP) Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/netapp_cdot_aggregate_soap.png

Remarks

- The cDOT user account that you use with this sensor needs access to **ONTAPI** (DATA ONTAP API) so that the sensor can request data from it. The access is enabled by default.
- If API access is disabled, use the following command locally on the cluster console to enable it: services web> modify -vserver clusterd -name ontapi -enabled true
- Read-only user rights are sufficient for the cDOT user account that you use with this sensor for access to ONTAPI. Modify or add this user with the role **readonly** in the console under **Cluster | ClusterX | Configuration | Security | Users**
- This sensor type supports ONTAPI version 1.21 (included in ONTAP version 8.2.x) and ONTAPI version 1.30 (included in ONTAP version 8.3.x), or later.

- Requires .NET 4.5 on the probe system.
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.
- Currently, this sensor type is in beta status. The methods of operating can change at any time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.

Requirement: .NET Framework

This sensor type requires the Microsoft .NET Framework to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the remote probe 3196. If the framework is missing, you cannot create this sensor.

Required .NET version (with latest update): .NET 4.5 or .NET 4.6. Please see the section **More** below for details.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

PRTG will perform a meta scan before you actually add this sensor type and requires basic information for this scan in advance. Provide the requested information in the appearing window. During the scan, PRTG will recognize all items available for monitoring based on your input. The following settings differ in comparison to the sensor's settings page:

Select the aggregates you want to monitor. PRTG creates one sensor for each aggregate you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

NETAPP CDOT SPECIFIC

NetApp cDOT Aggregates	Select all aggregates for which you want to add a sensor. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

NETAPP CDOT CREDENTIALS

Username	Enter a username for access to the NetApp cDOT API. Read-only rights for this cDOT user account are sufficient. Please enter a string.
Password	Enter the password of the user that you entered above for access to the NetApp cDOT API. Please enter a string.

NETAPP CDOT CREDENTIALS

Port	Enter a port number on which you can access the NetApp cDOT API. Please enter an integer value. The default port is **443**.
Transport Type	Define if the connection to the NetApp cDOT API is TLS/SSL secured. Choose between: ▪ **HTTP**: Use an unsecured HTTP connection. ▪ **HTTPS**: Use a TLS/SSL secured connection to the defined port to send the query.
Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).

NETAPP CDOT SPECIFIC

NetApp cDOT Aggregates	Shows the aggregate that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

DEBUG OPTIONS

Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section **Data Storage** 3226.

DEBUG OPTIONS

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply. If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply. If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: Which .NET version does PRTG require?

- https://kb.paessler.com/en/topic/60543

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.74 NetApp cDOT I/O (SOAP) Sensor

The NetApp cDOT I/O (SOAP) sensor monitors input and output operations of a NetApp clustered Data ONTAP (cDOT) storage system accessing the cDOT web Application Programming Interface (API) via Simple Object Access Protocol (SOAP). It can show the following:

- Number of Common Internet File System (CIFS) operations per second
- Disk read and write speed
- Number of FCP operations per second
- FCP read and write speed
- HDD read and write speed
- HTTP operations per second
- Number of internet Small Computer System Interface (iSCSI) operations per second
- iSCSI read and write speed
- Number of iSCSI partner operations per second
- iSCSI partner read and write speed
- Network read and write speed
- Number of Network File System (NFS) operations per second
- SSD read and write speed
- Tape read and write speed

NetApp cDOT I/O (SOAP) Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/netapp_cdot_io_soap.png

Remarks

- The cDOT user account that you use with this sensor needs access to **ONTAPI** (DATA ONTAP API) so that the sensor can request data from it. The access is enabled by default.
- If API access is disabled, use the following command locally on the cluster console to enable it: services web> modify -vserver clusterd -name ontapi -enabled true
- Read-only user rights are sufficient for the cDOT user account that you use with this sensor for access to ONTAPI. Modify or add this user with the role **readonly** in the console under **Cluster | ClusterX | Configuration | Security | Users**
- This sensor type supports ONTAPI version 1.21 (included in ONTAP version 8.2.x) and ONTAPI version 1.30 (included in ONTAP version 8.3.x), or later.

- Requires .NET 4.5 on the probe system.

Requirement: .NET Framework

This sensor type requires the Microsoft .NET Framework to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the remote probe 3196. If the framework is missing, you cannot create this sensor.

Required .NET version (with latest update): .NET 4.5 or .NET 4.6. Please see the section **More** below for details.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

PRTG will perform a meta scan before you actually add this sensor type and requires basic information for this scan in advance. Provide the requested information in the appearing window. During the scan, PRTG will recognize all items available for monitoring based on your input. The following settings differ in comparison to the sensor's settings page:

Select the cDOT system nodes which you want to monitor. PRTG creates one sensor for each node you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

NETAPP CDOT SPECIFIC

NetApp cDOT System Nodes	Select all nodes for which you want to add a sensor. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

NETAPP CDOT CREDENTIALS

Username	Enter a username for access to the NetApp cDOT API. Read-only rights for this cDOT user account are sufficient. Please enter a string.
Password	Enter the password of the user that you entered above for access to the NetApp cDOT API. Please enter a string.
Port	Enter a port number on which you can access the NetApp cDOT API. Please enter an integer value. The default port is **443**.
Transport Type	Define if the connection to the NetApp cDOT API is TLS/SSL secured. Choose between: ▪ **HTTP**: Use an unsecured HTTP connection. ▪ **HTTPS**: Use a TLS/SSL secured connection to the defined port to send the query.

NETAPP CDOT CREDENTIALS

Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).

NETAPP CDOT SPECIFIC

NetApp cDOT System Nodes	Shows the ID of the system node that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

DEBUG OPTIONS

Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section **Data Storage** 3226. You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: Which .NET version does PRTG require?

- https://kb.paessler.com/en/topic/60543

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

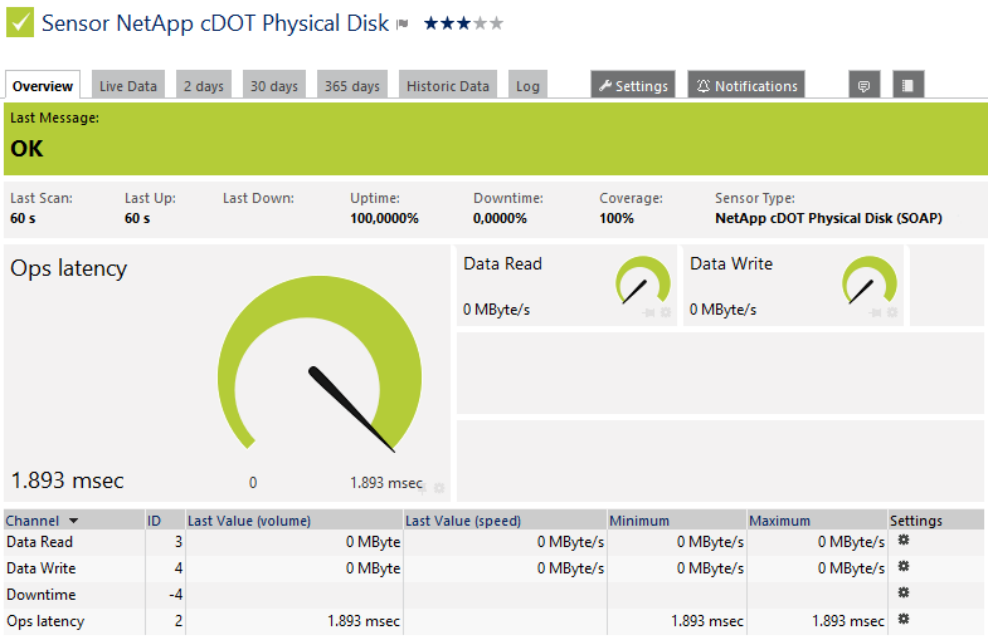
Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.75 NetApp cDOT Physical Disk (SOAP) Sensor

The NetApp cDOT Physical Disk (SOAP) sensor monitors disks of a NetApp clustered Data ONTAP (cDOT) storage system accessing the cDOT web Application Programming Interface (API) via Simple Object Access Protocol (SOAP). It can show the following:

- Latency of operations
- Data read and write speed



NetApp cDOT Physical Disk (SOAP) Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/netapp_cdot_physical_disk_soap.png

Remarks

- The cDOT user account that you use with this sensor needs access to **ONTAPI** (DATA ONTAP API) so that the sensor can request data from it. The access is enabled by default.
- If API access is disabled, use the following command locally on the cluster console to enable it: services web> modify -vserver clusterd -name ontapi -enabled true
- Read-only user rights are sufficient for the cDOT user account that you use with this sensor for access to ONTAPI. Modify or add this user with the role **readonly** in the console under **Cluster | ClusterX | Configuration | Security | Users**
- This sensor type supports ONTAPI version 1.21 (included in ONTAP version 8.2.x) and ONTAPI version 1.30 (included in ONTAP version 8.3.x), or later.
- Requires .NET 4.5 on the probe system.

Requirement: .NET Framework

This sensor type requires the Microsoft .NET Framework to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the remote probe 3196. If the framework is missing, you cannot create this sensor.

Required .NET version (with latest update): .NET 4.5 or .NET 4.6. Please see the section **More** below for details.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

PRTG will perform a meta scan before you actually add this sensor type and requires basic information for this scan in advance. Provide the requested information in the appearing window. During the scan, PRTG will recognize all items available for monitoring based on your input. The following settings differ in comparison to the sensor's settings page:

Select the disks you want to monitor. PRTG creates one sensor for each aggregate you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

NETAPP CDOT SPECIFIC

NetApp cDOT Disks	Select all disks for which you want to add a sensor. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

NETAPP CDOT CREDENTIALS

Username	Enter a username for access to the NetApp cDOT API. Read-only rights for this cDOT user account are sufficient. Please enter a string.
Password	Enter the password of the user that you entered above for access to the NetApp cDOT API. Please enter a string.
Port	Enter a port number on which you can access the NetApp cDOT API. Please enter an integer value. The default port is **443**.
Transport Type	Define if the connection to the NetApp cDOT API is TLS/SSL secured. Choose between: ▪ **HTTP**: Use an unsecured HTTP connection. ▪ **HTTPS**: Use a TLS/SSL secured connection to the defined port to send the query.

NETAPP CDOT CREDENTIALS

Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).

NETAPP CDOT SPECIFIC

NetApp cDOT Disk	Shows the disk that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

DEBUG OPTIONS

Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section **Data Storage** 3226. You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: Which .NET version does PRTG require?

- https://kb.paessler.com/en/topic/60543

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

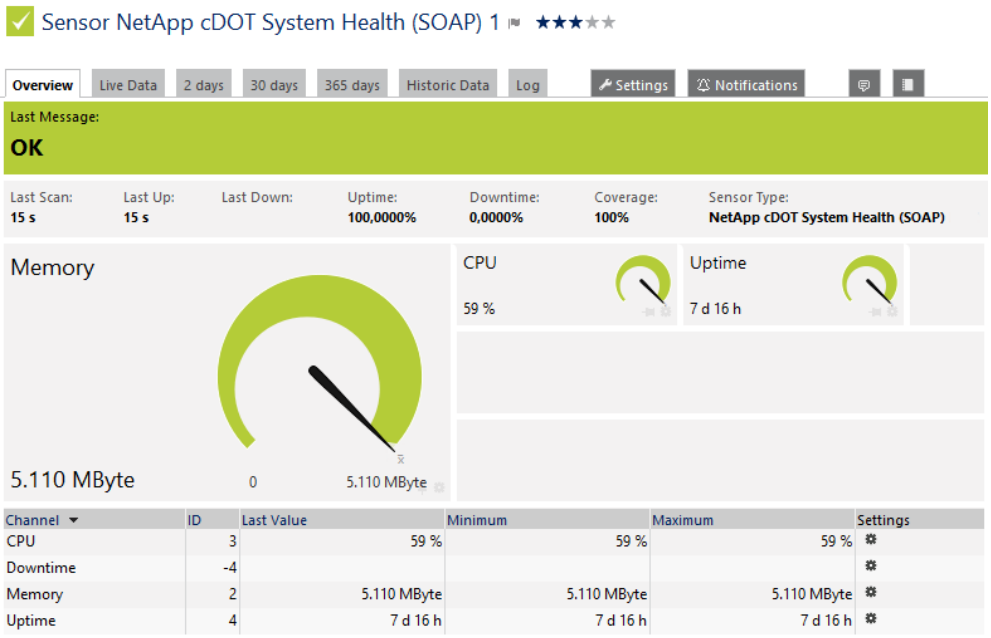
Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.76 NetApp cDOT System Health (SOAP) Sensor

The NetApp cDOT System Health (SOAP) sensor monitors the health of a NetApp clustered Data ONTAP (cDOT) storage system accessing the cDOT web Application Programming Interface (API) via Simple Object Access Protocol (SOAP). It can show the following:

- Memory usage
- CPU load
- Uptime



NetApp cDOT System Health (SOAP) Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/netapp_cdot_system_health_soap.png

Remarks

- The cDOT user account that you use with this sensor needs access to **ONTAPI** (DATA ONTAP API) so that the sensor can request data from it. The access is enabled by default.
- If API access is disabled, use the following command locally on the cluster console to enable it: services web> modify -vserver clusterd -name ontapi -enabled true
- Read-only user rights are sufficient for the cDOT user account that you use with this sensor for access to ONTAPI. Modify or add this user with the role **readonly** in the console under **Cluster | ClusterX | Configuration | Security | Users**
- This sensor type supports ONTAPI version 1.21 (included in ONTAP version 8.2.x) and ONTAPI version 1.30 (included in ONTAP version 8.3.x), or later.
- Requires .NET 4.5 on the probe system.

Requirement: .NET Framework

This sensor type requires the Microsoft .NET Framework to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the remote probe 3196. If the framework is missing, you cannot create this sensor.

Required .NET version (with latest update): .NET 4.5 or .NET 4.6. Please see the section **More** below for details.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

PRTG will perform a meta scan before you actually add this sensor type and requires basic information for this scan in advance. Provide the requested information in the appearing window. During the scan, PRTG will recognize all items available for monitoring based on your input. The following settings differ in comparison to the sensor's settings page:

Select the cDOT system nodes which you want to monitor. PRTG creates one sensor for each node you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

NETAPP CDOT SPECIFIC

NetApp cDOT System Nodes	Select the nodes for which you want to add a sensor. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

NETAPP CDOT CREDENTIALS

Username	Enter a username for access to the NetApp cDOT API. Read-only rights for this cDOT user account are sufficient. Please enter a string.
Password	Enter the password of the user that you entered above for access to the NetApp cDOT API. Please enter a string.
Port	Enter a port number on which you can access the NetApp cDOT API. Please enter an integer value. The default port is **443**.
Transport Type	Define if the connection to the NetApp cDOT API is TLS/SSL secured. Choose between: ▪ **HTTP**: Use an unsecured HTTP connection. ▪ **HTTPS**: Use a TLS/SSL secured connection to the defined port to send the query.

NETAPP CDOT CREDENTIALS

Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).

NETAPP CDOT SPECIFIC

NetApp cDOT System Nodes	Shows the ID of the system node that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

DEBUG OPTIONS

Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section **Data Storage** 3226. You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: Which .NET version does PRTG require?

- https://kb.paessler.com/en/topic/60543

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.77 NetFlow V5 Sensor

The NetFlow V5 sensor receives traffic data from a NetFlow V5 compatible device and shows the traffic by type. Ensure the sensor matches the NetFlow version your device is exporting! There are several filter options available to divide traffic into different channels.

This sensor can show the following traffic types in kbit per second:

- Chat (IRC, AIM)
- Citrix
- FTP/P2P (file transfer)
- Infrastructure (network services: DHCP, DNS, Ident, ICMP, SNMP)
- Mail (mail traffic: IMAP, POP3, SMTP)
- NetBIOS
- Remote control (RDP, SSH, Telnet, VNC)
- WWW (web traffic: HTTP, HTTPS)
- Total traffic
- Other protocols (other UDP and TCP traffic)

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

Channel	ID	Last Value (volume)	Last Value (speed)	Minimum	Maximum	Settings
Downtime	-4					
Other	0	0 KByte	0 kbit/s			
Total	-1	103 KByte	14 kbit/s	0 kbit/s	35 kbit/s	
Various	3009	69 KByte	9 kbit/s	0 kbit/s	23 kbit/s	
WWW	3001	34 KByte	5 kbit/s	0 kbit/s	12 kbit/s	

NetFlow V5 Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/netflow_v5.png

Remarks

- You must enable NetFlow export of the respective version on the monitored device for this sensor to work. The device must send the flow data stream to the IP address of the PRTG probe system on which the sensor is set up (either a local or remote probe).
- This sensor type cannot be used in cluster mode. You can set it up on a local probe or remote probe only, not on a cluster probe.

- Knowledge Base: How can I change the default groups and channels for xFlow and Packet Sniffer sensors?
- Knowledge Base: What is the Active Flow Timeout in Flow sensors?
- For a general introduction to the technology behind flow monitoring, please see manual section **Monitoring Bandwidth via Flows** 3099.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.

BASIC SENSOR SETTINGS

Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

NETFLOW SPECIFIC SETTINGS

Receive NetFlow Packets on UDP Port	Enter the UDP port number on which the flow packets are received. It must match the one you have configured in the NetFlow export options of your hardware router device. Please enter an integer value. When configuring export, make sure you select the appropriate NetFlow version for this sensor.
Sender IP	Enter the IP address of the sending device you want to receive the NetFlow from. Enter an IP address to receive data from a specific device only, or leave the field empty to receive data from any device on the specified port.
Receive NetFlow Packets on IP	Select the IP address(es) on which PRTG listens to NetFlow packets. The list of IP addresses you see here is specific to your setup. To select an IP address, add a check mark in front of the respective line. You can also select and deselect all items by using the check box in the table head. The IP address selected here must match the one you have configured in the NetFlow export options of your hardware router device. When configuring export, make sure you select the appropriate NetFlow version for this sensor.
Active Flow Timeout (Minutes)	Enter a time span in minutes after which new flow data must be received. If the timeout is reached and no new data was received during this time, the sensor switches to an **Unknown** status. Please enter an integer value. We recommend that you set the timeout one minute longer than the respective timeout configured in your hardware router device. The maximum timeout is 60 minutes. If you set this value too low, flow information might be lost! For more details, please see this Knowledge Base article: What is the Active Flow Timeout in Flow sensors?

NETFLOW SPECIFIC SETTINGS

If the target device sends incorrect time information that results in wrong monitoring data, please try to use 0 as active flow timeout. This will ignore the start and stop information of a flow as provided by the device and account all data to the current point in time. It might result in spikes but all data will be captured.

Sampling Mode

Define if you want to use the sampling mode. This setting must accord to the setting in the flow exporter. Choose between:

- **Off**: The standard flow will be used.
- **On**: Switch into sampling mode and specify the sampling rate below.

Sampling Rate

This field is only visible when sampling mode is **On** above. Enter a number that matches the sampling rate in your exporter device. If the number is different, monitoring results will be incorrect. Please enter an integer value.

Log Stream Data to Disk (for Debugging)

Define if you want the probe to write a logfile of the stream and packet data to the data folder (see **Data Storage** 3226). Choose between:

- **None (recommended)**: Do not write additional logfiles. Recommended for normal use cases.
- **Only for the 'Other' channel**: Only write logfiles of data that is not filtered otherwise and therefore accounted to the default **Other** channel.
- **All stream data**: Write logfiles for all data received.

Use with caution! When enabled, huge data files can be created. Please use for a short time and for debugging purposes only.

CHANNEL CONFIGURATION

Channel Selection

Define the categories the sensor accounts the traffic to. There are different groups of traffic available. Choose between:

- **Web**: Internet web traffic.
- **File Transfer**: Traffic caused by FTP.
- **Mail**: Internet mail traffic.
- **Chat**: Traffic caused by chat and instant messaging.

CHANNEL CONFIGURATION

- **Remote Control**: Traffic caused by remote control applications, such as RDP, SSH, Telnet, and VNC.
- **Infrastructure**: Traffic caused by network services, such as DHCP, DNS, Ident, ICMP, and SNMP.
- **NetBIOS**: Traffic caused by NetBIOS communication.
- **Citrix**: Traffic caused by Citrix applications.
- **Other Protocols**: Traffic caused by various other protocols via UDP and TCP.

For each traffic group, you can select how many channels will be used for each group, that is, how detailed the sensor divides the traffic. For each group, choose between:

- **No**: Do not account traffic of this group in its own channel. All traffic of this group is accounted to the default channel named **Other**.
- **Yes**: Count all traffic of this group and summarize it into one channel.
- **Detail**: Count all traffic of this group and further divide it into different channels. The traffic appears in several channels as shown in the **Content** column.
  Extensive use of this option can cause load problems on your probe system. We recommend setting specific, well-chosen filters for the data you really want to analyze.

You can change the default configuration for groups and channels. For details, please see this Knowledge Base article: How can I change the default groups and channels for xFlow and Packet Sniffer sensors?

FILTERING

Include Filter	Define if you want to filter any traffic. If you leave this field empty, all traffic will be included. To include specific traffic only, define filters using a special syntax. For detailed information, please see **Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors** 3175 section.
Exclude Filter	First, the filters defined in the **Include Filter** field are considered. From this subset, you can explicitly exclude traffic, using the same syntax. For detailed information, please see **Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors** 3175 section.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

PRIMARY TOPLIST

Primary Toplist	Define which will be your primary toplist. It will be shown in maps when adding a toplist object. Choose from: ▪ **Top Talkers** ▪ **Top Connections** ▪ **Top Protocols** ▪ [Any custom toplists you have added]

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

Toplists

For all flow and packet sniffer sensors there are **Toplists** available on the **Overview** tab of a sensor's detail page. Using toplists, you can review traffic data of small time periods in great detail. For more information, please see **Toplists** 2806 section.

More

Paessler Website: Paessler NetFlow Testers

- https://www.paessler.com/tools/netflowtester

Knowledge Base: How can I change the default groups and channels for xFlow and Packet Sniffer sensors?

- https://kb.paessler.com/en/topic/60203

Knowledge Base: Where is the volume line in graphs?

- https://kb.paessler.com/en/topic/61272

Knowledge Base: What is the Active Flow Timeout in Flow sensors?

- https://kb.paessler.com/en/topic/66485

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

Related Topics

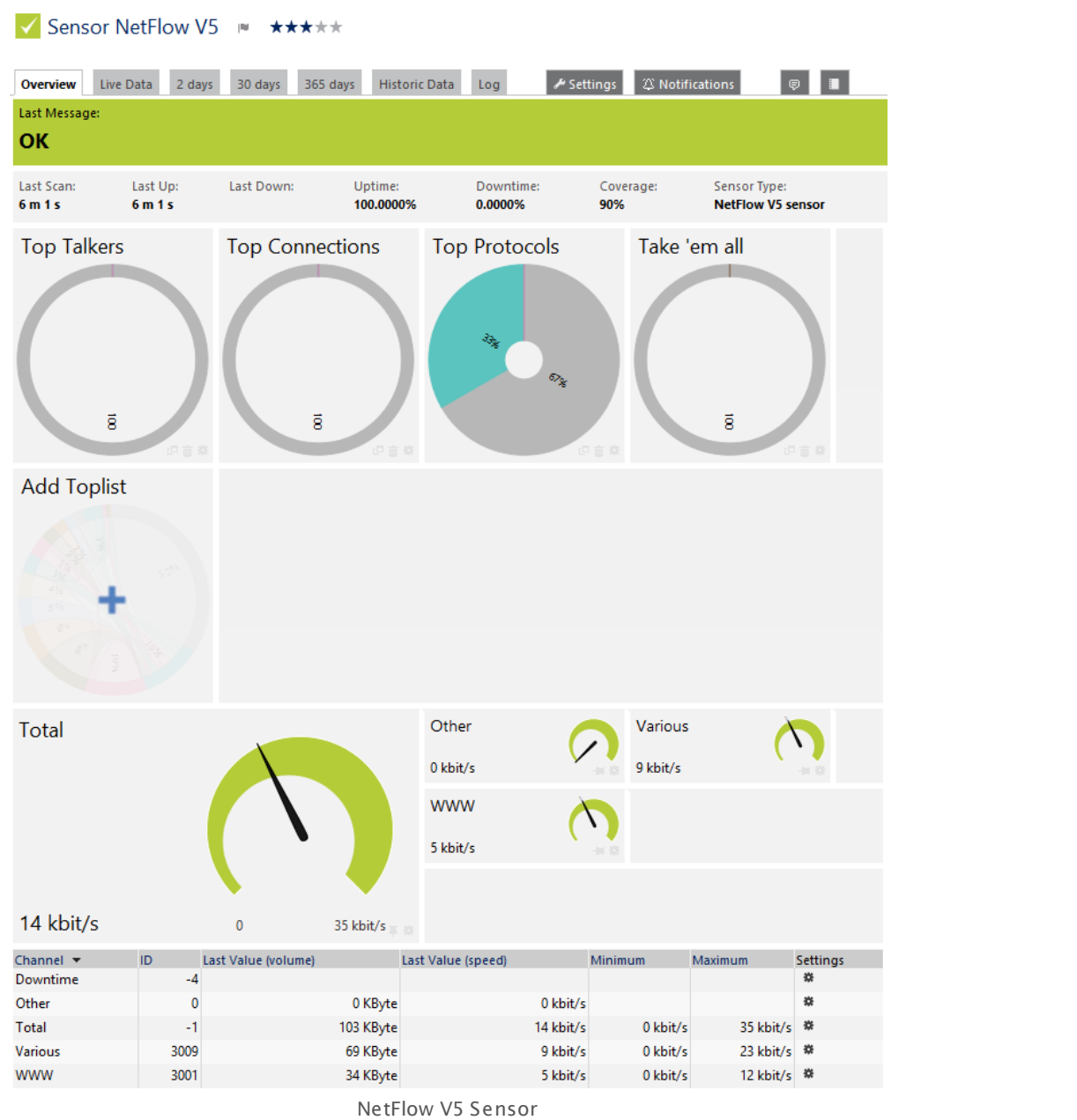
- **Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors** 3175
- **Channel Defintions for xFlow, IPFIX, and Packet Sniffer Sensors** 3180

7.8.78 NetFlow V5 (Custom) Sensor

The NetFlow V5 (Custom) sensor receives traffic data from a NetFlow V5 compatible device and shows the traffic by type. Please make sure the sensor matches the NetFlow version your device is exporting! In this custom sensor, you can define your own channel definitions to divide traffic into different channels.

- This sensor can show traffic by type individually according to your needs.

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



NetFlow V5 Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/netflow_v5.png

Remarks

- You must enable NetFlow export of the respective version on the monitored device for this sensor to work. The device must send the flow data stream to the IP address of the PRTG probe system on which the sensor is set up (either a local or remote probe).
- This sensor type cannot be used in cluster mode. You can set it up on a local probe or remote probe only, not on a cluster probe.
- Knowledge Base: What is the Active Flow Timeout in Flow sensors?
- This sensor does not support more than 50 channels officially.
- For a general introduction to the technology behind flow monitoring, please see manual section **Monitoring Bandwidth via Flows**.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Limited to 50 Sensor Channels

PRTG does not support more than 50 sensor channels officially. Depending on the data used with this sensor type, you might exceed the maximum number of supported sensor channels. In this case, PRTG will try to display all sensor channels. However, please be aware that you will experience limited usability and performance.

Add Sensor

The **Add Sensor** dialog appears when you manually add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

NETFLOW SPECIFIC SETTINGS

Receive NetFlow Packets on UDP Port	Enter the UDP port number on which the flow packets are received. It must match the one you have configured in the NetFlow export options of your hardware router device. Please enter an integer value. ⓘ When configuring export, make sure you select the appropriate NetFlow version for this sensor.
Sender IP	Enter the IP address of the sending device you want to receive the NetFlow from. Enter an IP address to receive data from a specific device only, or leave the field empty to receive data from any device on the specified port.
Receive NetFlow Packets on IP	Select the IP address(es) on which PRTG listens to NetFlow packets. The list of IP addresses you see here is specific to your setup. To select an IP address, add a check mark in front of the respective line. You can also select and deselect all items by using the check box in the table head. The IP address you select here must match the one you have configured in the NetFlow export options of your hardware router device.

NETFLOW SPECIFIC SETTINGS

When configuring export, please make sure you select the appropriate NetFlow version for this sensor.

Active Flow Timeout (Minutes)

Enter a time span in minutes after which new flow data must be received. If the timeout is reached and no new data was received during this time, the sensor switches to an **Unknown** status. Please enter an integer value.

We recommend that you set the timeout one minute longer than the respective timeout configured in your hardware router device. The maximum timeout is 60 minutes.

If you set this value too low, flow information might be lost!

For more details, please see this Knowledge Base article: What is the Active Flow Timeout in Flow sensors?

If the target device sends incorrect time information that results in wrong monitoring data, please try to use 0 as active flow timeout. This will ignore the start and stop information of a flow as provided by the device and account all data to the current point in time. It might result in spikes but all data will be captured.

Sampling Mode

Define if you want to use the sampling mode. This setting must accord to the setting in the flow exporter. Choose between:

- **Off**: The standard flow will be used.
- **On**: Switch into sampling mode and specify the sampling rate below.

Sampling Rate

This field is only visible when sampling mode is **On** above. Enter a number that matches the sampling rate in your device. If the number is different, monitoring results will be incorrect. Please enter an integer value.

Channel Definition

Please enter a channel definition to divide the traffic into different channels. Write each definition in one line. For detailed information, please see **Channel Definitions for xFlow, IPFIX, and Packet Sniffer Sensors** 3180 section. All traffic for which no channel is defined will be accounted to the default channel named **Other**.

Extensive use of many filters can cause load problems on your probe system. We recommend defining specific, well-chosen filters for the data you really want to analyze.

NETFLOW SPECIFIC SETTINGS

Log Stream Data to Disk (for Debugging)

Define if you want the probe to write a logfile of the stream and packet data to the data folder (see **Data Storage** 3226). Choose between:

- **None (recommended)**: Do not write additional logfiles. Recommended for normal use cases.
- **Only for the 'Other' channel**: Only write logfiles of data that is not filtered otherwise and therefore accounted to the default **Other** channel.
- **All stream data**: Write logfiles for all data received.

Use with caution! When enabled, huge data files can be created. Please use for a short time and for debugging purposes only.

FILTERING

Include Filter

Define if you want to filter any traffic. If you leave this field empty, all traffic will be included. To include specific traffic only, define filters using a special syntax. For detailed information, please see **Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors** 3175 section.

Exclude Filter

First, the filters defined in the **Include Filter** field are considered. From this subset, you can explicitly exclude traffic, using the same syntax. For detailed information, please see **Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors** 3175 section.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

PRIMARY TOPLIST

Primary Toplist	Define which will be your primary toplist. It will be shown in maps when adding a toplist object. Choose from: ▪ **Top Talkers** ▪ **Top Connections** ▪ **Top Protocols** ▪ [Any custom toplists you have added]

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

Toplists

For all flow and packet sniffer sensors there are **Toplists** available on the **Overview** tab of a sensor's detail page. Using toplists, you can review traffic data of small time periods in great detail. For more information, please see **Toplists** 2806 section.

More

Knowledge Base: Where is the volume line in graphs?

- https://kb.paessler.com/en/topic/61272

Knowledge Base: What is the Active Flow Timeout in Flow sensors?

- https://kb.paessler.com/en/topic/66485

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

Related Topics

- **Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors** 3175
- **Channel Defintions for xFlow, IPFIX, and Packet Sniffer Sensors** 3180

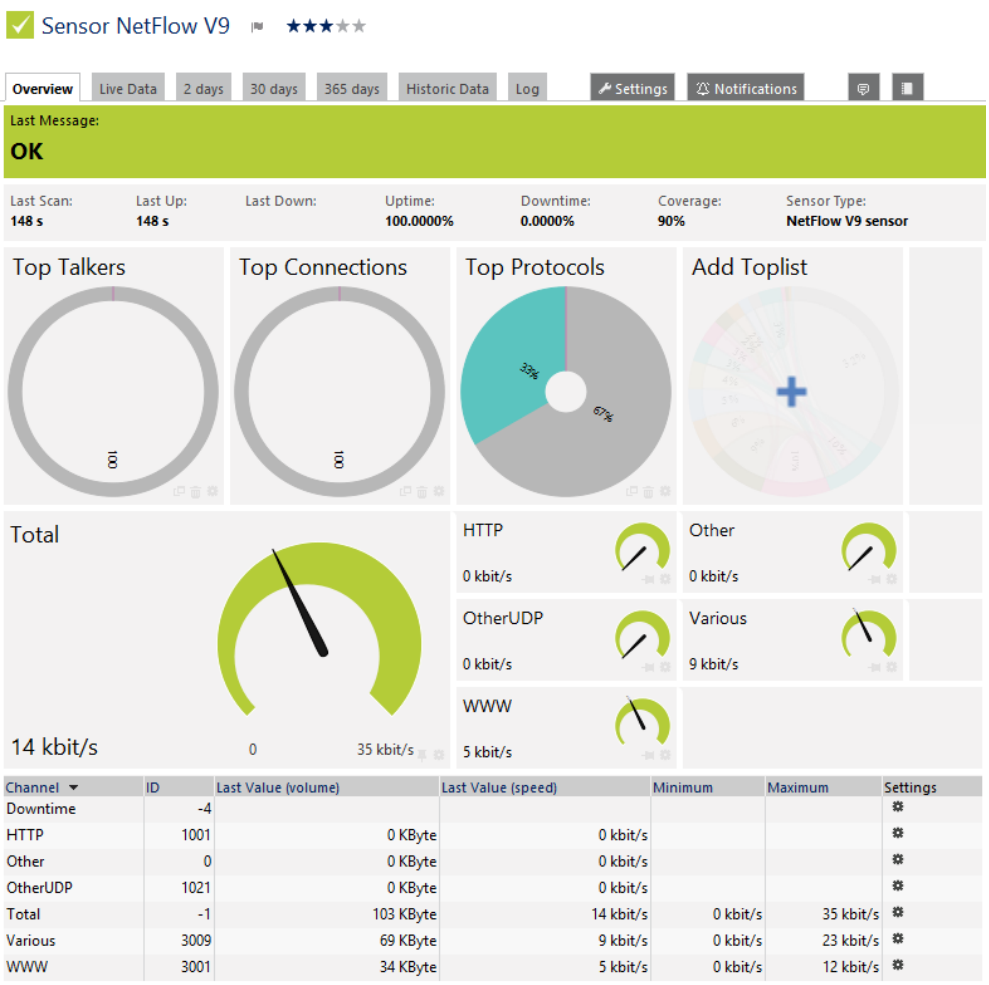
7.8.79 NetFlow V9 Sensor

The NetFlow V9 sensor receives traffic data from a NetFlow V9 compatible device and shows the traffic by type. Please make sure the sensor matches the NetFlow version your device is exporting! There are several filter options available to divide traffic into different channels.

This sensor can show the following traffic types in kbit per second:

- Chat (IRC, AIM)
- Citrix
- FTP/P2P (file transfer)
- Infrastructure (network services: DHCP, DNS, Ident, ICMP, SNMP)
- Mail (mail traffic: IMAP, POP3, SMTP)
- NetBIOS
- Remote control (RDP, SSH, Telnet, VNC)
- WWW (web traffic: HTTP, HTTPS)
- Total traffic
- Other protocols (other UDP and TCP traffic)

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



NetFlow V9 Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/netflow_v9.png

Remarks

- You must enable NetFlow export of the respective version on the monitored device for this sensor to work. The device must send the flow data stream to the IP address of the PRTG probe system on which the sensor is set up (either a local or remote probe).
- This sensor type cannot be used in cluster mode. You can set it up on a local probe or remote probe only, not on a cluster probe.
- Knowledge Base: How can I change the default groups and channels for xFlow and Packet Sniffer sensors?
- Knowledge Base: What is the Active Flow Timeout in Flow sensors?
- For a general introduction to the technology behind flow monitoring, please see manual section **Monitoring Bandwidth via Flows** 3099.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

NETFLOW SPECIFIC SETTINGS

Receive NetFlow Packets on UDP Port	Enter the UDP port number on which the flow packets are received. It must match the one you have configured in the NetFlow export options of your hardware router device. Please enter an integer value. When configuring export, make sure you select the appropriate NetFlow version for this sensor.
Sender IP	Enter the IP address of the sending device you want to receive the NetFlow from. Enter an IP address to receive data from a specific device only, or leave the field empty to receive data from any device on the specified port.
Receive NetFlow Packets on IP	Select the IP address(es) on which PRTG listens to NetFlow packets. The list of IP addresses you see here is specific to your setup. To select an IP address, add a check mark in front of the respective line. You can also select and deselect all items by using the check box in the table head. The IP address selected here must match the one you have configured in the NetFlow export options of your hardware router device. When configuring export, make sure you select the appropriate NetFlow version for this sensor.
Active Flow Timeout (Minutes)	Enter a time span in minutes after which new flow data must be received. If the timeout is reached and no new data was received during this time, the sensor switches to an **Unknown** status. Please enter an integer value. We recommend that you set the timeout one minute longer than the respective timeout configured in your hardware router device. The maximum timeout is 60 minutes. If you set this value too low, flow information might be lost! For more details, please see this Knowledge Base article: What is the Active Flow Timeout in Flow sensors? If the target device sends incorrect time information that results in wrong monitoring data, please try to use 0 as active flow timeout. This will ignore the start and stop information of a flow as provided by the device and account all data to the current point in time. It might result in spikes but all data will be captured.
Sampling Mode	Define if you want to use the sampling mode. This setting must accord to the setting in the flow exporter. Choose between: ▪ **Off**: The standard flow will be used.

NETFLOW SPECIFIC SETTINGS

- **On**: Switch into sampling mode and specify the sampling rate below.

Sampling Rate

This field is only visible when sampling mode is **On** above. Enter a number that matches the sampling rate in your exporter device. If the number is different, monitoring results will be incorrect. Please enter an integer value.

Log Stream Data to Disk (for Debugging)

Define if you want the probe to write a logfile of the stream and packet data to the data folder (see **Data Storage** 3226). Choose between:

- **None (recommended)**: Do not write additional logfiles. Recommended for normal use cases.
- **Only for the 'Other' channel**: Only write logfiles of data that is not filtered otherwise and therefore accounted to the default **Other** channel.
- **All stream data**: Write logfiles for all data received.

Use with caution! When enabled, huge data files can be created. Please use for a short time and for debugging purposes only.

CHANNEL CONFIGURATION

Channel Selection

Define the categories the sensor accounts the traffic to. There are different groups of traffic available. Choose between:

- **Web**: Internet web traffic.
- **File Transfer**: Traffic caused by FTP.
- **Mail**: Internet mail traffic.
- **Chat**: Traffic caused by chat and instant messaging.
- **Remote Control**: Traffic caused by remote control applications, such as RDP, SSH, Telnet, and VNC.
- **Infrastructure**: Traffic caused by network services, such as DHCP, DNS, Ident, ICMP, and SNMP.
- **NetBIOS**: Traffic caused by NetBIOS communication.
- **Citrix**: Traffic caused by Citrix applications.
- **Other Protocols**: Traffic caused by various other protocols via UDP and TCP.

CHANNEL CONFIGURATION

For each traffic group, you can select how many channels will be used for each group, that is, how detailed the sensor divides the traffic. For each group, choose between:

- **No**: Do not account traffic of this group in its own channel. All traffic of this group is accounted to the default channel named **Other**.
- **Yes**: Count all traffic of this group and summarize it into one channel.
- **Detail**: Count all traffic of this group and further divide it into different channels. The traffic appears in several channels as shown in the **Content** column.
  Extensive use of this option can cause load problems on your probe system. We recommend setting specific, well-chosen filters for the data you really want to analyze.

You can change the default configuration for groups and channels. For details, please see this Knowledge Base article: How can I change the default groups and channels for xFlow and Packet Sniffer sensors?

FILTERING

Include Filter	Define if you want to filter any traffic. If you leave this field empty, all traffic will be included. To include specific traffic only, define filters using a special syntax. For detailed information, please see **Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors** 3175 section.
Exclude Filter	First, the filters defined in the **Include Filter** field are considered. From this subset, you can explicitly exclude traffic, using the same syntax. For detailed information, please see **Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors** 3175 section.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

SENSOR DISPLAY

	You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

PRIMARY TOPLIST

Primary Toplist	Define which will be your primary toplist. It will be shown in maps when adding a toplist object. Choose from: ▪ **Top Talkers** ▪ **Top Connections** ▪ **Top Protocols** ▪ [Any custom toplists you have added]

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply. If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply. If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

Toplists

For all flow and packet sniffer sensors there are **Toplists** available on the **Overview** tab of a sensor's detail page. Using toplists, you can review traffic data of small time periods in great detail. For more information, please see **Toplists** 2806 section.

More

Paessler Website: Paessler NetFlow Testers

- https://www.paessler.com/tools/netflowtester

Knowledge Base: How can I change the default groups and channels for xFlow and Packet Sniffer sensors?

- https://kb.paessler.com/en/topic/60203

Knowledge Base: Where is the volume line in graphs?

- https://kb.paessler.com/en/topic/61272

Knowledge Base: What is the Active Flow Timeout in Flow sensors?

- https://kb.paessler.com/en/topic/66485

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

Related Topics

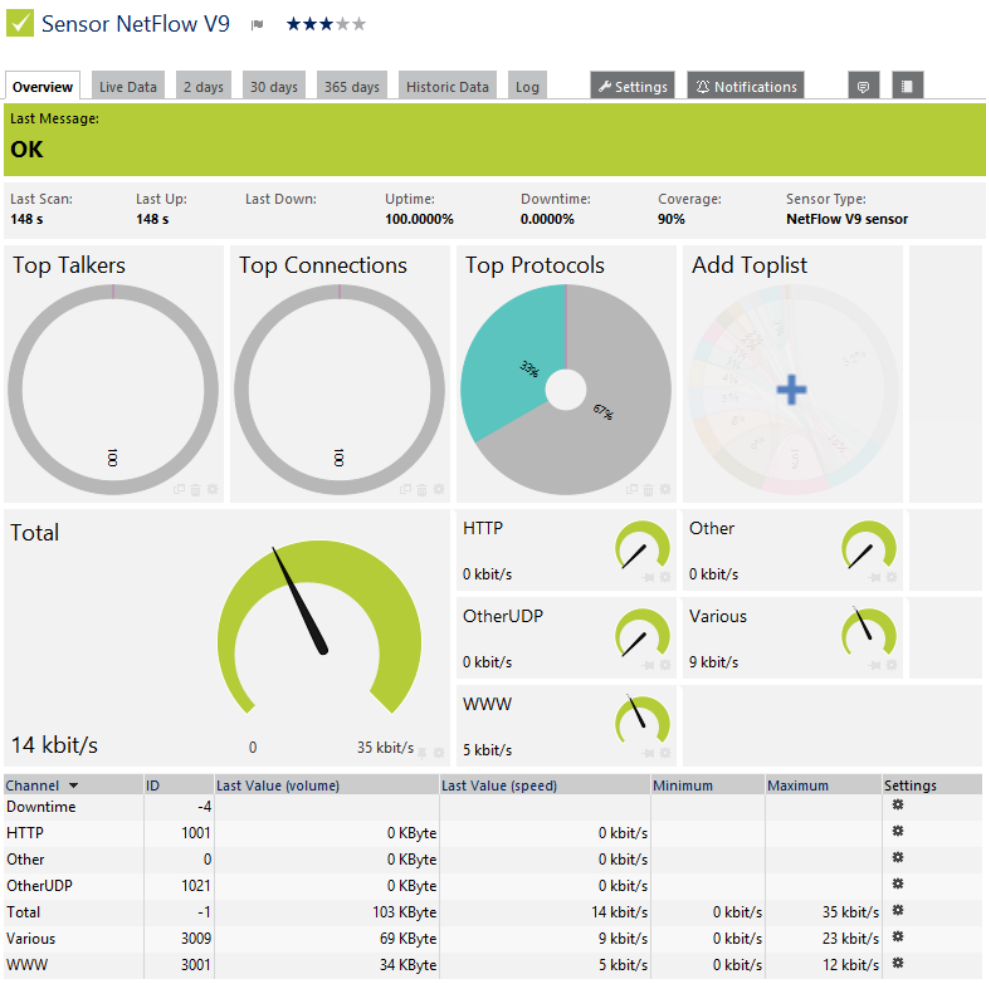
- **Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors** 3175
- **Channel Defintions for xFlow, IPFIX, and Packet Sniffer Sensors** 3180

7.8.80 NetFlow V9 (Custom) Sensor

The NetFlow V9 (Custom) sensor receives traffic data from a NetFlow V9 compatible device and shows the traffic by type. Please make sure the sensor matches the NetFlow version your device is exporting! In this custom sensor, you can define your own channel definitions to divide traffic into different channels.

- This sensor can show traffic by type individually according to your needs.

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Channel	ID	Last Value (volume)	Last Value (speed)	Minimum	Maximum	Settings
Downtime	-4					
HTTP	1001	0 KByte	0 kbit/s			
Other	0	0 KByte	0 kbit/s			
OtherUDP	1021	0 KByte	0 kbit/s			
Total	-1	103 KByte	14 kbit/s	0 kbit/s	35 kbit/s	
Various	3009	69 KByte	9 kbit/s	0 kbit/s	23 kbit/s	
WWW	3001	34 KByte	5 kbit/s	0 kbit/s	12 kbit/s	

NetFlow V9 Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/netflow_v9.png

Remarks

- You must enable NetFlow export of the respective version on the monitored device for this sensor to work. The device must send the flow data stream to the IP address of the PRTG probe system on which the sensor is set up (either a local or remote probe).

- This sensor type cannot be used in cluster mode. You can set it up on a local probe or remote probe only, not on a cluster probe.
- Knowledge Base: What is the Active Flow Timeout in Flow sensors?
- This sensor does not support more than 50 channels 1243 officially.
- For a general introduction to the technology behind flow monitoring, please see manual section **Monitoring Bandwidth via Flows** 3099.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Limited to 50 Sensor Channels

PRTG does not support more than 50 sensor channels officially. Depending on the data used with this sensor type, you might exceed the maximum number of supported sensor channels. In this case, PRTG will try to display all sensor channels. However, please be aware that you will experience limited usability and performance.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	Enter one or more **Tags**, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

NETFLOW SPECIFIC SETTINGS

Receive NetFlow Packets on UDP Port	Enter the UDP port number on which the flow packets are received. It must match the one you have configured in the NetFlow export options of your hardware router device. Please enter an integer value. When configuring export, make sure you select the appropriate NetFlow version for this sensor.
Sender IP	Enter the IP address of the sending device you want to receive the NetFlow from. Enter an IP address to receive data from a specific device only, or leave the field empty to receive data from any device on the specified port.
Receive NetFlow Packets on IP	Select the IP address(es) on which PRTG listens to NetFlow packets. The list of IP addresses you see here is specific to your setup. To select an IP address, add a check mark in front of the respective line. You can also select and deselect all items by using the check box in the table head. The IP address you select here must match the one you have configured in the NetFlow export options of your hardware router device. When configuring export, please make sure you select the appropriate NetFlow version for this sensor.
Active Flow Timeout (Minutes)	Enter a time span in minutes after which new flow data must be received. If the timeout is reached and no new data was received during this time, the sensor switches to an **Unknown** status. Please enter an integer value. We recommend that you set the timeout one minute longer than the respective timeout configured in your hardware router device. The maximum timeout is 60 minutes.

NETFLOW SPECIFIC SETTINGS

If you set this value too low, flow information might be lost!

For more details, please see this Knowledge Base article: What is the Active Flow Timeout in Flow sensors?

If the target device sends incorrect time information that results in wrong monitoring data, please try to use 0 as active flow timeout. This will ignore the start and stop information of a flow as provided by the device and account all data to the current point in time. It might result in spikes but all data will be captured.

Sampling Mode	Define if you want to use the sampling mode. This setting must accord to the setting in the flow exporter. Choose between: ▪ **Off**: The standard flow will be used. ▪ **On**: Switch into sampling mode and specify the sampling rate below.
Sampling Rate	This field is only visible when sampling mode is **On** above. Enter a number that matches the sampling rate in your device. If the number is different, monitoring results will be incorrect. Please enter an integer value.
Channel Definition	Please enter a channel definition to divide the traffic into different channels. Write each definition in one line. For detailed information, please see **Channel Definitions for xFlow, IPFIX, and Packet Sniffer Sensors** 3180 section. All traffic for which no channel is defined will be accounted to the default channel named **Other**. Extensive use of many filters can cause load problems on your probe system. We recommend defining specific, well-chosen filters for the data you really want to analyze.
Log Stream Data to Disk (for Debugging)	Define if you want the probe to write a logfile of the stream and packet data to the data folder (see **Data Storage** 3226). Choose between: ▪ **None (recommended)**: Do not write additional logfiles. Recommended for normal use cases. ▪ **Only for the 'Other' channel**: Only write logfiles of data that is not filtered otherwise and therefore accounted to the default **Other** channel. ▪ **All stream data**: Write logfiles for all data received.

NETFLOW SPECIFIC SETTINGS

Use with caution! When enabled, huge data files can be created. Please use for a short time and for debugging purposes only.

FILTERING

Include Filter

Define if you want to filter any traffic. If you leave this field empty, all traffic will be included. To include specific traffic only, define filters using a special syntax. For detailed information, please see **Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors** 3175 section.

Exclude Filter

First, the filters defined in the **Include Filter** field are considered. From this subset, you can explicitly exclude traffic, using the same syntax. For detailed information, please see **Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors** 3175 section.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.
- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

SENSOR DISPLAY

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

PRIMARY TOPLIST

Primary Toplist	Define which will be your primary toplist. It will be shown in maps when adding a toplist object. Choose from: ▪ **Top Talkers** ▪ **Top Connections** ▪ **Top Protocols** ▪ [Any custom toplists you have added]

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

SCANNING INTERVAL

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

Toplists

For all flow and packet sniffer sensors there are **Toplists** available on the **Overview** tab of a sensor's detail page. Using toplists, you can review traffic data of small time periods in great detail. For more information, please see **Toplists** 2806 section.

More

Knowledge Base: Where is the volume line in graphs?

- https://kb.paessler.com/en/topic/61272

Knowledge Base: What is the Active Flow Timeout in Flow sensors?

- https://kb.paessler.com/en/topic/66485

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

Related Topics

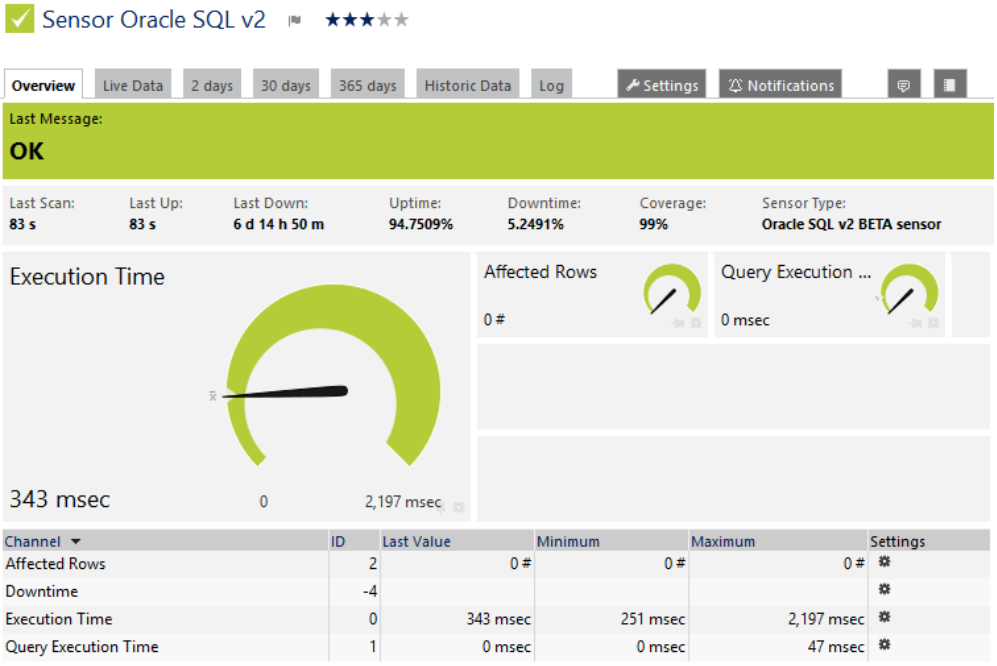
- **Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors** 3175
- **Channel Defintions for xFlow, IPFIX, and Packet Sniffer Sensors** 3180

7.8.81 Oracle SQL v2 Sensor

The Oracle SQL v2 sensor monitors a database on an Oracle server and executes a defined query.

It can show the following:

- Execution time of the whole request (including connection buildup, query execution, transaction handling, disconnection)
- Execution time of a given query
- Number of rows which were addressed by the query (including select statements if you process data tables)
- It can also process the data table and show defined values in individual channels.



Oracle SQL v2 Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/oracle_sql_v2.png

Remarks

- Requires 1136 .NET 4.0 on the probe system.
- Define credentials, custom port (if required), and timeout in settings section **Credentials for Database Management Systems** 370 of the parent device, or in the settings of a group or probe above.
- PRTG Manual: **Monitoring Databases** 3120 (includes an example 3121 for channel value selection)
- Knowledge Base: How to setup the SQL v2 sensors in PRTG? Is there a guide?

- Knowledge Base: How can I monitor strings from an SQL database and show a sensor status depending on it?
- Knowledge Base: How can I monitor error tables in SQL databases?
- Your SQL query must be stored in a file on the system of the probe the sensor is created on. If you use it on a remote probe, store the file on the system running the remote probe. In a cluster setup, copy the file to every cluster node.
- Save the SQL script with the query into the **\Custom Sensors\sql\oracle** subfolder of your PRTG installation. See manual section **Data Storage** 3226 for more information about how to find this path.
- This sensor type supports Oracle database servers version 10.2 or higher

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Requirement: .NET Framework

This sensor type requires the Microsoft .NET Framework to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the remote probe 3196. If the framework is missing, you cannot create this sensor.

Required .NET version (with latest updates): .NET 4.0 (Client Profile is sufficient), .NET 4.5, or .NET 4.6.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/60543

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DATABASE SPECIFIC

Identifier	Enter the Oracle System ID (SID) or the SERVICE_NAME of the database the sensor will connect to. Specify below which type of identifier you use. By default, the sensor uses the SID as connection string. The identifier is defined in the CONNECT_DATA part of the TNSNames.ora file on the Oracle instance. For example, a system ID can look like this: orcl
Identification Method	Define which type of identifier you use to connect to the database. This type depends on the configuration of your Oracle server. Choose between: ▪ **Use SID as identifier (default)**: Connect to the database instance using a system ID as connection string. Enter the SID above. ▪ **Use SERVICE_NAME as identifier:** Connect to the database instance using a SERVICE_NAME as connection string. Enter the SERVICE_NAME above.

DATA

SQL Query File	Select an SQL script file that includes a valid SQL statement to execute on the server. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew. The script will be executed with every scanning interval. The list contains SQL scripts from the database management system specific **\Custom Sensors\sql** subfolder of your PRTG installation. Store your script there. If used on a remote probe, the file must be stored on the system running the remote probe. If used on a cluster probe, you must store the file on all servers running a cluster node! For more information on how to find this path, please see **Data Storage** 3226 section. By default, there is the demo script **Demo Serveruptime.sql** available that you can use to monitor the uptime of the target server. For example, a correct expression in the file could be: SELECT AVG (UnitPrice) FROM Products. If you want to use transactions, separate the individual steps with semicolons ";". Please be aware that with each request, the full result set will be transferred, so use filters and limits in your query. You can use the following placeholders in your query file to have them replaced by an input parameter: ▪ Microsoft SQL, MySQL, PostgreSQL: **@prtg** ▪ Oracle SQL: **:prtg** ▪ ADO SQL: **?** (question mark) This is useful if you have various SQL sensors with queries that differ in only one parameter.
Use Input Parameter	Define if you want to pass a parameter to your SQL query file. This will replace the placeholder %prtg (Microsoft SQL, MySQL, PostgreSQL), or :prtg (Oracle SQL), or ? (ADO SQL) in the SQL query. Choose between: ▪ **Don't use input parameter (default)**: Execute the SQL query file without using placeholders. ▪ **Use input parameter**: Execute an SQL query file that contains a placeholder. Provide the parameter you want to use in the query below.

DATA

Input Parameter	This field is only visible if you choose **Use input parameter** above. Enter the parameter you want to pass to the SQL query file. This parameter replaces the placeholder %prtg or :prtg or ? in the SQL query. You can also use PRTG placeholders for custom sensors (command line parameters) as input parameter, for example, %sensorid or %deviceid. For details, see **Application Programming Interface (API) Definition** 3174. Provide strings as they are and do not surround them with quotation marks. PRTG will correctly insert string parameters into the query automatically.
Use Transaction	Define if you want to use transactions and if they will affect the database content. Choose between: ▪ **Don't use transaction (default)**: No transactions will be executed. ▪ **Use transaction and always rollback**: Choose this option to ensure that no data in the database will be changed by the query. In the SQL query file, separate the single steps of the transaction with semicolons. ▪ **Use transaction and commit on success**: Choose this option to perform changes on the database with the query. The changes will only apply if all execution steps succeed without any errors. In the SQL query file, separate the single steps of the transaction with semicolons.
Data Processing	Define if you want to process data from the database. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew. Choose between: ▪ **Just execute the query**: If you select this option, the sensor will only show information about the number of affected rows and the execution time of the query. Affected rows are rows that were changed somehow with the query (for example, created, deleted, edited). ▪ **Count table rows**: Choose this option if you perform a SELECT statement and want to monitor how many rows of the data table this statement returns. ▪ **Process data table**: Select this option to read and analyze the queried data table. If you select this option, the sensor will count rows with SELECT statements as well.

DATA

Handle DBNull in Channel Values as	This setting is only visible if you select **Process data table** above. Define the sensor behavior if DBNull is returned by the query. Choose between: ▪ **Error**: The sensor will show a **Down** status if DBNull is reported. ▪ **Number 0**: The sensor will recognize the result DBNull as a valid value and interpret it as the number 0.
Select Channel Value by	This setting is only visible if you select **Process data table** above. Define how the desired cell in the database table will be selected. This is necessary to configure the cells that will be used in the sensor channels. Choose between: ▪ **Column number**: The channel value will be determined by using the value in row 0 of the column whose number you specify below. ▪ **Column name**: The channel value will be determined by using the value in row 0 of the column whose name you specify below. ▪ **Row number**: The channel value will be determined by using the value in column 0 of the row whose number you specify below. ▪ **Key value pair**: The channel value will be determined by searching in column 0 for the key you specify below and returning the value in column 1 of the same row where the key value was found. The option you choose here also defines the method to optionally determine a value for the sensor message. For details, see setting **Use Data Table Value in Sensor Message** below. Please see manual section **Monitoring Databases** 3120 for an example 3121 for channel value selection.
Sensor Channel #x	This setting is only visible if you select **Process data table** above. You can define up to 10 different channels for the data processing of this sensor. You have to define at least one data channel if you process the data table, so you will see all available settings for Channel #1 without enabling it manually. For all other possible channels, choose between: ▪ **Disable**: This channel will not be added to the sensor. ▪ **Enable**: This channel will be added to the sensor. Define the settings as described above. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

DATA

Sensor Channel #x Name	This setting is only visible if you select **Process data table** above. Enter a unique name for the channel. Please enter a string. Channels will be generated dynamically with this name as identifier. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Sensor Channel #x Column Number	This setting is only visible if you select **Column number** above. Provide the number of the column which will be used to determine the channel value in row 0. Please enter an integer value.
Sensor Channel #x Column Name	This setting is only visible if you select **Column number** above. Provide the name of the column which will be used to determine the channel value in row 0. Please enter a string.
Sensor Channel #x Row Number	This setting is only visible if you select **Row number** above. Provide the number of the row which will be used to determine the channel value in column 0. Please enter an integer value.
Sensor Channel #x Key	This setting is only visible if you select **Key value pair** above. Provide the key to search for in column 0 of the data table. The value in column 1 of the same row where the key value was found will be used to determine the channel value. Please enter a string.
Sensor Channel #x Mode	This setting is only visible if you select **Process data table** above. Define how to display the determined value in the channel. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew. Choose between: ▪ **Absolute (recommended)**: Shows the value as the sensor retrieves it from the data table. ▪ **Difference**: The sensor calculates and shows the difference between the last and the current value returned from the data table.
Sensor Channel #x Unit	This setting is only visible if you select **Process data table** above. Define the unit of the channel value. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew. Choose between: ▪ BytesBandwidth ▪ BytesMemory ▪ BytesDisk ▪ Temperature

DATA

- Percent
- TimeResponse
- TimeSeconds
- TimeHours
- Count
- CPU
- BytesFile
- SpeedDisk
- SpeedNet
- Custom
- Value Lookup

For more information about the available units, please refer to the PRTG **Application Programming Interface (API) Definition** for custom sensors.

To use lookups with this channel, choose **Value Lookup** and select your lookup file below. Do not use **Custom** for using lookups with this sensor!

Sensor Channel #x Custom Unit

This setting is only visible if you select **Custom** above. Define a unit for the channel value. Please enter a string.

Sensor Channel #x Value Lookup

This settings is only visible if you select **Value Lookup** above. Select a lookup file that you want to use with this channel.

Use Data Table Value in Sensor Message

This setting is only visible if you select **Process data table** above. Define if the sensor message will show a value from the data table. Choose between:

- **Disable**: Do not use a custom sensor message.
- **Enable**: Define a custom sensor message with a defined value of the data table. Define the value selection below.

The method to determine a value for the sensor message is defined in setting **Select Channel Value by** above.

Sensor Message Column Number

This setting is only visible if you select **Column number** and **Use Data Table Value in Sensor Message** above. Enter the number of a column. The sensor message will show the value in row 0 of this column. Please enter an integer value.

Columns and rows start with index 0.

DATA

Sensor Message Column Name	This setting is only visible if you select **Column name** and **Use Data Table Value in Sensor Message** above. Enter the name of a column. The sensor message will show the value in row 0 of this column. Please enter a string. Columns and rows start with index 0.
Sensor Message Row Number	This setting is only visible if you select **Row number** and **Use Data Table Value in Sensor Message** above. Enter the number of a row. The sensor message will show value in column 0 of this row. Please enter an integer value. Columns and rows start with index 0.
Sensor Message Key	This setting is only visible if you select **Key value pair** and **Use Data Table Value in Sensor Message** above. Enter a key to search for in column 0 of the data table. The sensor message will show the value in column 1 of the row where the key has been found. Please enter a string. Columns and rows start with index 0.
Sensor Message	This setting is only visible if you select **Use Data Table Value in Sensor Message** above. Define the sensor message. Please enter a string. Use the placeholder {0} at the position where the value will be added. Example: **The message is {0}**
If Sensor Message Changes	Define what this sensor will do when the sensor value changes. You can choose between: ▪ **Ignore changes (default)**: The sensor takes no action on change. ▪ **Trigger 'change' notification**: The sensor sends an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification 2791 whenever the sensor value changes.
Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result.

DATA

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section Data Storage 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. ⓘ Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: How to setup the SQL v2 sensors in PRTG? Is there a guide?

- https://kb.paessler.com/en/topic/70618

Knowledge Base: How can I monitor strings from an SQL database and show a sensor status depending on it?

- https://kb.paessler.com/en/topic/63259

Knowledge Base: How do I monitor the size of a Microsoft SQL server database?

- https://kb.paessler.com/en/topic/18183

Knowledge Base: How can I monitor error tables in SQL databases?

- https://kb.paessler.com/en/topic/70774

Knowledge Base: Which .NET version does PRTG require?

- https://kb.paessler.com/en/topic/60543

PRTG Manual:

- **Monitoring Databases** 3120

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

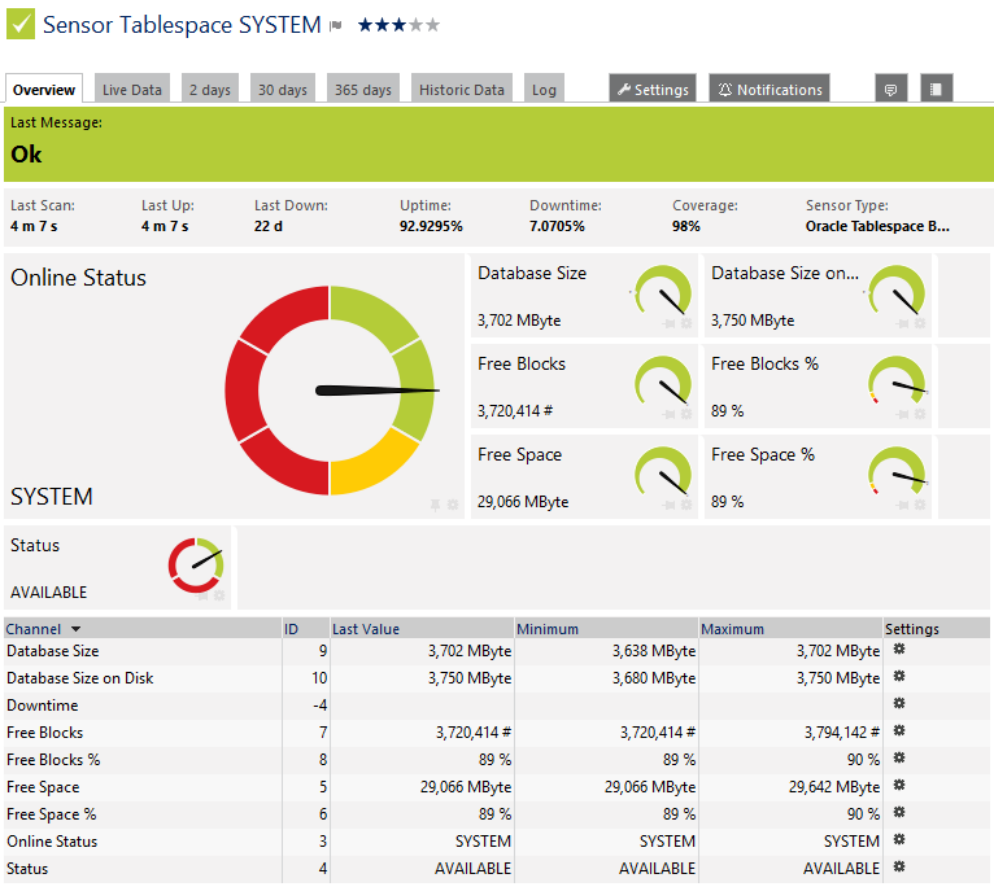
Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.82 Oracle Tablespace Sensor

The Oracle Tablespace sensor monitors a tablespace on an Oracle server. It can show the following:

- Online status (online, system, recover, sysoff, offline, unknown)
- Status (available, invalid, unknown)
- Free disk space in bytes and percent
- Number of free blocks and in percent
- Current database size
- Database size on disk (managed tablespace)



Channel	ID	Last Value	Minimum	Maximum	Settings
Database Size	9	3,702 MByte	3,638 MByte	3,702 MByte	
Database Size on Disk	10	3,750 MByte	3,680 MByte	3,750 MByte	
Downtime	-4				
Free Blocks	7	3,720,414 #	3,720,414 #	3,794,142 #	
Free Blocks %	8	89 %	89 %	90 %	
Free Space	5	29,066 MByte	29,066 MByte	29,642 MByte	
Free Space %	6	89 %	89 %	90 %	
Online Status	3	SYSTEM	SYSTEM	SYSTEM	
Status	4	AVAILABLE	AVAILABLE	AVAILABLE	

Oracle Tablespace Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/oracle_tablespace.png

Remarks

- This sensor type supports Oracle database servers version 10.2 or higher.
- Requires 1269 .NET 4.0 on the probe system.

- Requires 1269 sufficient privileges for the account that you use for the connection. We recommend that you use the SYSTEM account.
- Define credentials, custom port (if required), and timeout in settings section **Credentials for Database Management Systems** 370 of the parent device, or in the settings of a group or probe above.
- PRTG Manual: **Monitoring Databases** 3120
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Requirement: .NET Framework

This sensor type requires the Microsoft .NET Framework to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the remote probe 3196. If the framework is missing, you cannot create this sensor.

Required .NET version (with latest updates): .NET 4.0 (Client Profile is sufficient), .NET 4.5, or .NET 4.6.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/60543

Requirement: Sufficient Account Privileges

Please use an account for the connection that has the privileges to see all (or specific) views. We recommend that you use the SYSTEM account if possible, otherwise grant your DBA the SELECT_CATALOG_ROLE to the account that you use. Without sufficient privileges you may see the error message "ORA-00942: table or view does not exist".

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

In the appearing dialog box in the **Add Sensor** dialog, enter an identifier 1270 to access the tablespace selection and click **OK**. Select the tablespaces in the Oracle database you want to monitor. PRTG creates one sensor for each tablespace you choose. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

TABLESPACE SPECIFIC

Tablespace	Select the tablespaces you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

ORACLE SPECIFIC

Identifier	Enter the Oracle System ID (SID) or the SERVICE_NAME of the database the sensor will connect to. Specify below which type of identifier you use. By default, the sensor uses the SID as connection string. The identifier is defined in the CONNECT_DATA part of the TNSNames.ora file on the Oracle instance. For example, a system ID can look like this: orcl
Identification Method	Define which type of identifier which you use to connect to the database. This type depends on the configuration of your Oracle server. Choose between: ▪ **Use SID as identifier (default)**: Connect to the database instance using a system ID as connection string. Enter the SID above. ▪ **Use SERVICE_NAME as identifier**: Connect to the database instance using a SERVICE_NAME as connection string. Enter the SERVICE_NAME above.
Sensor Name Prefix	Define if you want to use the SERVICE_NAME as prefix for the sensor name. If you have multiple databases on your Oracle server, this will help you to distinguish the monitored tablespaces. Choose between: ▪ **Do not use a prefix for the sensor name**: The sensor name will only show the name of the monitored tablespace. ▪ **Use SERVICE_NAME as prefix for the sensor name**: PRTG will add the SERVICE_NAME to the beginning of the sensor name.

TABLESPACE SPECIFIC

Tablespace	Shows the tablespace that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: Which .NET version does PRTG require?

- https://kb.paessler.com/en/topic/60543

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.83 Packet Sniffer Sensor

The Packet Sniffer sensor monitors the headers of data packets that pass a local network card using a built-in packet sniffer. You can choose from predefined channels. The sensor analyzes only header traffic.

This sensor can show the following traffic types in kbit per second:

- Chat (IRC, AIM)
- Citrix
- FTP/P2P (file transfer)
- Infrastructure (network services: DHCP, DNS, Ident, ICMP, SNMP)
- Mail (mail traffic: IMAP, POP3, SMTP)
- NetBIOS
- Remote control (RDP, SSH, Telnet, VNC)
- WWW (web traffic: HTTP, HTTPS)
- Total traffic
- Other protocols (other UDP and TCP traffic)

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

Channel	ID	Last Value (volume)	Last Value (speed)	Minimum	Maximum	Settings
Downtime	-4					
Infrastructure	3007	33 KByte	5 kbit/s	2 kbit/s	5 kbit/s	
NetBIOS	3008	223 KByte	30 kbit/s	14 kbit/s	30 kbit/s	
Other	0	196 KByte	27 kbit/s	0 kbit/s	27 kbit/s	
Remote Control	3005	36 KByte	5 kbit/s	1 kbit/s	5 kbit/s	
Total	-1	3.068 KByte	419 kbit/s	0 kbit/s	419 kbit/s	
Various	3009	1.518 KByte	207 kbit/s	101 kbit/s	207 kbit/s	
WWW	3001	1.063 KByte	145 kbit/s	0 kbit/s	145 kbit/s	

Packet Sniffer Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/packet_sniffer.png

Remarks

- By default, this sensor works only on a probe device.
- Knowledge Base: How can I change the default groups and channels for xFlow and Packet Sniffer sensors?
- For a general introduction to the technology behind packet sniffing, please see manual section **Monitoring Bandwidth via Packet Sniffing** 3097.
- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.

By default, you can only monitor traffic passing the PRTG probe system where the **Probe Device** with the sensor is set up (either a local or remote probe). To monitor other traffic in your network, you can configure a monitoring port (if available) that the switch sends a copy of all traffic to. You can then physically connect this port to a network card of the computer the PRTG probe (either local or remote probe) is running on. This way, PRTG can analyze the complete traffic that passes through the switch. This feature of your hardware may be called Switched Port Analyzer (SPAN), port mirroring, or port monitoring.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.

BASIC SENSOR SETTINGS

Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SNIFFER SPECIFIC

Include Filter	Define if you want to filter any traffic. If you leave this field empty, the sensor includes all traffic. To include specific traffic only, define filters using a special syntax. For detailed information, please see **Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors** 3175 section.
Exclude Filter	First, the filters you define in the **Include Filter** field are considered. From this subset, you can explicitly exclude traffic, using the same syntax. For detailed information, please see **Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors** 3175 section.
Network Adapters	Define the network adapters that this sensor monitors. You see a list of names with all adapters available on the probe system. To select an adapter, set a check mark symbol in front of the respective name. You can also select and deselect all items by using the check box in the table head.
Log Stream Data to Disk (for Debugging)	Define if the probe will write a logfile of the stream and packet data to the data folder (see **Data Storage** 3226). Choose between: ▪ **None (recommended)**: Do not write additional logfiles. We recommend this for normal use cases. ▪ **Only for the 'Other' channel**: Only write logfiles of data that is not filtered otherwise and therefore accounted to the default **Other** channel. ▪ **All stream data**: Write logfiles for all data received. Use with caution! When enabled, huge data files can be created. Please use for a short time and for debugging purposes only.

CHANNEL CONFIGURATION

Channel Selection

Define the categories the sensor accounts the traffic to. There are different groups of traffic available. Choose between:

- **Web**: Internet web traffic.
- **File Transfer**: Traffic caused by FTP.
- **Mail**: Internet mail traffic.
- **Chat**: Traffic caused by chat and instant messaging.
- **Remote Control**: Traffic caused by remote control applications, such as RDP, SSH, Telnet, and VNC.
- **Infrastructure**: Traffic caused by network services, such as DHCP, DNS, Ident, ICMP, and SNMP.
- **NetBIOS**: Traffic caused by NetBIOS communication.
- **Citrix**: Traffic caused by Citrix applications.
- **Other Protocols**: Traffic caused by various other protocols via UDP and TCP.

For each traffic group, you can select how many channels will be used for each group, that is, how detailed the sensor divides the traffic. For each group, choose between:

- **No**: Do not account traffic of this group in its own channel. All traffic of this group is accounted to the default channel named **Other**.
- **Yes**: Count all traffic of this group and summarize it into one channel.
- **Detail**: Count all traffic of this group and further divide it into different channels. The traffic appears in several channels as shown in the **Content** column.
  Extensive use of this option can cause load problems on your probe system. We recommend setting specific, well-chosen filters for the data you really want to analyze.

You can change the default configuration for groups and channels. For details, please see this Knowledge Base article: How can I change the default groups and channels for xFlow and Packet Sniffer sensors?

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

PRIMARY TOPLIST

Primary Toplist	Define which will be your primary toplist. It will be shown in maps when adding a toplist object. Choose from: ▪ **Top Talkers** ▪ **Top Connections** ▪ **Top Protocols** ▪ [Any custom toplists you have added]

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. ⓘ Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

Toplists

For all flow and packet sniffer sensors there are **Toplists** available on the **Overview** tab of a sensor's detail page. Using toplists, you can review traffic data of small time periods in great detail. For more information, please see **Toplists** 2806 section.

More

Knowledge Base: How can I change the default groups and channels for xFlow and Packet Sniffer sensors?

- https://kb.paessler.com/en/topic/60203

Knowledge Base: Where is the volume line in graphs?

- https://kb.paessler.com/en/topic/61272

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

Related Topics

- **Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors** 3175
- **Channel Defintions for xFlow, IPFIX, and Packet Sniffer Sensors** 3180

7.8.84 Packet Sniffer (Custom) Sensor

The Packet Sniffer (Custom) sensor monitors the headers of data packets that pass a local network card using built-in packet sniffer. You can define your own channels. There are no predefined channels for this sensor type. This sensor analyzes only header traffic.

- This sensor can show traffic by type individually to your needs.

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

Channel	ID	Last Value (volume)	Last Value (speed)	Minimum	Maximum	Settings
Downtime	-4					
Infrastructure	3007	33 KByte	5 kbit/s	2 kbit/s	5 kbit/s	
NetBIOS	3008	223 KByte	30 kbit/s	14 kbit/s	30 kbit/s	
Other	0	196 KByte	27 kbit/s	0 kbit/s	27 kbit/s	
Remote Control	3005	36 KByte	5 kbit/s	1 kbit/s	5 kbit/s	
Total	-1	3.068 KByte	419 kbit/s	0 kbit/s	419 kbit/s	
Various	3009	1.518 KByte	207 kbit/s	101 kbit/s	207 kbit/s	
WWW	3001	1.063 KByte	145 kbit/s	0 kbit/s	145 kbit/s	

Packet Sniffer Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/packet_sniffer.png

Remarks

- By default, this sensor works only on a probe device.

- This sensor does not support more than 50 channels 1290 officially.
- For a general introduction to the technology behind packet sniffing, please see manual section **Monitoring Bandwidth via Packet Sniffing** 3097.
- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.

By default, you can only monitor traffic passing the PRTG probe system where the **Probe Device** with the sensor is set up (either a local or remote probe). To monitor other traffic in your network, you can configure a monitoring port (if available) that the switch sends a copy of all traffic to. You can then physically connect this port to a network card of the computer the PRTG probe (either local or remote probe) is running on. This way, PRTG can analyze the complete traffic that passes through the switch. This feature of your hardware may be called Switched Port Analyzer (SPAN), port mirroring, or port monitoring.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Limited to 50 Sensor Channels

PRTG does not support more than 50 sensor channels officially. Depending on the data used with this sensor type, you might exceed the maximum number of supported sensor channels. In this case, PRTG will try to display all sensor channels. However, please be aware that you will experience limited usability and performance.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SNIFFER SPECIFIC

Include Filter	Define if you want to filter any traffic. If you leave this field empty, the sensor includes all traffic. To include specific traffic only, define filters using a special syntax. For detailed information, please see **Filter Rules for xFlow and Packet Sniffer Sensors** 3175 section.
Exclude Filter	First, the filters you define in the **Include Filter** field are considered. From this subset, you can explicitly exclude traffic, using the same syntax. For detailed information, please see **Filter Rules for xFlow and Packet Sniffer Sensors** 3175 section.
Channel Definition	Please enter a channel definition to divide the traffic into different channels. Write each definition in one line. For detailed information, please see **Channel Defintions for xFlow and Packet Sniffer Sensors** 3180 section. All traffic for which no channel is defined is accounted to the default channel named **Other**.

SNIFFER SPECIFIC

Extensive use of many filters can cause load problems on your probe system. We recommend defining specific, well-chosen filters for the data you really want to analyze. We recommend that you do not use more than 20 channels in graphs and tables, and not more than 100 channels in total. For performance reasons, it is better to add several sensors with less channels each.

Network Adapters

Define the network adapters that this sensor monitors. You see a list of names with all adapters available on the probe system. To select an adapter, set a check mark symbol in front of the respective name. You can also select and deselect all items by using the check box in the table head.

Log Stream Data to Disk (for Debugging)

Define if the probe will write a log file of the stream and packet data to the data folder (see **Data Storage** 3226). Choose between:

- **None (recommended)**: Do not write additional log files. Recommended for normal use cases.
- **Only for the 'Other' channel**: Only write log files of data that is not filtered otherwise and therefore accounted to the default **Other** channel.
- **All stream data**: Write log files for all data received.

Use with caution! Enabling this option might create huge data files. Please use for a short time and for debugging purposes only.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

PRIMARY TOPLIST

Primary Toplist	Define which will be your primary toplist. It will be shown in maps when adding a toplist object. Choose from: ▪ **Top Talkers** ▪ **Top Connections** ▪ **Top Protocols** ▪ [Any custom toplists you have added]

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

Toplists

For all flow and packet sniffer sensors there are **Toplists** available on the **Overview** tab of a sensor's detail page. Using toplists, you can review traffic data of small time periods in great detail. For more information, please see **Toplists** 2806 section.

More

Knowledge Base: Where is the volume line in graphs?

- https://kb.paessler.com/en/topic/61272

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

Related Topics

- **Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors** 3175
- **Channel Defintions for xFlow, IPFIX, and Packet Sniffer Sensors** 3180

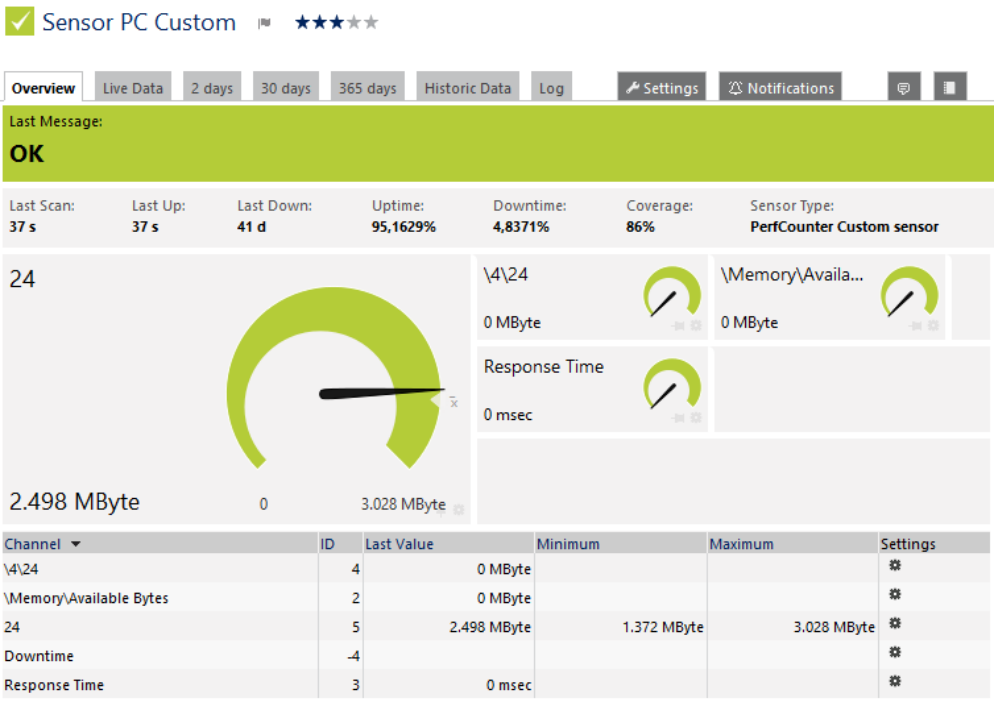
7.8.85 PerfCounter Custom Sensor

The PerfCounter Custom sensor monitors a configured set of Windows Performance Counters. You can define your own channels. There are no predefined channels available for this sensor type.

- This sensor can show Windows performance counters individually to your needs.

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

To find out which performance counters are available on the target system and what their names are, please see this Knowledge Base article: How can I find out the names of available Performance Counters?



PerfCounter Custom Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/perfcounter_custom.png

Remarks

- Requires Windows credentials in the parent device settings.
- Requires the Windows Remote Registry service to be running on the target computer.
- Requires Windows Server 2008 R2 or later on the probe system.
- Knowledge Base: How can I find out the names of available Performance Counters?
- Knowledge Base: My Performance Counter sensor does not work. What can I do?
- You cannot add different performance counters with the same name to one sensor.

- If a performance counter contains angle brackets (< or >), please do not edit the channel settings because this might cause an error.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Requirement: Windows Credentials

Requires credentials for Windows systems to be defined for the device you want to use the sensor on. In the parent device's 365 **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. If you fail to do so, a connection via Performance Counters will not be possible.

The user account has to be a member of the Performance Monitor Users user group on the target system.

Requirement: Remote Registry Service

In order for this sensor to work with Windows Performance Counters, please make sure the RemoteRegistry "Remote Registry" Windows service is running on the target computer. If you fail to do so, a connection via Performance Counters will not be possible.

To enable the service, please log in to the respective computer and open the services manager (for example, via services.msc). In the list, find the respective service and set its Start Type to Automatic.

Requirement: Windows Version

In order for this sensor to work with Windows Performance Counters, please make sure a Windows version 2008 R2 or later is installed on the computer running the PRTG probe: This is either on the local system (on every node, if on a cluster probe), or on the system running a remote probe 3196.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

PERFORMANCE COUNTER SETTINGS

List of Counters	Enter a list of performance counters which will be queried. Define one counter per row. PRTG will create one channel for each counter. Use the following syntax: the name of the counter, followed by two colons (::) and the unit. Example: **\Processor(_Total)\% Processor Time::%** It is not possible to monitor different performance counters with the same name in one sensor. The sensor uses the counter as channel name, so this would create duplicate channels which PRTG does not support. If you want to monitor different performance counters with the same name, please add one sensor for each counter. You can also create a custom sensor 2778. For example, you can write a PowerShell query that connects to the target device, retrieves the desired counters with the Get-Counter cdmlet, and reports them back to PRTG as individual channels. If your custom performance counter includes an angle bracket (< or >), please do not edit the **Sensor Channels Settings** 2782 (for example, limits) after creating the sensor! This might lead to a malfunctioning sensor.
Mode	Define the mode for the return value of the performance counter. This setting determines if the returning value will be displayed as absolute value or if the difference between the last and the current value will be used. Choose between: ▪ **Absolute (recommended)**: The returning value will be displayed as absolute value. ▪ **Difference**: The difference between last and current value will be displayed. Please make sure that all counters that you monitor are capable of this mode if you select it.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

PERFORMANCE COUNTER SETTINGS

List of Counters	Shows the performance counters that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Mode	Shows the mode in which the sensor displays the returning values. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

SENSOR DISPLAY

	You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

SCANNING INTERVAL

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: How can I find out the names of available Performance Counters?

- https://kb.paessler.com/en/topic/50673

Knowledge Base: Remote Monitoring of Specific Performance Counters

- https://kb.paessler.com/en/topic/59804

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

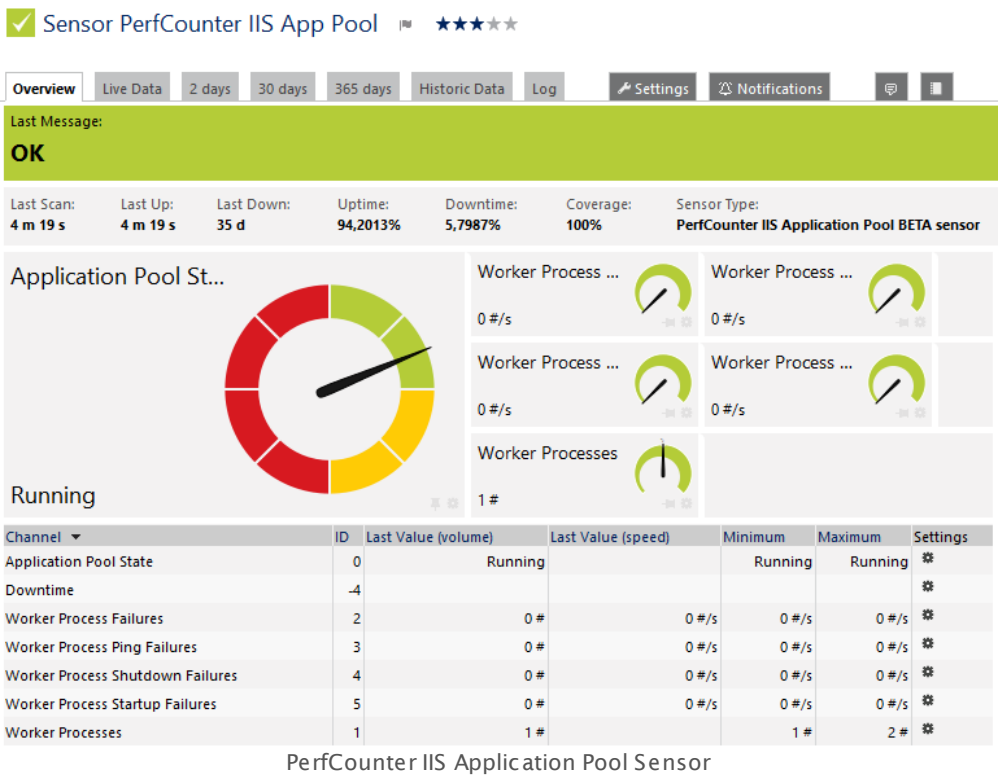
7.8.86 PerfCounter IIS Application Pool Sensor

The PerfCounter IIS Application Pool sensor monitors a Microsoft Internet Information Services (IIS) application pool using Windows Performance Counters.

It can show the following:

- Overall status of the application pool:
  - Running (sensor status 163 **Up**)
  - Initialized or Shutdown Pending (**Warning**)
  - Unavailable, Uninitialized, Stopping, Stopped, or Delete Pending (**Down**)
- Number of worker processes
- Number of failures in worker processes per second
- Number of ping failures per second
- Number of shutdown failures per second
- Number of startup failures per second

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Channel	ID	Last Value (volume)	Last Value (speed)	Minimum	Maximum	Settings
Application Pool State	0	Running		Running	Running	
Downtime	-4					
Worker Process Failures	2	0 #	0 #/s	0 #/s	0 #/s	
Worker Process Ping Failures	3	0 #	0 #/s	0 #/s	0 #/s	
Worker Process Shutdown Failures	4	0 #	0 #/s	0 #/s	0 #/s	
Worker Process Startup Failures	5	0 #	0 #/s	0 #/s	0 #/s	
Worker Processes	1	1 #		1 #	2 #	

PerfCounter IIS Application Pool Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/PerfCounter_IIS_Application_Pool.png

Remarks

- Requires 1310 Microsoft IIS version 7.5 or later on the target system.
- Requires 1310 Windows credentials in the parent device settings.
- Requires 1310 the Windows Remote Registry service to be running on the target computer.
- Requires 1310 Windows Server 2008 R2 or later on the probe system.
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Requirement: Microsoft IIS Version 7.5

To monitor Microsoft Internet Information Services (IIS) application pools, this sensor needs IIS version 7.5 or later to be installed on the target system.

Requirement: Windows Credentials

Requires credentials for Windows systems to be defined for the device you want to use the sensor on. In the parent device's 365 **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. If you fail to do so, a connection via Performance Counters will not be possible.

The user account has to be a member of the Performance Monitor Users user group on the target system.

Requirement: Remote Registry Service

In order for this sensor to work with Windows Performance Counters, please make sure the RemoteRegistry "Remote Registry" Windows service is running on the target computer. If you fail to do so, a connection via Performance Counters will not be possible.

To enable the service, please log in to the respective computer and open the services manager (for example, via services.msc). In the list, find the respective service and set its Start Type to Automatic.

Requirement: Windows Version

In order for this sensor to work with Windows Performance Counters, please make sure a Windows version 2008 R2 or later is installed on the computer running the PRTG probe: This is either on the local system (on every node, if on a cluster probe), or on the system running a remote probe 3196.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the Microsoft Internet Information Services (IIS) application pools that you want to monitor. PRTG creates one sensor for each pool you select in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

IIS APPLICATION POOL SPECIFIC

Application Pool	Select the application pools you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	Enter one or more **Tags**, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

IIS APPLICATION POOL SPECIFIC

Application Pool	Shows the name of the application pool that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. ⓘ You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.

SCANNING INTERVAL

- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. ⓘ To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies [2822] in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector [210] to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** [360] or in the superior **Group Settings** [334].

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.87 Ping Sensor

The Ping sensor sends an Internet Control Message Protocol (ICMP) echo request ("Ping") from the computer running the probe to the device it is created on to monitor the availability of a device. Default is 5 Pings per scanning interval.

It can show the following:

- Ping time
- Minimum Ping time when using more than one Ping per interval
- Maximum Ping time when using more than one Ping per interval
- Packet loss in percent when using more than one Ping per interval

Ping Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/ping.png

Remarks

- Knowledge Base: How to create/customize statistical PING sensor?
- Knowledge Base: Can I create an inverse Ping sensor?

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

PING SETTINGS

Timeout (Sec.)	Enter a timeout in seconds for the Ping. If the reply takes longer than this value defines, the sensor will cancel the request and show an error message. The maximum timeout value is 300 seconds (5 minutes).
Packet Size (Bytes)	Enter the packet size in bytes for the Ping. You can choose any value between 1 and 10000. We recommend that you use the default value.
Ping Method	Define the kind of Ping check that the sensor performs. Choose between: ▪ **Send one single Ping**: With each scanning interval, send a single Ping only. A sensor in this setting will show the Ping time only. This setting is good for simple availability monitoring. ▪ **Send multiple Ping request**: With each scanning interval, send multiple Pings in a row. A sensor in this setting will also show minimum and maximum Ping time as well as packet loss (in percent). This setting is good if you want to create reports about average Ping times out of a series of ping requests. This is the default setting. ⓘ When using multiple requests, all of them have to be lost to show a **Down** status 163. For example, if there is only one Ping request answered in a series of five, the sensor will still show a green **Up** status.
Ping Count	This field is only visible if you enable **Send multiple Ping request** above. Enter the number of Pings that the sensor sends in a row for one interval. Please enter an integer value. The default value is 5.
Ping Delay (in ms)	This field is only visible if you enable **Send multiple Ping request** above. Enter the time in milliseconds the sensor waits between two Ping requests. Please enter an integer value. The default value is 5. ⓘ Increase the value if the target device drops Ping packets due to denial-of-service (DOS) suspicion.
Auto Acknowledge	You can define that a **Down** status of this sensor will be acknowledged 191 automatically. ▪ **Show "Down" status on error (default)**: Do not automatically acknowledge an alarm if this sensor changes to a **Down** status. ▪ **Show "Down (Acknowledged)" status on error**: Automatically acknowledge an alarm. If this sensor changes to a **Down** status, it will automatically show **Down (Acknowledged)** instead.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: How to create/customize statistical PING sensor?

- https://kb.paessler.com/en/topic/1873

Knowledge Base: Can I create an inverse Ping sensor?

- https://kb.paessler.com/en/topic/10203

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.88 Ping Jitter Sensor

The Ping Jitter sensor sends a series of Internet Control Message Protocol (ICMP) echo requests ("Pings") to the given URI to determine the statistical jitter.

This sensor shows the following:

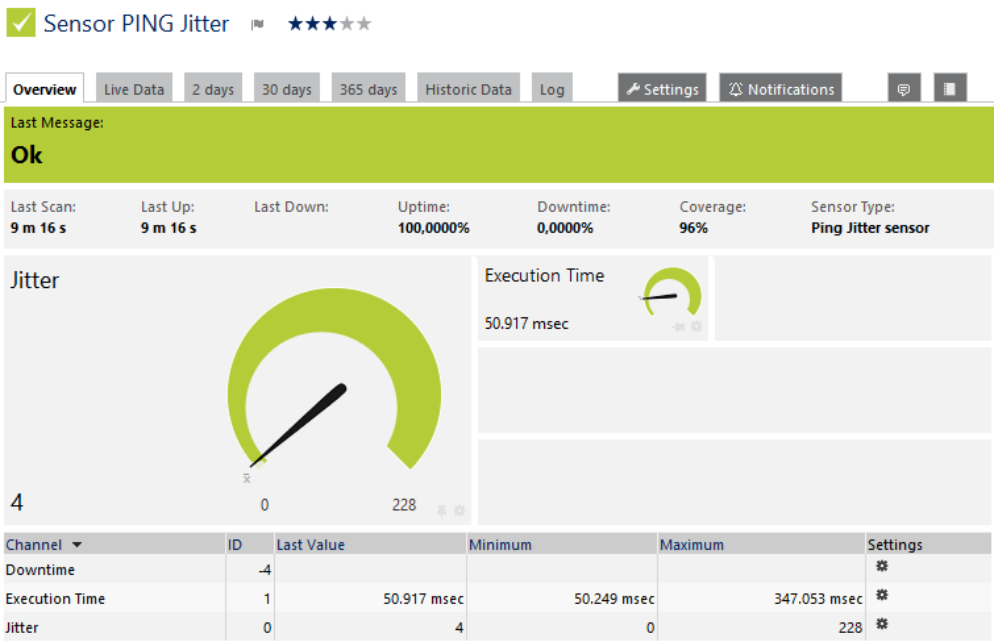
- Statistical jitter value
- Execution time

The Real Time Jitter value is updated every time a packet is received using the formula described in RFC 1889:

Jitter = Jitter + (abs(ElapsedTime – OldElapsedTime) – Jitter) / 16

The Statistical Jitter value is calculated on the first x packets received using the statistical variance formula:

Jitter Statistical = SquareRootOf(SumOf((ElapsedTime[i] – Average) ^ 2) / (ReceivedPacketCount – 1))



Ping Jitter Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/ping_jitter.png

Remarks

- Requires 1329 .NET 4.0 or 4.5 on the probe system. If the sensor shows the error PE087, please additionally install .NET 3.5 on the probe system.
- We recommend Windows 2012 R2 on the probe system for best performance of this sensor.

Requirement: .NET Framework

This sensor type requires the Microsoft .NET Framework to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the remote probe 3196. If the framework is missing, you cannot create this sensor.

Required .NET version (with latest updates): .NET 4.0 (Client Profile is sufficient), .NET 4.5, or .NET 4.6.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/60543

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

BASIC SENSOR SETTINGS

	You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SETTINGS

Ping Count	Define the number of Internet Control Message Protocol (ICMP) pings that this sensor sends. Please enter an integer value.

DEBUG OPTIONS

Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section **Data Storage** 3226. You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: Which .NET version does PRTG require?

- https://kb.paessler.com/en/topic/60543

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

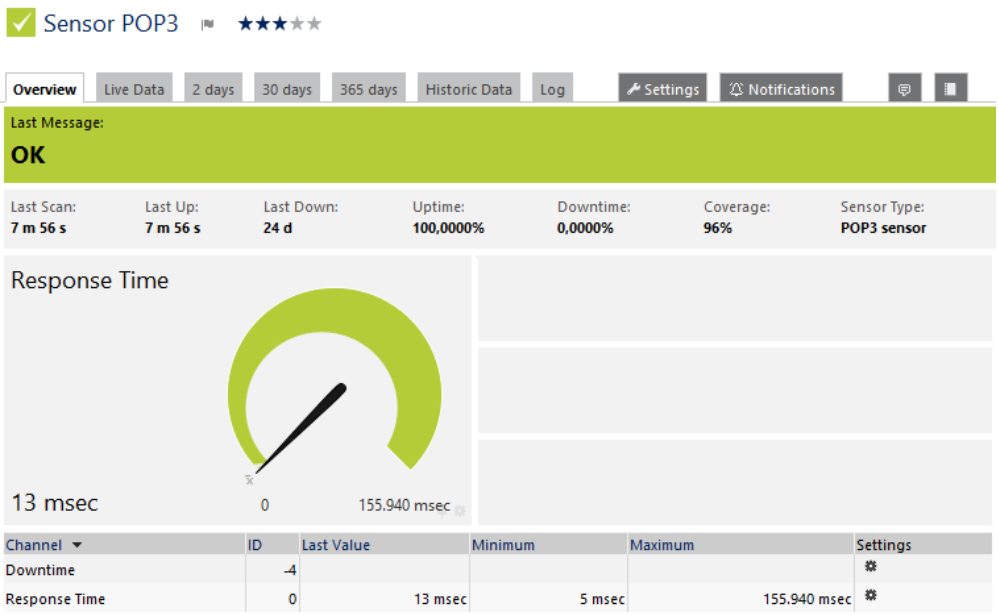
Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.89 POP3 Sensor

The POP3 sensor monitors an email server using Post Office Protocol version 3 (POP3).

- It shows the response time of the server.



POP3 Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/pop3.png

Remarks

- This sensor type does not support Secure Remote Password (SRP) ciphers.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

POP3 SPECIFIC

Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).
Port	Specify the port that the sensor uses for the POP3 connection. This is usually port 110 for non-secure connections and usually port 995 for SSL connections. The actual setting depends on the server you are connecting to. Please enter an integer value. We recommend that you use the default value. If you do not get a connection, please try another port number.

TRANSPORT-LEVEL SECURITY

Sensor Specific	Define the security level for the sensor connection. Choose between:

TRANSPORT-LEVEL SECURITY

- **Use Transport-Level Security if available using StartTLS (default)**: Choose this option to try to connect to the server using TLS and StartTLS. If the server does not support this, the sensor will try to connect without encryption.
- **Use Transport-Level Security if available**: Choose this option to try to connect to the server using TLS. If the server does not support this, the sensor will try to connect without encryption.
- **Enforce Transport-Level Security using StartTLS**: Choose this option to try connecting to the server using TLS and StartTLS. If the server does not support this, the sensor will show a **Down** status 163.
- **Enforce Transport-Level Security**: Choose this option to try to connect to the server using TLS. If the server does not support this, the sensor will show a **Down** status 163.

If the sensor connects to a server via StartTLS, the connection is established unencrypted first. After the connection is established, the sensor sends a certain command (StartTLS) over the unencrypted connection to negotiate a secure connection via the SSL/TLS protocol.

If the sensor uses TLS without StartTLS, the negotiation of a secure connection happens immediately (implicitly) so that no commands are sent in unencrypted plain text. If there is no secure connection possible, no communication will take place.

POP3 AUTHENTICATION

Type	Select the kind of authentication for the POP3 connection. Choose between: ▪ **Without login**: Monitor the connection to the POP3 server only. ▪ **Username and password**: Log on to the POP3 server with username and password (simple login, non-secure). ▪ **128-bit MD5 hash value (APOP)**: Send the password in an encrypted form using APOP. This option must be supported by the POP3 server you connect to.
Username	This field is only visible if you select an option with login above. Enter a username for POP3 authentication. Please enter a string.
Password	This field is only visible if you select an option with login above. Enter a password for POP3 authentication. Please enter a string.
Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section **Data Storage** 3226. You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

SENSOR DISPLAY

Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. ⓘ To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

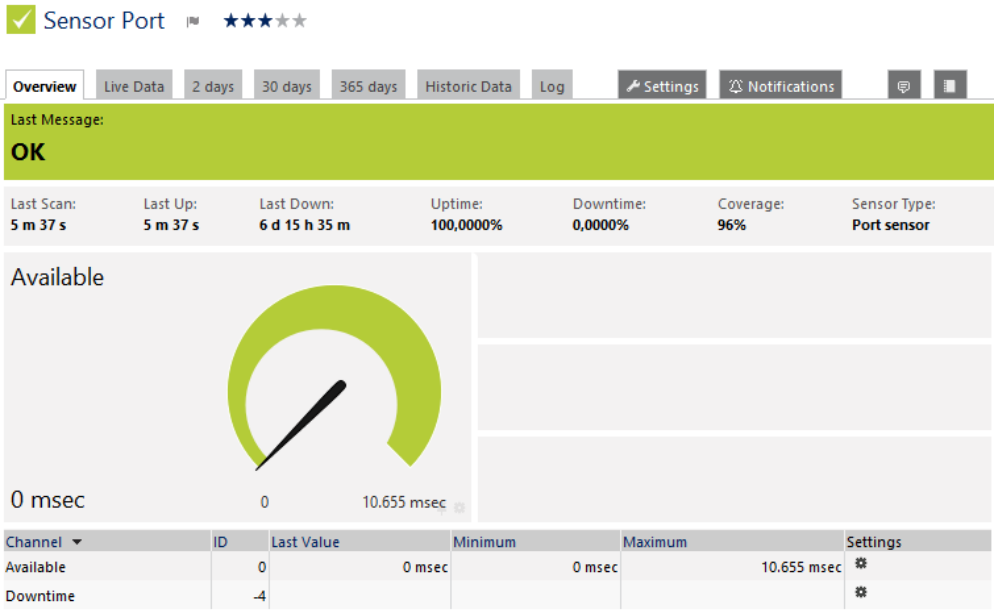
Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.90 Port Sensor

The Port sensor monitors a network service by connecting to its port. It tries to connect to the specified TCP/IP port number of a device and waits for the request to be accepted. Depending on your settings, it can alert you either when the monitored port is open, or when it is closed.

- The sensor shows the time until a request to a port is accepted.



Port Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/port.png

Remarks

- This sensor type does not support Secure Remote Password (SRP) ciphers.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

PORT SPECIFIC

Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).
Port	Enter the number of the port to which this sensor connects. Please enter an integer value.

TRANSPORT-LEVEL SECURITY

Security	Define the security level for the sensor connection. Choose between: ▪ **Use Transport-Level Security (default)**: Establish the connection with the strongest TLS method that the target device provides.

TRANSPORT-LEVEL SECURITY

- **Do not use Transport-Level Security**: Establish the connection without encryption.

ADVANCED SENSOR SETTINGS

Goal	Define how the sensor will report on the port defined above. Choose between: ▪ **Open**: The sensor shows a green **Up** status if the port is open, and a red **Down** status if the port is closed. ▪ **Closed**: The sensor shows a green **Up** status if the port is closed, and a red **Down** status if the port is open.
Command	Define whether the sensor will send a command after opening the port. Choose between: ▪ **Don't send command**: Only check if a connection to the port is possible. ▪ **Send command**: Open a Telnet session to the respective port and send the command. ⓘ You cannot use this option if the target machine is a web server.
Command	This field is only visible if you enable **Send command** above. Enter a command that the sensor sends in a Telnet session to the respective port. You cannot use line breaks, only a simple Telnet command in a single line. Please enter a string.
Response	Define if the sensor will process the received response further. Choose between: ▪ **Ignore response**: Do not check the response. ▪ **Check response code (integer)**: Check if the response matches a defined response code. Define below. ▪ **Check response text**: Check if the response matches a defined response text. Define below.
Allowed Code	This field is only visible if you enable **Check response code (integer)** above. Enter a code that the target device must return. If it does not match, the sensor will show a **Down** status. Please enter an integer value.

Check For Existing Keywords (positive)	This setting is only visible if you activated **Check response text** above. Check if a certain keyword is part of the received value. If there is no match, the sensor will show a **Down** status. ▪ **Disable**: Do not check for positive keywords. ▪ **Enable keyword check (positive)**: Check if a certain keyword exists in the received value. Define below.
Response Must Include	This setting is only visible if you activate keyword check above. Enter a search string that the returned value must contain.
For Keyword Search Use	Define the method that you want to use for the search string. Choose between: ▪ **Plain Text**: Search for a simple string. ▪ **Regular Expression**: Search using a regular expression. For more details, see **Regular Expressions** 3193 section.
Check For Existing Keywords (negative)	This setting is only visible if you activated text processing above. Check if a certain keyword is not part of the received value. If there is a match, the sensor will show a **Down** status. ▪ **Disable**: Do not check for negative keywords. ▪ **Enable keyword check (negative)**: Check if a certain keyword does not exist in the received value. Define below.
Text Must Not Include	This setting is only visible if you activate keyword check above. Enter a search string that the returned value must not contain.
For Keyword Search Use	Define the method you want to use for the search string. Choose between: ▪ **Plain Text**: Search for a simple string. ▪ **Regular Expression**: Search using a regular expression. For more details, see **Regular Expressions** 3193 section.

DEBUG OPTIONS

Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result.

DEBUG OPTIONS

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section Data Storage 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.
- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings 2782 settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

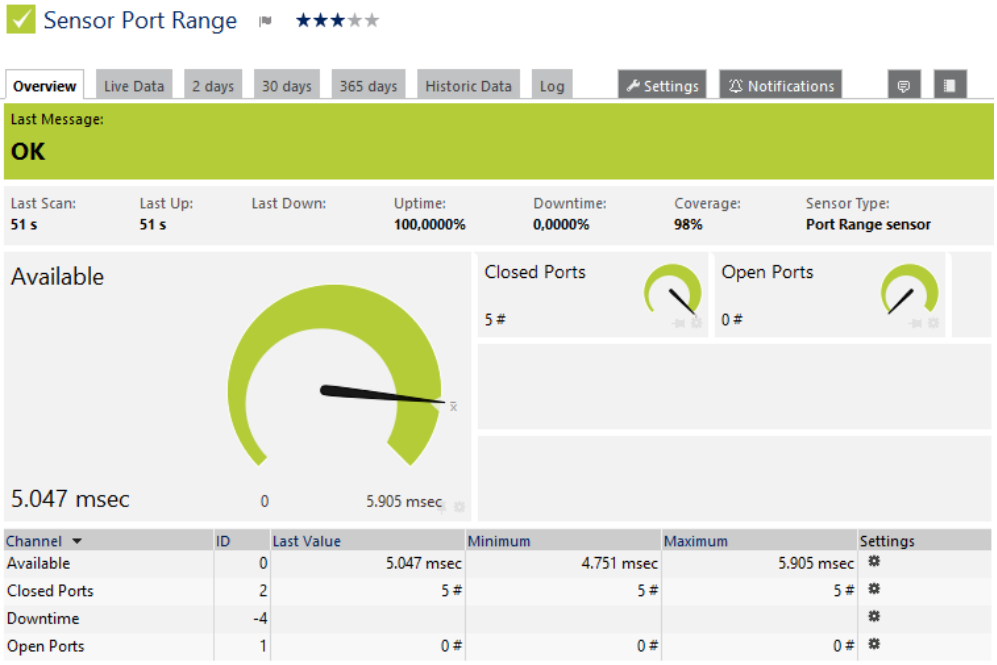
7.8.91 Port Range Sensor

The Port Range sensor monitors a network service by connecting to various TCP/IP ports. It tries to connect to the specified TCP/IP port numbers of a device in succession and waits for each request to be accepted.

It shows the following:

- Number of closed ports
- Number of open ports
- Time until requests are accepted

Optionally, you can set limits in the sensor channel settings 2782. This way you can get alerts about open and closed ports.



Port Range Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/port_range.png

Remarks

- This sensor type does not support Secure Remote Password (SRP) ciphers.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

PORT RANGE SPECIFIC

Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).
Port-by-Port-Delay (ms)	Specify in milliseconds how long the sensor will wait to go to the next port while running through all given ports.
Port Range Selection Method	Define whether you want to monitor all ports within a range or if you want to monitor several individual ports. Choose between: ▪ **Port range with start/end:** Monitor ports within a range. ▪ **List of ports:** Monitor several individual ports.
Range Start	This field is only visible if you enable **Port range with start/end** above. Enter the port number where the scan starts. Please enter an integer value.
Range End	This field is only visible if you enable **Port range with start/end** above. Enter the port number where the scan ends. Please enter an integer value.
Port List	This field is only visible if you enable **List of ports** above. Enter the numbers of the ports the sensor will try to connect to. Enter one or more individual integer values, each port in one line.
If Value Changes	Define what the sensor will do if the number of closed ports or open ports changes. Choose between: ▪ **Ignore changes**: No action is taken on change. ▪ **Trigger 'change' notification**: The sensor sends an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification 2791 whenever the sensor value changes.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

SENSOR DISPLAY

	You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

SCANNING INTERVAL

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

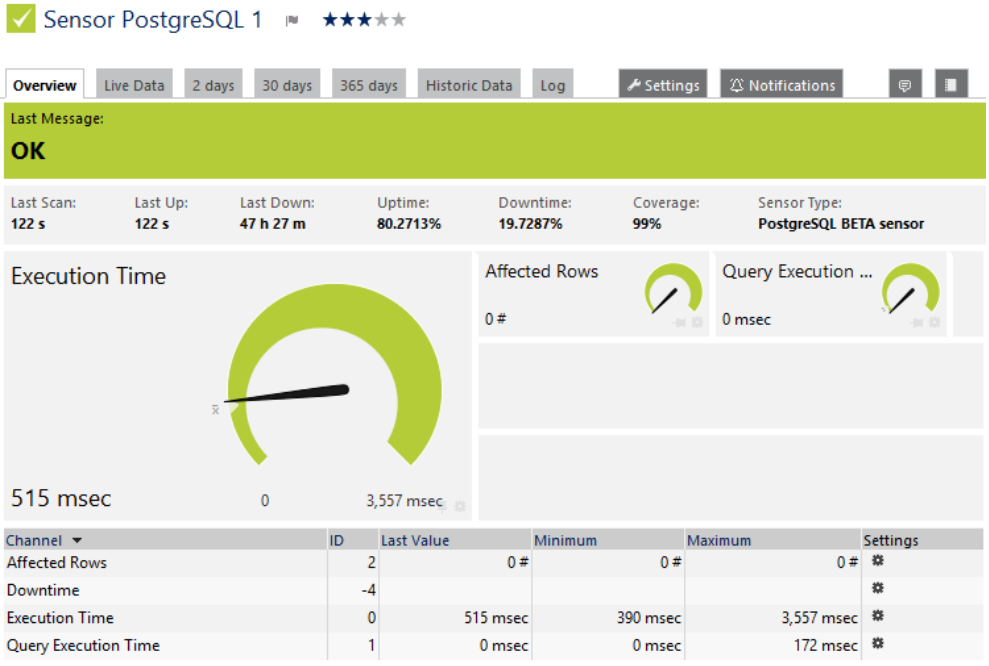
For more general information about settings, please see the **Object Settings** 188 section.

7.8.92 PostgreSQL Sensor

The PostgreSQL sensor monitors a database on a PostgreSQL server and executes a defined query.

It can show the following:

- Execution time of the whole request (including connection buildup, query execution, transaction handling, disconnection)
- Execution time of a given query
- Number of rows that were addressed by the query (including select statements if you process data tables)
- It can also process the data table and show defined values in individual channels.



PostgreSQL Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/postgresql.png

Remarks

- Requires 1364 .NET 4.0 on the probe system.
- Define credentials, custom port (if required), and timeout in settings section **Credentials for Database Management Systems** 370 of the parent device, or in the settings of a group or probe above.
- Your SQL query must be stored in a file on the system of the probe the sensor is created on. If you use it on a remote probe, store the file on the system running the remote probe. In a cluster setup, copy the file to every cluster node.

- Save the SQL script with the query into the **\Custom Sensors\sql\postgresql** subfolder of your PRTG installation. See manual section **Data Storage** 3226 for more information about how to find this path
- This sensor type supports PostgreSQL 7.x or later.
- PRTG Manual: **Monitoring Databases** 3120 (includes an example 3121 for channel value selection)
- Knowledge Base: How can I monitor strings from an SQL database and show a sensor status depending on it?

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Requirement: .NET Framework

This sensor type requires the Microsoft .NET Framework to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the remote probe 3196. If the framework is missing, you cannot create this sensor.

Required .NET version (with latest updates): .NET 4.0 (Client Profile is sufficient), .NET 4.5, or .NET 4.6.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/60543

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DATABASE SPECIFIC

Database	Enter the name of the PostgreSQL database to which the sensor connects (for example, MyDatabase). This is a logical entity on the database server where database objects like tables or stored procedures exist.
SSL Mode	Select the PostgreSQL SSL mode for the sensor connection. PostgreSQL SSL connections require OpenSSL to be installed on both the target server and on the PRTG probe system with this sensor. The SSL mode options you can choose here are the same as the values of the PostgreSQL sslmode parameter. PRTG sends it with the sensor requests. Choose between these SSL modes: ▪ **Disable** ▪ **Allow** ▪ **Prefer** ▪ **Require**

DATABASE SPECIFIC

For details about the PostgreSQL SSL modes, please refer to the PostgreSQL documentation.

DATA

SQL Query File

Select an SQL script file that includes a valid SQL statement to execute on the server. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

The script will be executed with every scanning interval. The list contains SQL scripts from the database management system specific **\Custom Sensors\sql** subfolder of your PRTG installation. Store your script there. If used on a remote probe, the file must be stored on the system running the remote probe. If used on a cluster probe, you must store the file on all servers running a cluster node!

For more information on how to find this path, please see **Data Storage** 3226 section. By default, there is the demo script **Demo Serveruptime.sql** available that you can use to monitor the uptime of the target server.

For example, a correct expression in the file could be: SELECT AVG (UnitPrice) FROM Products. If you want to use transactions, separate the individual steps with semicolons ";".

Please be aware that with each request, the full result set will be transferred, so use filters and limits in your query.

You can use the following placeholders in your query file to have them replaced by an input parameter:

- Microsoft SQL, MySQL, PostgreSQL: **@prtg**
- Oracle SQL: **:prtg**
- ADO SQL: **?** (question mark)

This is useful if you have various SQL sensors with queries that differ in only one parameter.

Use Input Parameter

Define if you want to pass a parameter to your SQL query file. This will replace the placeholder %prtg (Microsoft SQL, MySQL, PostgreSQL), or :prtg (Oracle SQL), or ? (ADO SQL) in the SQL query. Choose between:

DATA

- **Don't use input parameter (default)**: Execute the SQL query file without using placeholders.
- **Use input parameter**: Execute an SQL query file that contains a placeholder. Provide the parameter you want to use in the query below.

Input Parameter

This field is only visible if you choose **Use input parameter** above. Enter the parameter you want to pass to the SQL query file. This parameter replaces the placeholder %prtg or :prtg or ? in the SQL query.

You can also use PRTG placeholders for custom sensors (command line parameters) as input parameter, for example, %sensorid or %deviceid. For details, see **Application Programming Interface (API) Definition**.

Provide strings as they are and do not surround them with quotation marks. PRTG will correctly insert string parameters into the query automatically.

Use Transaction

Define if you want to use transactions and if they will affect the database content. Choose between:

- **Don't use transaction (default)**: No transactions will be executed.
- **Use transaction and always rollback**: Choose this option to ensure that no data in the database will be changed by the query. In the SQL query file, separate the single steps of the transaction with semicolons.
- **Use transaction and commit on success**: Choose this option to perform changes on the database with the query. The changes will only apply if all execution steps succeed without any errors. In the SQL query file, separate the single steps of the transaction with semicolons.

Data Processing

Define if you want to process data from the database. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew. Choose between:

- **Just execute the query**: If you select this option, the sensor will only show information about the number of affected rows and the execution time of the query. Affected rows are rows that were changed somehow with the query (for example, created, deleted, edited).
- **Count table rows**: Choose this option if you perform a SELECT statement and want to monitor how many rows of the data table this statement returns.

DATA

	▪ **Process data table**: Select this option to read and analyze the queried data table. If you select this option, the sensor will count rows with SELECT statements as well.
Handle DBNull in Channel Values as	This setting is only visible if you select **Process data table** above. Define the sensor behavior if DBNull is returned by the query. Choose between: ▪ **Error**: The sensor will show a **Down** status if DBNull is reported. ▪ **Number 0**: The sensor will recognize the result DBNull as a valid value and interpret it as the number 0.
Select Channel Value by	This setting is only visible if you select **Process data table** above. Define how the desired cell in the database table will be selected. This is necessary to configure the cells that will be used in the sensor channels. Choose between: ▪ **Column number**: The channel value will be determined by using the value in row 0 of the column whose number you specify below. ▪ **Column name**: The channel value will be determined by using the value in row 0 of the column whose name you specify below. ▪ **Row number**: The channel value will be determined by using the value in column 0 of the row whose number you specify below. ▪ **Key value pair**: The channel value will be determined by searching in column 0 for the key you specify below and returning the value in column 1 of the same row where the key value was found. The option you choose here also defines the method to optionally determine a value for the sensor message. For details, see setting **Use Data Table Value in Sensor Message** below. Please see manual section **Monitoring Databases** 3120 for an example 3121 for channel value selection.
Sensor Channel #x	This setting is only visible if you select **Process data table** above. You can define up to 10 different channels for the data processing of this sensor. You have to define at least one data channel if you process the data table, so you will see all available settings for Channel #1 without enabling it manually. For all other possible channels, choose between: ▪ **Disable**: This channel will not be added to the sensor. ▪ **Enable**: This channel will be added to the sensor. Define the settings as described above.

DATA

	Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Sensor Channel #x Name	This setting is only visible if you select **Process data table** above. Enter a unique name for the channel. Please enter a string. Channels will be generated dynamically with this name as identifier. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Sensor Channel #x Column Number	This setting is only visible if you select **Column number** above. Provide the number of the column which will be used to determine the channel value in row 0. Please enter an integer value.
Sensor Channel #x Column Name	This setting is only visible if you select **Column number** above. Provide the name of the column which will be used to determine the channel value in row 0. Please enter a string.
Sensor Channel #x Row Number	This setting is only visible if you select **Row number** above. Provide the number of the row which will be used to determine the channel value in column 0. Please enter an integer value.
Sensor Channel #x Key	This setting is only visible if you select **Key value pair** above. Provide the key to search for in column 0 of the data table. The value in column 1 of the same row where the key value was found will be used to determine the channel value. Please enter a string.
Sensor Channel #x Mode	This setting is only visible if you select **Process data table** above. Define how to display the determined value in the channel. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew. Choose between: ▪ **Absolute (recommended)**: Shows the value as the sensor retrieves it from the data table. ▪ **Difference**: The sensor calculates and shows the difference between the last and the current value returned from the data table.
Sensor Channel #x Unit	This setting is only visible if you select **Process data table** above. Define the unit of the channel value. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew. Choose between: ▪ BytesBandwidth

DATA

- BytesMemory
- BytesDisk
- Temperature
- Percent
- TimeResponse
- TimeSeconds
- TimeHours
- Count
- CPU
- BytesFile
- SpeedDisk
- SpeedNet
- Custom
- Value Lookup

For more information about the available units, please refer to the PRTG **Application Programming Interface (API) Definition** 3174 for custom sensors.

To use lookups 3183 with this channel, choose **Value Lookup** and select your lookup file below. Do not use **Custom** for using lookups with this sensor!

Sensor Channel #x Custom Unit

This setting is only visible if you select **Custom** above. Define a unit for the channel value. Please enter a string.

Sensor Channel #x Value Lookup

This settings is only visible if you select **Value Lookup** above. Select a lookup 3183 file that you want to use with this channel.

Use Data Table Value in Sensor Message

This setting is only visible if you select **Process data table** above. Define if the sensor message will show a value from the data table. Choose between:

- **Disable**: Do not use a custom sensor message.
- **Enable**: Define a custom sensor message with a defined value of the data table. Define the value selection below.

The method to determine a value for the sensor message is defined in setting **Select Channel Value by** above.

DATA

Sensor Message Column Number	This setting is only visible if you select **Column number** and **Use Data Table Value in Sensor Message** above. Enter the number of a column. The sensor message will show the value in row 0 of this column. Please enter an integer value. Columns and rows start with index 0.
Sensor Message Column Name	This setting is only visible if you select **Column name** and **Use Data Table Value in Sensor Message** above. Enter the name of a column. The sensor message will show the value in row 0 of this column. Please enter a string. Columns and rows start with index 0.
Sensor Message Row Number	This setting is only visible if you select **Row number** and **Use Data Table Value in Sensor Message** above. Enter the number of a row. The sensor message will show value in column 0 of this row. Please enter an integer value. Columns and rows start with index 0.
Sensor Message Key	This setting is only visible if you select **Key value pair** and **Use Data Table Value in Sensor Message** above. Enter a key to search for in column 0 of the data table. The sensor message will show the value in column 1 of the row where the key has been found. Please enter a string. Columns and rows start with index 0.
Sensor Message	This setting is only visible if you select **Use Data Table Value in Sensor Message** above. Define the sensor message. Please enter a string. Use the placeholder {0} at the position where the value will be added. Example: **The message is {0}**
If Sensor Message Changes	Define what this sensor will do when the sensor value changes. You can choose between: ▪ **Ignore changes (default)**: The sensor takes no action on change. ▪ **Trigger 'change' notification**: The sensor sends an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification 2791 whenever the sensor value changes.
Sensor Result	Define what PRTG will do with the sensor results. Choose between:

DATA

- **Discard sensor result**: Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section Data Storage 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.
- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings 2782 settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: How can I monitor strings from an SQL database and show a sensor status depending on it?

- https://kb.paessler.com/en/topic/63259

Knowledge Base: Which .NET version does PRTG require?

- https://kb.paessler.com/en/topic/60543

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

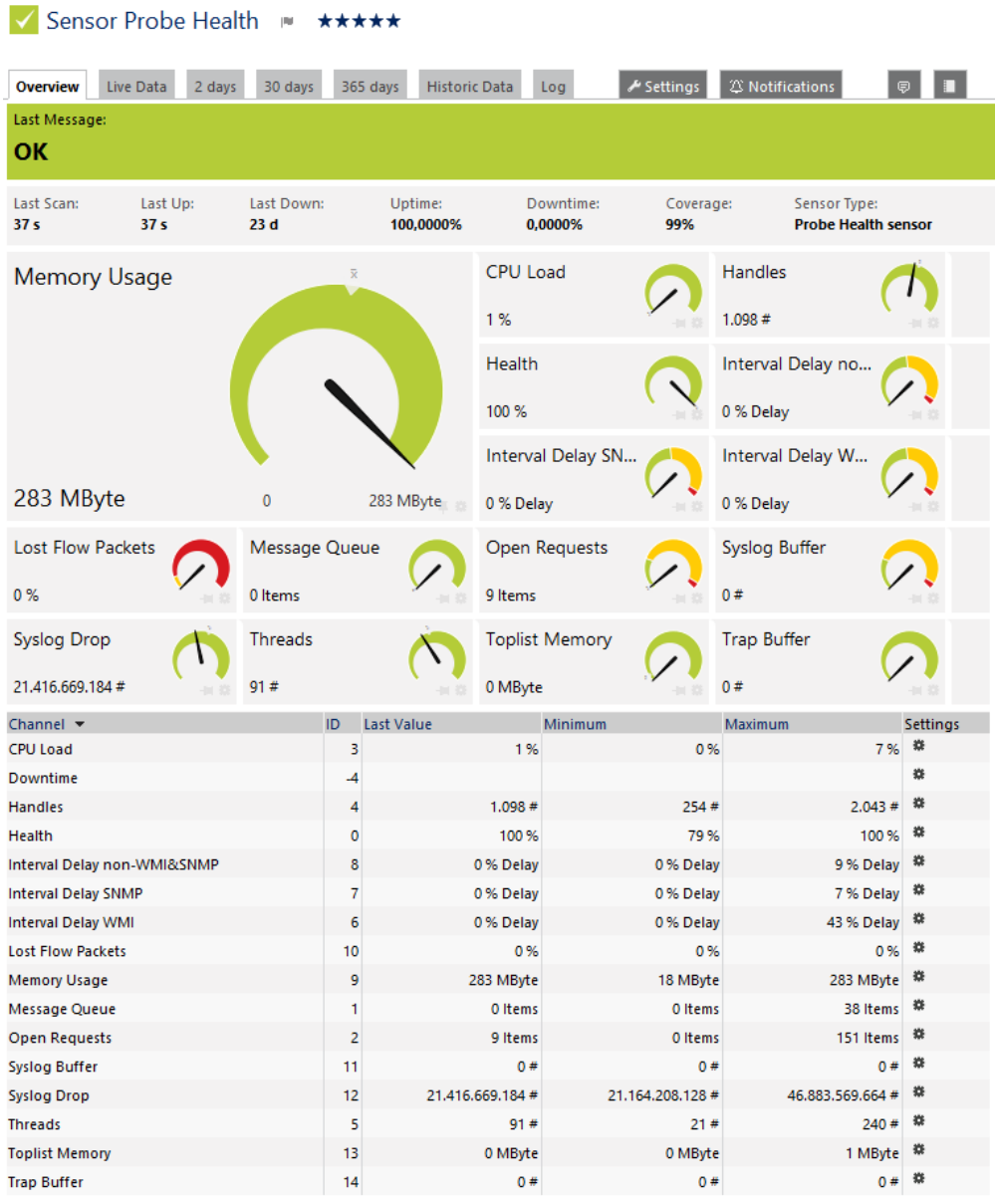
7.8.93 Probe Health Sensor

The Probe Health sensor monitors internal PRTG parameters. It shows the status of the PRTG probe (either for the local probe, a remote probe 3196, or a cluster 116 probe).

It checks various parameters of your PRTG system that can affect the quality of the monitoring results:

- **Health**: This index value sums up the probe state into a value between 100% (healthy) and 0% (failing). Frequent or repeated health values below 100% should be investigated.
- **Probe Process CPU Load**: This channel shows the current percentage CPU load that the probe process causes. Extensive CPU load can lead to false, incomplete, and incorrect monitoring results. This value usually should stay below 50%.
- **Data Storage Free**: This channel shows the free disk space on the probe system.
- **Handles**: This is a counter for the data structures of the operating system. It is responsible for internal resource management. Repeated obviously increasing values should be investigated.
- **Interval Delay non-WMI&SNMP**: This channel shows the percentage interval delay for all sensor types which are not from the type SNMP or WMI. If this value is over 0%, try to increase the scanning intervals 307 or distribute your sensors over multiple probes 3196.
- **Interval Delay SNMP**: This channel shows the percentage interval delay for SNMP sensors. If this value is above 0%, there are probably too many very slow SNMP V3 sensors. In this case, try to increase the monitoring intervals 307 or distribute the sensors over several probes 3196.
- **Interval Delay WMI**: This channel shows the percentage interval delay for WMI sensors. If this value is above 0%, WMI sensors could not check the target device according to their interval. 100% means that WMI sensors on the average are checked with twice their interval. For values above 0% try to increase the monitoring intervals 307 or distribute the sensors over several probes 3196 to keep the number of WMI sensors per probe below 120 (with 60 seconds interval) or 600 (with 300 seconds interval).
- **Lost Flow Packets**: This channel shows the percentage of lost flow 3099 packets. The higher this value, the less flow packages PRTG can handle. Usually, this value should be 0%. Investigate increasing values.
- **Memory Usage**: This channel shows the amount of memory being used by the PRTG probe service as reported by the memory manager. Repeated obviously increasing values should be investigated. If the value is constantly above 2 GB this indicates that PRTG runs at its limits. In this case you should distribute some sensors to Remote Probe 3196.
- **Message Queue**: This channel shows the number of monitoring results from the probe which have not been processed yet by the core. This value usually should stay below 1/10 of the sensor count.
- **Open Requests**: This channel shows the number of currently active monitoring requests. This value should stay below the maximum of 500 open requests.
- **Syslog Buffer**: This channel shows the number of buffered syslog packages. Usually, this value should be 0 (or very low). Investigate increasing values.
- **Threads**: This channel shows the number of program parts which are running simultaneously currently. This value can increase with heavy load. The number should not exceed 100 in normal operation.

- **Toplist Memory**: This channel shows the amount of RAM that the Toplists 2806 on this probe are using. Stay below 1 GB memory usage (depending on available memory on the probe system). If necessary, reduce the number of toplists or distribute them on multiple probes 3196 .
- **Trap Buffer**: This channel shows the number of buffered SNMP traps. Usually, this value should be 0 (or very low). Investigate increasing values.



Channel	ID	Last Value	Minimum	Maximum	Settings
CPU Load	3	1 %	0 %	7 %	
Downtime	-4				
Handles	4	1.098 #	254 #	2.043 #	
Health	0	100 %	79 %	100 %	
Interval Delay non-WMI&SNMP	8	0 % Delay	0 % Delay	9 % Delay	
Interval Delay SNMP	7	0 % Delay	0 % Delay	7 % Delay	
Interval Delay WMI	6	0 % Delay	0 % Delay	43 % Delay	
Lost Flow Packets	10	0 %	0 %	0 %	
Memory Usage	9	283 MByte	18 MByte	283 MByte	
Message Queue	1	0 Items	0 Items	38 Items	
Open Requests	2	9 Items	0 Items	151 Items	
Syslog Buffer	11	0 #	0 #	0 #	
Syslog Drop	12	21.416.669.184 #	21.164.208.128 #	46.883.569.664 #	
Threads	5	91 #	21 #	240 #	
Toplist Memory	13	0 MByte	0 MByte	1 MByte	
Trap Buffer	14	0 #	0 #	0 #	

Probe Health Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/probe_health.png

Remarks

- PRTG creates this sensor automatically and you cannot delete it.

- You can create this sensor only on a probe device (either local probe, a remote probe 3196, or a cluster 116 probe).
- Knowledge Base: My probe system is running out of disk space. What can I do?

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

SENSOR DISPLAY

	You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

SCANNING INTERVAL

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: My probe system is running out of disk space. What can I do?

- https://kb.paessler.com/en/topic/64628

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

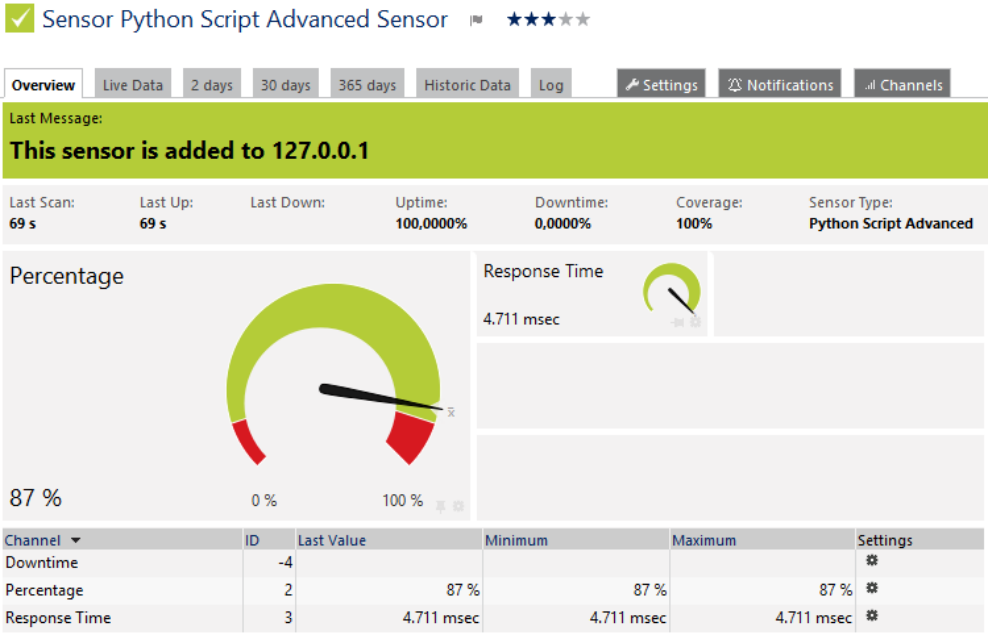
For more general information about settings, please see the **Object Settings** 188 section.

7.8.94 Python Script Advanced Sensor

The Python Script Advanced sensor executes a Python script on the computer running the local or remote probe. This option is provided as part of the PRTG Application Programming Interface (API). The return value of this sensor must be valid JSON or XML. For details about the return value format, please see the Application Programming Interface (API) Definition 3174.

PRTG includes a CPython 3.4.2 interpreter to execute Python scripts for this sensor type. Because of this you, do not have to install anything manually to use the Python Script Advanced sensor. Your Python scripts must be compatible with Python 3 to run with this interpreter. It is located in the the **\Python34** subfolder of your PRTG program directory. You can find the paepy package to easily create PRTG API conforming JSON output in the **\Python34\Lib\site-packages** folder.

- The sensor can show values returned by the Python script in multiple channels.



Python Script Advanced Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/python_script_advanced.png

Remarks

- You must store the script file on the system of the probe where you create the sensor: If used on a remote probe, you must store the file on the system running the remote probe. In a cluster setup, copy the file to every cluster node.
- For best sensor usage, we recommend that the return value is JSON encoded.
- The timeout of the sensor is its scanning interval 1390 minus 1 second. Ensure your Python script does not run longer than this.
- Print commands in the Python script are not supported and lead to an invalid JSON result.
- Exceptions in the script are not supported.

- Sensor channel values greater than 2^62 are not supported.
- We recommend Windows 2012 R2 on the probe system for best performance of this sensor.
- This sensor does not support more than 50 channels[1386] officially.
- Knowledge Base: What is the Mutex Name in PRTG's EXE/Script Sensor's settings?

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Limited to 50 Sensor Channels

PRTG does not support more than 50 sensor channels officially. Depending on the data used with this sensor type, you might exceed the maximum number of supported sensor channels. In this case, PRTG will try to display all sensor channels. However, please be aware that you will experience limited usability and performance.

Add Sensor

The **Add Sensor** dialog appears when you manually[288] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SENSOR SETTINGS

Python Script

Select a Python script from the list. The sensor will execute it with every scanning interval[1390].

This list shows all Python script files available in the **\Custom Sensors\python** subdirectory of the probe system's PRTG program directory (see **Data Storage**[3226]). For the files to appear in this list, please store the files into this folder ending in PY. To show the expected values and sensor status, your files must return the expected XML or JSON format to standard output. Values and message must be embedded in the XML or JSON. We recommend JSON encoded return values.

For detailed information on how to build custom sensors and for the expected return format, please see the API documentation (**Application Programming Interface (API) Definition**[3174]). There, find detailed information on the **Custom Sensors** tab.

When using custom sensors on the **Cluster Probe**, please copy your files to every cluster node installation.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SETTINGS

Python Script	Shows the Python script file that the sensor executes with each scan as defined at sensor creation. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Security Context	Define the Windows user account that the sensor uses to run the Python interpreter. Choose between:

SENSOR SETTINGS

- **Use security context of probe service**: Run the selected file under the same Windows user account the probe is running on. By default, this is the Windows system user account (if not manually changed).
- **Use Windows credentials of parent device**: Use the Windows user account defined in the settings of the parent device on which you create this sensor. Please navigate to the parent device settings 360 of this sensor to change these Windows credentials.

Device Credentials

Define if you want to transmit device credentials to the Python script. PRTG adds the device credentials to the JSON object that is passed to the script as command line parameter. Please navigate to parent device settings 360 of this sensor to change these credentials. Choose between:

- **Do not transmit device credentials**: No device credentials are given to the script.
- **Transmit Windows credentials**: Windows credentials 365 are given to the script.
- **Transmit Linux credentials**: Linux credentials 365 are given to the script.
- **Transmit SNMP credentials**: SNMP credentials 368 are given to the script.
- **Transmit all device credentials**: Windows, Linux, and SNMP credentials are all given to the script.

All parameters are transmitted in plain text.

Additional Parameters

Define additional parameters to add to the JSON object that is passed to the script as command line parameter.

Please enter a string or leave the field empty.

All parameters are transmitted in plain text.

Mutex Name

Define any desired mutex name for the process. All script sensors having the same mutex name will be executed serially (not simultaneously). This is useful if you use a lot of sensors and want to avoid high resource usage caused by processes running simultaneously. Please enter a string or leave the field empty.

For more details, please see this Knowledge Base article: What is the Mutex Name in PRTG's EXE/Script Sensor's settings?

DEBUG OPTIONS

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result**: Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section Data Storage 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

You can use **Write sensor result to disk** to inspect the passed JSON object that contains all parameters (PRTG on premises only). This way you can find out which key you can access when you script.

Transmitted passwords are masked in the log file.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.
- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings 2782 settings).

SENSOR DISPLAY

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.

SCANNING INTERVAL

- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** Custom channel types can be set on sensor level only.

More

Knowledge Base: What is the Mutex Name in PRTG's EXE/Script Sensor's settings?

- https://kb.paessler.com/en/topic/6673

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.95 QoS (Quality of Service) One Way Sensor

The QoS (Quality of Service) One Way sensor monitors parameters regarding the quality of a network connection between two probes. This is important, for example, when using Voice over IP (VoIP) over this connection.

The sensor sends a series of UDP packets from the parent probe to another probe and measures these parameters:

- Jitter in milliseconds (maximum, minimum, average)
- Packet delay variation in milliseconds (maximum, minimum, average)
- Corrupted packets in percent
- Duplicated packets in percent
- Lost packets in percent
- Packets out of order in percent
- Time to last packet in milliseconds

Channel	ID	Last Value	Minimum	Maximum	Settings
Downtime	-4				
Jitter Average	7	3 ms	0 ms	7 ms	
Jitter Max	8	3 ms	0 ms	11 ms	
Jitter Min	6	0 ms	0 ms	0 ms	
Packet Delay Variation Average	10	0 ms	0 ms	0 ms	
Packet Delay Variation Max	11	29 ms	1 ms	79 ms	
Packet Delay Variation Min	9	-21 ms	-21 ms	-1 ms	
Packets Corrupted	5	0 %	0 %	0 %	
Packets Duplicated	4	0 %	0 %	0 %	
Packets Lost	2	0 %	0 %	0 %	
Packets Out of Order	3	0 %	0 %	0 %	
Time to Last Packet	0	20.988 msec	20.981 msec	21.004 msec	

QoS (Quality of Service) One Way Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/qos.png

Remarks

- You have to configure at least one remote probe [3195] in your PRTG on premises setup for this sensor to work, and at least two remote probes in PRTG on demand.
- You can create this sensor on the Probe Device of either a local or remote probe.
- For a general introduction to the technology behind Quality of Service monitoring, please see manual section **Monitoring Quality of Service** [3104].

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you manually [288] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** [360] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree [151], as well as in alarms [190], logs [198], notifications [2829], reports [2862], maps [2885], libraries [2845], and tickets [200].
Parent Tags	Shows **Tags** [124] that this sensor inherits [124] from its parent device, group, and probe [118]. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** [124], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

BASIC SENSOR SETTINGS

	You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

QUALITY OF SERVICE MEASUREMENT

Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).
Target Probe	Define the target probe that will receive the UDP packets. The dropdown menu shows all local and remote probes in your setup. When running the sensor on the PRTG on premises local probe, select a remote probe as **Target Probe**. If no remote probe is available, please install and connect a remote probe 3195 first. When running the sensor on a remote probe, select either another remote probe or the local probe in PRTG on premises as target. The sensor will measure values for the network track between the probe the sensor is created on and the target probe. You must ensure that firewalls, NAT rules, etc. allow UDP packets to reach the target probe. The Windows firewall on the target system will be opened automatically by the probe. In PRTG on demand you can only select another remote probe as target probe. QoS measurements for connections to the cloud probe are not are not possible.
Target Host/IP	Define the IP address of the target probe to which the probe the sensor is created on connects. If you do not use NAT rules, this is usually the address shown above next to the target probe's name.
Port	Define the **source** and **target** port for the UDP packets. This port is used on both the source and target probe. Use a different port for each QoS sensor to make sure packets can be assigned correctly. Enter an integer value between 1024 and 65536.

QUALITY OF SERVICE MEASUREMENT

	This port must be available on both the source and target system.
Number of Packets	Define how many packets the sensor sends with each scanning interval. Please enter an integer value. Default value is **1000**. We recommend that you use the default value.
Size of Packets (Bytes)	Define the size in bytes of the packets that the sensor sends. Please enter an integer value. Default value is **172**. We recommend that you use the default value.
Time between Packets (ms)	Define the time in milliseconds that the sensor waits between two packets. Please enter an integer value. Default value is **20**. We recommend that you use the default value.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. ⓘ Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.96 QoS (Quality of Service) Round Trip Sensor

The QoS (Quality of Service) Round Trip sensor monitors parameters regarding the quality of a network connection between two probes. This is important, for example, when using Voice over IP (VoIP) over this connection. The sensor sends a series of UDP packets from the source probe to a target at the 'end' of the connection line. Then, the packets are sent back to the original probe ("round trip").

The sensor measures the following parameters:

- Jitter in milliseconds (maximum, minimum, average)
- Packet delay variation in milliseconds (maximum, minimum, average)
- MOS (Mean Opinion Score)
- Corrupted packets in percent
- Duplicated packets in percent
- Lost packets in percent
- Packets out of order in percent
- Round trip time (RTT) in milliseconds (maximum, minimum, average)
- Time to last packet in milliseconds

Channel	ID	Last Value	Minimum	Maximum	Settings
Downtime	-4				
Jitter Average	7	6 msec	0 msec	53 msec	
Jitter Max	8	9 msec	0 msec	738 msec	
Jitter Min	6	0 msec	0 msec	8 msec	
MOS	12	4.4	1.0	4.4	
Packet Delay Variation Average	10	0 msec	-12 msec	0 msec	
Packet Delay Variation Max	11	26 msec	6 msec	4,597 msec	
Packet Delay Variation Min	9	-27 msec	-4,555 msec	-6 msec	
Packets Corrupted	5	0 %	0 %	0 %	
Packets Duplicated	4	0 %	0 %	0 %	
Packets Lost	2	0 %	0 %	92 %	
Packets Out of Order	3	0 %	0 %	0 %	
RTT (Average)	13	2 msec	2 msec	57 msec	
RTT (Maximum)	15	28 msec	8 msec	4,601 msec	
RTT (Minimum)	14	0 msec	0 msec	0 msec	
Time to Last Packet	0	31,329 msec	4,909 msec	60,995 msec	

QoS (Quality of Service) Round Trip Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/qos_round_trip.png

Remarks

- You have to configure at least one remote probe [3195] in your PRTG on premises setup and at least two remote probes in PRTG on demand, or you need to set up the PRTG QoS Reflector tool on the target machine at the endpoint of the monitored connection.
- Knowledge Base: How can I monitor QoS roundtrips without using remote probes?
- Knowledge Base: How does PRTG calculate the MOS score for QoS sensors?
- For a general introduction to the technology behind Quality of Service monitoring, please see manual section **Monitoring Quality of Service** [3104].

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

QUALITY OF SERVICE MEASUREMENT

Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).
QoS Target	Define the type of target that will receive the UDP packets. Choose between: ▪ **PRTG Probe (recommended)**: The connection endpoint is a PRTG probe. ▪ **Custom Target**: Choose this option if you want to use the PRTG QoS Reflector as connection endpoint. See section **More** 1411 for information about this tool.
Target Probe	This setting is only available if you select PRTG probe as QoS target. In the dropdown menu, you see all local and remote probes of your setup. When running the sensor on the PRTG on premises local probe, select a remote probe as **Target Probe**. If no remote probe is available, install and connect a remote probe 3195 first or use the QoS Reflector. When running the sensor on a remote probe, select either another remote probe or the local probe in PRTG on premises as target. The sensor will measure values for the network track between the probe the sensor is created on and the target probe. You must ensure that firewalls, NAT rules, etc. will allow the UDP packets to reach the target probe. The Windows firewall on the target system will be automatically opened by the probe. For further information, see the **More** 1411 section below. In PRTG on demand you can only select another remote probe as target probe. QoS measurements for connections to the cloud probe are not are not possible.
Target Host/IP	Define the IP address of the QoS target. If you use the QoS Reflector, enter the address of the machine on which the reflector script runs. If you use a probe, enter the address of the probe to which the probe the sensor is created on connects. If you do not use NAT rules, this is usually the address shown above next to the target probe's name.
Port	Define the **source** and **target** port for the UDP packets. This port will be used on both the source and target probe. Use a different port for each QoS sensor to make sure packets can be assigned correctly. Enter an integer value between 1024 and 65536. This port must be available on both the source and target system.
Number of Packets	Define how many packets the sensor sends for each scanning interval. Please enter an integer value. Default value is **1000**. We recommend that you use the default value.
Size of Packets (Bytes)	Define the size in bytes of the packets that the sensor sends.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: How does PRTG calculate the MOS score for QoS sensors?

- https://kb.paessler.com/en/topic/59491

Knowledge Base: How can I monitor QoS roundtrips without using remote probes?

- https://kb.paessler.com/en/topic/61176

Knowledge Base: What connection settings are necessary for the QoS (Quality of Service) Round Trip Sensor?

- https://kb.paessler.com/en/topic/65410

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

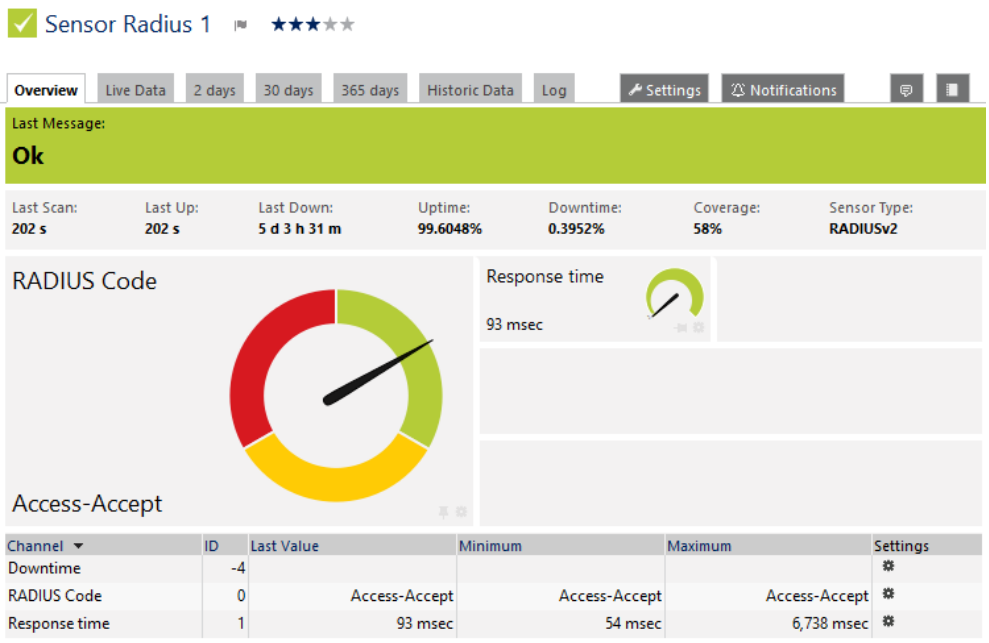
Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.97 RADIUS v2 Sensor

The RADIUS v2 sensor monitors a Remote Authentication Dial-In User Service (RADIUS) server according to RFC 2865. The sensor tries to authenticate at the server and shows the following:

- Response time
- RADIUS code: Access-Accept (sensor status [163] **Up**), Access-Challenge (sensor status **Warning**), Access-Reject (sensor status **Down**)
- If authentication fails, the sensor shows a **Down** status [163].



RADIUS v2 Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/radius_v2.png

Remarks

- Requires [1413] .NET 4.5 on the probe system.
- This sensor only supports plain text authentication (Password Authentication Protocol (PAP)).
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** [3183].

Requirement: .NET Framework

This sensor type requires the Microsoft .NET Framework to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the remote probe [3196]. If the framework is missing, you cannot create this sensor.

Required .NET version (with latest update): .NET 4.5 or .NET 4.6. Please see the section **More** below for details.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

RADIUS SPECIFIC

Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value, the request is aborted and an error message is triggered. The maximum value is 900 seconds (15 minutes). Please enter an integer value.
User	Enter the username that is used for authentication at the RADIUS server. Please enter a string.
Password	Enter the password that is used for authentication between the client (this is the PRTG probe on which the sensor runs) and the RADIUS server. Please enter a string.
Secret	Enter the shared secret that is used for authentication between the authenticator (this is the PRTG probe) and the RADIUS server. Please enter a string.
Port	Enter the port number that is used for the connection to the RADIUS server. The default value is **1812**. Please enter an integer value.
Network Access Server	Define how to identify the Network Access Server (NAS). Choose between: ▪ **Use NAS IP address**: Enter the IP address for identification below. ▪ **Use NAS identifier**: Enter the identifier below.
NAS IP Address	This field is only visible if you select **Use NAS IP address** as an identification method above. Enter a valid IP address for the Network Access Server (NAS) that originates the access request.
NAS Identifier	This field is only visible if you select **Use NAS identifier** above. Enter an identifier for the NAS that originates the access request.
Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section **Data Storage** 3226.

- You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: Which .NET version does PRTG require?

- https://kb.paessler.com/en/topic/60543

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

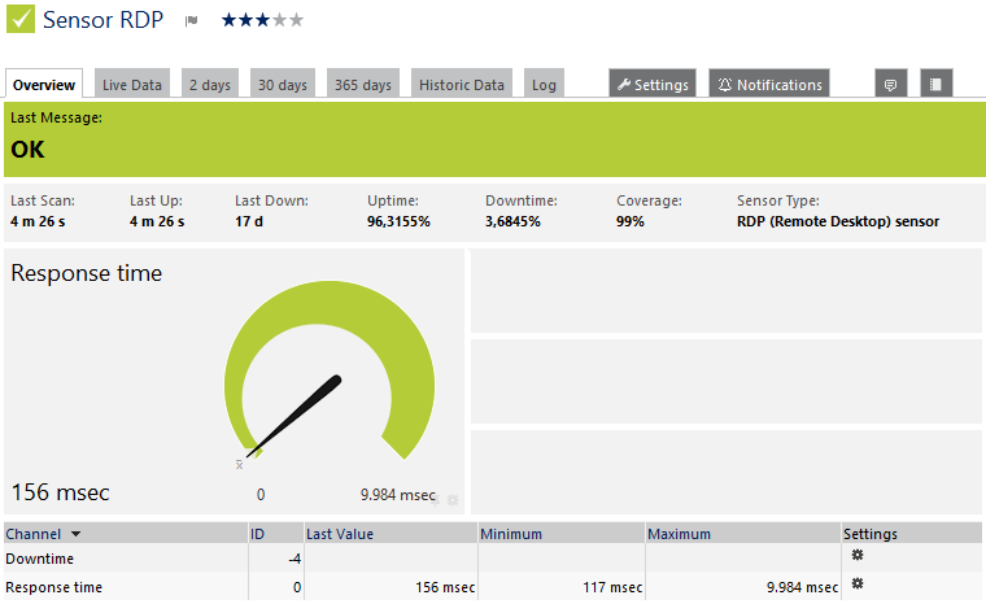
Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.98 RDP (Remote Desktop) Sensor

The RDP (Remote Desktop) sensor monitors remote desktop services (RDP, Terminal Services Client).

- It shows the response time of the service.



RDP (Remote Desktop) Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/rdp_remote_desktop.png

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SPECIFIC

Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).
Port	Enter the number of the port to which this sensor connects. Please enter an integer value. Default value is **3389**. We recommend that you use the default value.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

SENSOR DISPLAY

	You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

SCANNING INTERVAL

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: Does PRTG impair my Citrix environment?

- https://kb.paessler.com/en/topic/61880

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

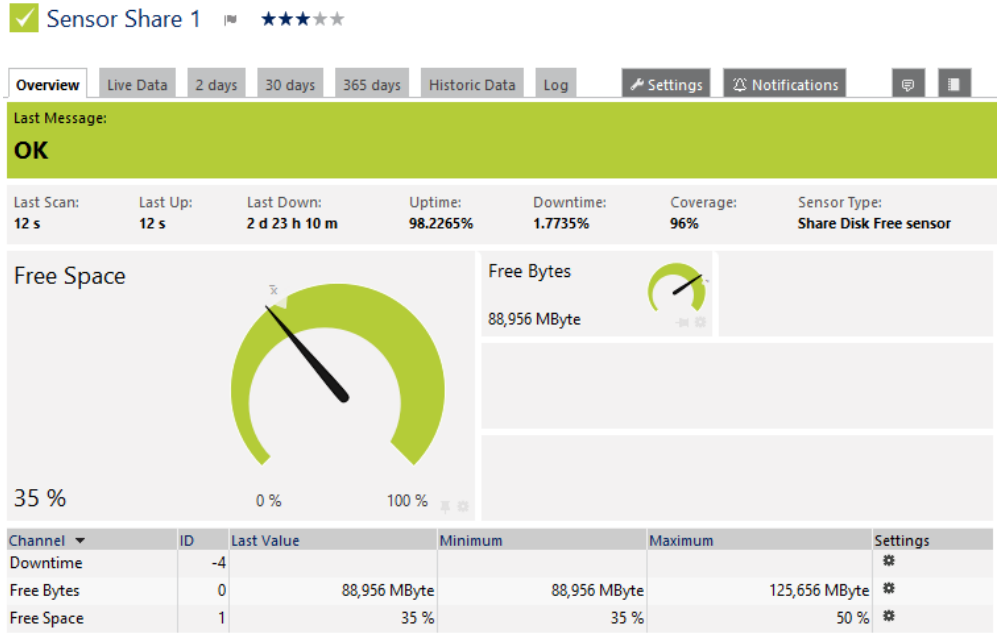
Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.99 Share Disk Free Sensor

The Share Disk Free sensor monitors free disk space of a share (Windows/Samba) using Server Message Block (SMB).

- It shows the free disk space in percent and bytes.



Share Disk Free Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/share_disk_free.png

Remarks

- Requires 1430 the LanmanServer Windows service to be running on the target device.
- This sensor only works if no quotas are enabled on the target share. If there are quotas enabled for the user account this sensor uses to connect to the share, the absolute value will be okay, but the percentage variable will show wrong values.
- Knowledge Base: What can I do if PRTG doesn't succeed with monitoring a share? PE029 PE032

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Requirement: LanmanServer Windows Service

To monitor shares on Windows machines, please make sure the LanmanServer "Server" Windows service is running on the target computer.

To enable the service, please log in to the respective computer and open the services manager (for example, via services.msc). In the list, find the respective service and set its Start Type to Automatic.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SHARE CONFIGURATION

Share

Enter the name of the share this sensor will monitor. Only a share name is allowed here (for example, enter C$). Please do not enter a complete UNC name here. The server name (\\server\) is taken from the parent device of this sensor.

To provide any shares under Windows, the LanmanServer "Server" Windows service must be running on the target computer.

Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.
- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: What can I do if PRTG doesn't succeed with monitoring a share? PE029 PE032

- https://kb.paessler.com/en/topic/513

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.100 Sensor Factory Sensor

The Sensor Factory sensor is a powerful tool that allows you to monitor entire business processes that involve several components.

You can define one or more channels that combine monitoring results from other sensors or devices. You can create your own individual sensor with channels based on data from other sensors or devices.

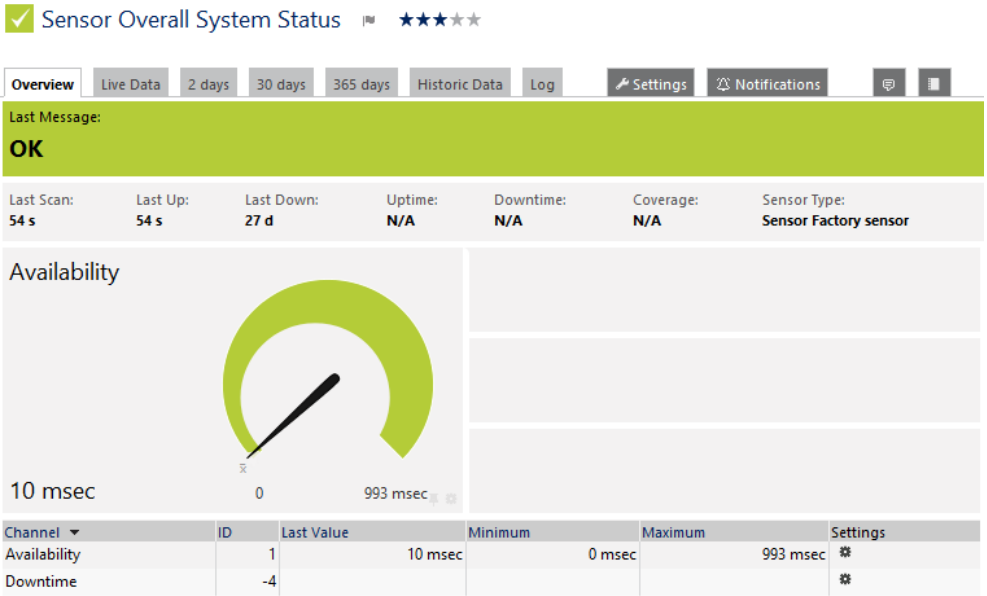
Samples for usage are:

- Show single channels of one or more sensors in one graph.
- Use the data from single channels of one or more sensors to calculate new values (for example, you can subtract, multiply, and divide).
- Create graphs with data from other sensor channels and add horizontal lines at specific vertical positions.

The Sensor Factory sensor does not show values in the **Downtime** channel because they cannot be calculated for this sensor type.

If you want to create only a cumulated sensor status based on specific source sensors, we recommend that you use the **Business Process Sensor** 528 instead.

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Sensor Factory Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/sensor_factory.png

Remarks

- This sensor does not support more than 50 channels [1439] officially.
- Ensure the scanning interval [1442] of this sensor is equal to or greater than the scanning interval of the source sensor(s) to avoid incorrect sensor behavior. For example, "no data" messages or erratic changes of the sensor status can be a result of an invalid scanning interval.
- Knowledge Base: How can I monitor the overall status of the business process "Email"?
- The Sensor Factory sensor might not work with flow sensors [3099]. Sensor types using active flow timeout, this is, NetFlow and jFlow sensors [386], are not supported by the Sensor Factory sensor.
- Reports [175] cannot show uptime or downtime data for this sensor type.
- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.

Limited to 50 Sensor Channels

PRTG does not support more than 50 sensor channels officially. Depending on the data used with this sensor type, you might exceed the maximum number of supported sensor channels. In this case, PRTG will try to display all sensor channels. However, please be aware that you will experience limited usability and performance.

Add Sensor

The **Add Sensor** dialog appears when you manually [288] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** [360] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR FACTORY SPECIFIC SETTINGS

Channel Definition	Enter a channel definition for the sensor. Using a specific syntax, you can refer to data from channels of other sensors here. You can also calculate values. Enter one channel definition for each new channel you want to add to this sensor. Please see section **Define Sensor Channels** 1446 below.
Error Handling	Define the behavior of the sensor if one of the sensors defined above is in an error status. In this case, you can set the sensor factory sensor either to down or to warning status. Choose between:

SENSOR FACTORY SPECIFIC SETTINGS

- **Factory sensor shows error status when one or more source sensors are in error status**: If at least one sensor that you use in a channel definition is in a **Down** status, the Factory sensor shows a **Down** status as well until all referred sensors leave this status. While the Sensor Factory sensor is **Down**, it will still show data of all available sensor channels.
  If a lookup definition 3183 or an error limit 2783 triggers the error status of the source sensor, the Sensor Factory will not show a **Down** status. This is because the Sensor Factory should only show this status if it cannot calculate values.
- **Factory sensor shows warning status when one or more source sensors are in error status**: If at least one sensor that you use in a channel definition is in a **Down** status, the factory sensor shows a **Warning** status until all referred sensors leave the **Down** status.
  If a lookup definition 3183 or an error limit 2783 triggers the error status of the source sensor, the Sensor Factory will not show a **Warning** status. This is because the Sensor Factory should only show this status if it cannot calculate values.
- **Use custom formula**: Define the status of the Factory sensor by adding a status definition in the field below.

Status Definition

This field is only visible if you choose **Use custom formula** above. Define when the sensor will switch to a **Down** status. You can use the status() function in combination with Boolean operations. For advanced users it is also possible to calculate a status value. Please see section **Define Sensor Status** 1453 below.

If a Sensor Has No Data

Choose how this Sensor Factory sensor reacts if a sensor referred to in the channel definition does not provide any data (for example, because it is paused or does not exist). Choose between:

- **Do not calculate factory channels that use the sensor**: For defined channels that use one or more sensor(s) that deliver no data, no data is shown.
- **Calculate the factory channels and use zero as source value**: If a sensor that you use in a channel definition does not deliver any data, zero values will be filled in instead. The sensor factory calculates the channel value and shows it using these zero values.

In the case a sensor in the channel of a factory sensor has no data, the factory sensor will always show a **Warning** status, no matter which of the above options you select.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

Define Sensor Channels

The channels of a Sensor Factory sensor are controlled by the **Channel Definition** text field. Using a special syntax you can refer to other sensor channels, calculate values, and add horizontal lines. You can define factory sensor channels using data from any other sensor's channels on your PRTG server.

Example

You see a definition of two factory sensor channels. Both use the channel() function which simply collects data from the channels of other sensors in your monitoring and displays them:

```
#1:Local Probe Health
channel(1001,0)
#2:Local Traffic Out[kbit]
channel(1004,1)
```

The first channel of the factory sensor (#1) collects data from the **Health** channel (ID 0) of the **Probe Health** sensor (ID 1001) running on the Local Probe device. The second channel (#2) collects data from the **Traffic out** channel (ID 1) of a traffic sensor (ID 1004) measuring the system's local network card. Both channels will be shown together in the factory sensor's data tables and graphs.

The basic syntax for a sensor factory channel definition looks like this:

```
#<id>:<name>[<unit>]
<formula>
```

For each channel one section is used. A section begins with the # sign. Function names in formulas are not case sensitive.

The parameters are:

- **<id>** is the ID of the factory sensor's channel and must be a unique number > 0.
- **<name>** is the name of the factory sensor's channel (displayed in graphs and tables).
- **[<unit>]** is an optional unit description for the factory sensor's channel (for example, bytes). If you do not provide a unit, the sensor factory selects a suitable unit string automatically (recommended).
- **<formula>** contains the formula to calculate the factory sensor's channel. For the formula, you can use the following functions: **channel()** 1448, **min()** 1449, **max()** 1449, **avg()** 1449, or **percent()** 1450.

Define Sensor Channels—Formula Calculations

Within a formula, the following elements are allowed to perform calculations with the values that are returned by one or more functions:

- Basic operations: + (add), - (substract), * (multiply), / (divide)
  Example: 3 + 5 * 2
- Brackets: **( )**
  Example: 3 * (2 + 6)

- Compare: = (equal), <> (not equal), > (greater), < (less), >= (greater or equal), <= (less or equal)
  If the comparison resolves to true, the value is 10,000; if false, the value is 0. For delta sensors the speed is compared.

Example

You see a Sensor Factory channel definition with calculation.

```
#1:Traffic Total x Minus Traffic Out y
( channel(2001,-1) - channel(1004,1) ) * 2
```

This full channel definition results in a factory sensor that shows a calculation with values from two channels (channel IDs -1 and 1) of two traffic sensors (sensor IDs 2001 and 1004). The returned values are subtracted and then multiplied by two.

Channels can be gauge values (for example, ping ms) or delta values (for example, traffic kbit/s). Not all combinations are allowed in a formula.

When performing percentage calculation, please use the **percent() Function** 1450 to make sure you obtain the expected values!

There are calculations you cannot do:

- You cannot add/subtract a delta from a gauge channel (and vice-versa).
- You cannot multiply two delta channels.
- You cannot compare a delta with a gauge channel.
- You cannot use a channel of (another) Sensor Factory sensor channel in the formula.

Define Sensor Channels—channel() Function

The **channel()** function allows to read the data from a channel of a different sensor. The syntax is:

```
channel(<sensorId>,<channelId>)
```

The parameters are:

- **<sensorId>** is the ID of the sensor. It is displayed on the sensor details page in the page header bar 155.
- **<channelId>** is the ID of the sensor channel. It is displayed in the respective field of the channel settings 2783.

Example

```
channel(2001,2)
```

This function reads the data from channel ID 2 of the sensor with the ID 2001.

```
#1:Sample
channel(2001,2)
```

This full channel definition reads the data from channel ID 2 of the sensor with the ID 2001 and displays it in the first factory sensor channel (#1), without any additional calculations.

Define Sensor Channels—min() and max() Functions

The **min()** and **max()** functions return the minimum or maximum of two values. The syntax is:

```
min(<a>,<b>)
max(<a>,<b>)
```

Values for **<a>** and **<b>** are either numbers or channel() 1448 functions.

Examples

```
min(10,5)
```

This function in the first line returns 5, because this is the smaller value out of 10 and 5.

```
min( channel(2001,1),channel(2002,1) )
```

This function returns the minimum of the values of channel 1 of the sensor with ID 2001 and channel 1 of the sensor with ID 2002.

Define Sensor Channels—avg() Function

The **avg()** function returns the average of the two values. This equals: (a+b) / 2. The syntax is:

```
avg(<a>,<b>)
```

Values for **<a>** and **<b>** are either numbers or channel() 1448 functions.

Examples

```
avg(20,10)
```

This function returns 15: (20+10) / 2 = 15.

```
avg( channel(2001,1),channel(2002,1) )
```

This function returns the average of channel 1 of the sensor with ID 2001 and channel 1 of the sensor with ID 2002.

Define Sensor Channels—percent() Function

The **percent()** function calculates the percent value of two given values, for example, a channel and a fixed value. The syntax is:

```
percent(<source>,<maximum>[,<unit>])
```

The parameters are:

- **<source>** is the value the percent is calculated for. This is usually a **channel()** 1448 function.
- **<maximum>** is the limit value used for the percent calculation.
- **[<unit>]** is an optional unit the maximum is provided in. You can use constants with this function (see **Constants** 1452 section below for a list). This can be used for gauge (for example, Ping sensors 1319) or delta (for example, traffic sensors). If no unit is provided, 1 will be used.
  The sensor adds the unit string % automatically.

PRTG will calculate: <source> / <maximum> * <unit> * 100

Examples

```
#1:Usage Traffic In
percent(channel(2001,0),100,kilobit)
#2:Usage Traffic Out
percent(channel(2001,1),100,kilobit)
```

This full channel definition results in a factory sensor that shows two channels of a traffic sensor (sensor ID 2001): Traffic in (channel ID 0) and traffic out (channel ID 1). The sensor displays the values % of maximum bandwidth (100 kilobit/second).

```
#1:Ping %
percent(channel(2002,0),200)
```

This full channel definition results in a factory sensor that shows the **Ping Time** channel (channel ID 0) of a Ping sensor (sensor ID 2002). The sensor displays the values as a percentage of 200 ms.

Define Sensor Channels—Horizontal Lines

You can add lines to the graph using a formula without **channel()** function. Use a fixed value instead. The syntax is:

```
#<id>:<name>[<unit>]
<value>
```

The parameters are:

- **<id>** is the ID of the factory sensor's channel and must be a unique number > 1. Although the sensor does not show a horizontal line as a channel, the ID has to be unique.
- **<name>** is the name of the factory sensor's channel. PRTG does not display this name in graphs and tables, but you can use it as a comment to describe the nature of the line.
- **[<unit>]** is an optional unit description (for example, kbit/s). If you do not provide a unit, PRTG applies the line automatically to the scale of the first factory sensor channel. If your factory sensor uses different units, provide a unit to make sure the line is added for the right scale. Enter the unit exactly as shown in your graph's legend. If you enter a unit that does not yet exist in your graph, a new scale will be added automatically.
- **<value>** contains a number defining where the line will be shown in the graph.

Examples

```
#5:Line at 100ms [ms]
100
```

This channel definition results in a graph that shows a horizontal line at the value of **100** on the **ms** scale.

```
#6:Line at 2 Mbit/s [kbit/s]
2000
```

This channel definition results in a graph that shows a horizontal line at the value of **2000** on the **kbit/s** scale.

```
#1:Ping Time
channel(2002,0)
#2:Line at 120ms [ms]
120
```

This full channel definition results in a factory sensor that shows the **Ping Time** channel (channel ID 0) of a Ping sensor (sensor ID 2002). Additionally, the sensor graphs will show a horizontal line at **120 ms**.

Define Sensor Channels—Constants

The following constants are defined and can be used in calculations:

- **one** = 1
- **kilo** = 1000
- **mega** = 1000 * kilo
- **giga** = 1000 * mega
- **tera** = 1000 * giga
- **byte** = 1
- **kilobyte** = 1024
- **megabyte** = 1024 * kilobyte
- **gigabyte** = 1024 * megabyte
- **terabyte** = 1024 * gigabyte
- **bit** = 1/8
- **kilobit** = kilo / 8
- **megabit** = mega / 8

- **gigabit** = giga / 8
- **terabit** = tera / 8

Define Sensor Status—status() Function

The status of a Sensor Factory sensor can be controlled by the **Status Definition** text field, if you enable the custom formula option in the **Sensor Settings** 1438. Using a special syntax, you can define when the factory sensor changes to a **Down** status. In all other cases, the sensor will be in an **Up** status. The syntax is:

```
status(sensorID) <boolean> status(sensorID)
```

The parameters are:

- **<sensorId>** is the ID of the sensor you want to check the status of. It is displayed on the sensor details page in the page header bar 155.
- **<boolean>** is one of the Boolean operators **AND**, **OR**, or **NOT**. If the resulting expression is true, the factory sensor will change to a **Down** status.

Examples

```
status(2031) AND status(2044)
```

This changes the factory sensor to a **Down** status if both sensors, with IDs 2031 and 2044, are **Down**. Otherwise the factory sensor shows an **Up** status.

```
status(2031) OR status(2044)
```

This changes the factory sensor to a **Down** status if at least one of the sensors with ID 2031 or ID 2044 is **Down**. Otherwise the factory sensor shows an **Up** status.

```
status(2031) AND NOT status(2044)
```

This changes the factory sensor to a **Down** status if the sensor with ID 2031 is **Down**, but the sensor with ID 2044 is not in a **Down** status. Otherwise the factory sensor shows an **Up** status.

A status() function with **NOT** has to be connected with **AND** or **OR** if it is combined with other status() functions:

```
status(sensorID) AND NOT status(sensorID)
status(sensorID) OR NOT status(sensorID)
```

```
( status(2031) AND status(2044) ) OR status(2051)
```

This changes the factory sensor to a **Down** status if both the sensor with ID 2031 and the sensor with ID 2044 is **Down**, or if the sensor with ID 2051 is **Down**. Otherwise the factory sensor shows an **Up** status.

Additionally, the following elements are allowed to perform calculations and comparisons with the values that are returned by the status functions:

- Basic operations: + (add), - (substract), * (multiply), / (divide)
  Example: 3 + 5 * 2
- Brackets: **( )**
  Example: 3 * (2 + 6)
- Compare: = (equal), <> (not equal), > (greater), < (less), >= (greater or equal), <= (less or equal)
  If the comparison resolves to true, the value is 10,000; if false, the value is 0. For delta sensors the speed is compared.

Internally, the status() function returns the downtime channel of the sensor in hundreds of percent (10,000 = 100%).

- true corresponds to a value of 10,000 which is a **Down** status.

- false corresponds to a value of 0 which is an **Up** status.

If you understand this, you are able to use more complex formulas.

Example

```
( status(1031) + status(1032) + status(1033) + status(1034) ) >= 20000
```

This changes the factory sensor to a **Down** status if at least any two of the sensors with IDs 1031, 1032, 1033, or 1034 are **Down**. Otherwise the factory sensor shows an **Up** status.

You can also use the status() function in channel definitions 1446. Using this functionality, it is possible, for example, to display the numeric status value of sensors in a factory sensor channel.

Using Factory Sensors in a Cluster Setup

If you run PRTG in Clustering 116 mode, please note these additional facts:

- If you add a Sensor Factory sensor underneath the **Cluster Probe**, and in the Sensor Factory formula you refer to a channel of a sensor running on the **Cluster Probe** as well, the Sensor Factory sensor shows the data of all cluster nodes for this sensor channel.
- If you add a Sensor Factory sensor underneath the **Local Probe**, and in the Sensor Factory formula you refer to a channel of a sensor running on the **Cluster Probe**, the Sensor Factory sensor only shows data of the primary master node for this sensor channel.

More

Video Tutorial: How to Create a Factory Sensor for the Monitoring of Complex Processes in PRTG

- https://www.paessler.com/support/videos/prtg-advanced/factory-sensor

Knowledge Base: How can I monitor the overall status of the business process "Email"?

- https://kb.paessler.com/en/topic/60737

Knowledge Base: Can I add sensors to Sensor Factory sensors using tags?

- https://kb.paessler.com/en/topic/5143

Knowledge Base: What can I do with PRTG's Sensor Factory Sensors?

- https://kb.paessler.com/en/topic/583

Paessler Blog: Monitoring Business Processes—Transformation of Technical Outages to the Real Business Impact

- https://www.paessler.com/blog/2014/06/26/all-about-prtg/monitoring-business-processes

Edit Sensor Channels

To change display settings and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

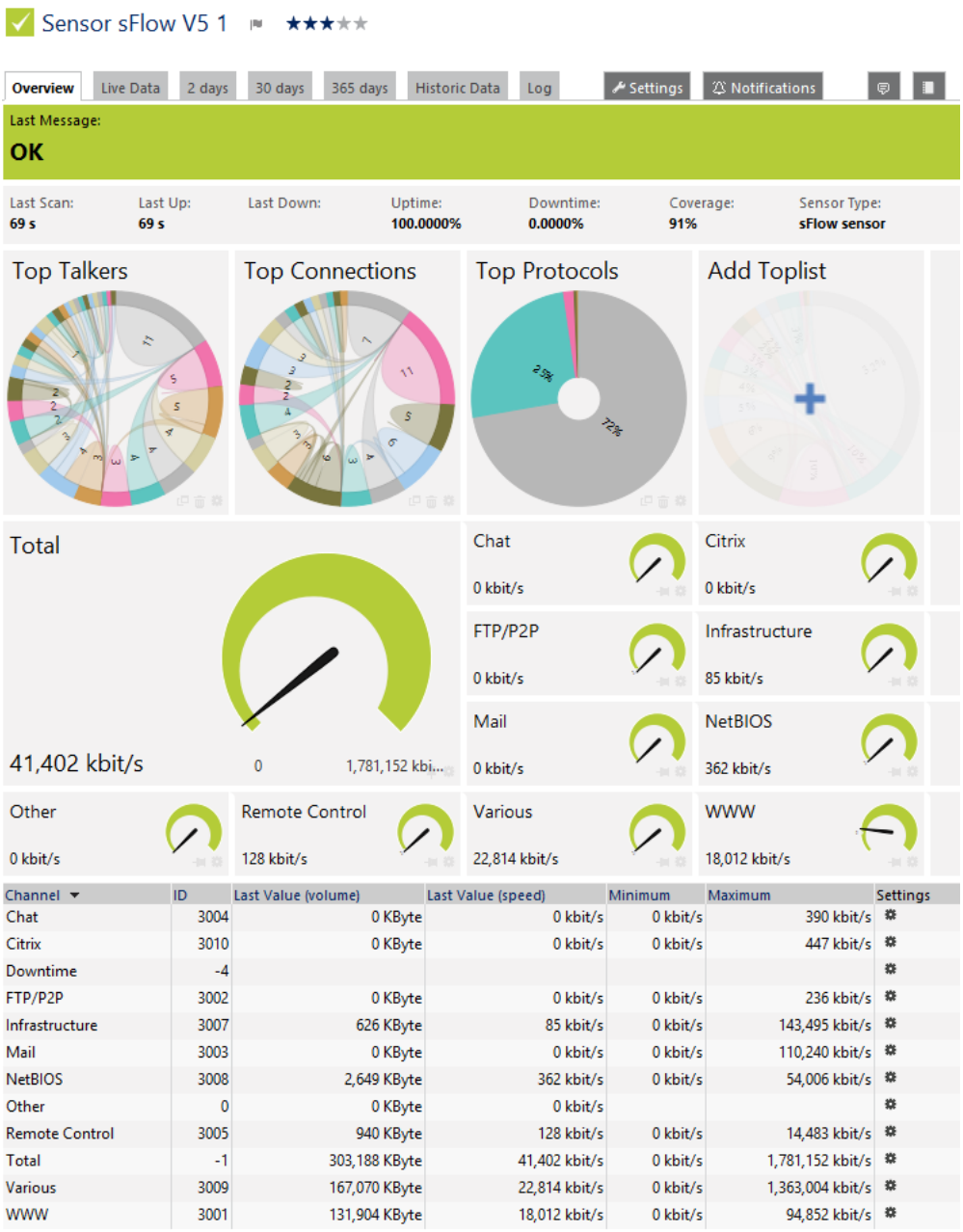
7.8.101 sFlow Sensor

The sFlow sensor receives traffic data from an sFlow V5 compatible device and shows the traffic by type. Only header traffic will be analyzed. Ensure the device matches the sFlow version V5! There are several filter options available to divide traffic into different channels.

This sensor can show the following traffic types in kbit per second:

- Chat (IRC, AIM)
- Citrix
- FTP/P2P (file transfer)
- Infrastructure (network services: DHCP, DNS, Ident, ICMP, SNMP)
- Mail (mail traffic: IMAP, POP3, SMTP)
- NetBIOS
- Remote control (RDP, SSH, Telnet, VNC)
- WWW (web traffic: HTTP, HTTPS)
- Total traffic
- Other protocols (other UDP and TCP traffic)

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Channel	ID	Last Value (volume)	Last Value (speed)	Minimum	Maximum	Settings
Chat	3004	0 KByte	0 kbit/s	0 kbit/s	390 kbit/s	
Citrix	3010	0 KByte	0 kbit/s	0 kbit/s	447 kbit/s	
Downtime	-4					
FTP/P2P	3002	0 KByte	0 kbit/s	0 kbit/s	236 kbit/s	
Infrastructure	3007	626 KByte	85 kbit/s	0 kbit/s	143,495 kbit/s	
Mail	3003	0 KByte	0 kbit/s	0 kbit/s	110,240 kbit/s	
NetBIOS	3008	2,649 KByte	362 kbit/s	0 kbit/s	54,006 kbit/s	
Other	0	0 KByte	0 kbit/s			
Remote Control	3005	940 KByte	128 kbit/s	0 kbit/s	14,483 kbit/s	
Total	-1	303,188 KByte	41,402 kbit/s	0 kbit/s	1,781,152 kbit/s	
Various	3009	167,070 KByte	22,814 kbit/s	0 kbit/s	1,363,004 kbit/s	
WWW	3001	131,904 KByte	18,012 kbit/s	0 kbit/s	94,852 kbit/s	

sFlow Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/sflow.png

Remarks

- You must enable sFlow V5 export on the monitored device for this sensor to work. The device must send the flow data stream to the IP address of the PRTG probe system on which the sensor is set up (either a local or remote probe).
- The sensor accepts RAW data only. The stream must be sent via IPv4.

- This sensor type cannot be used in cluster mode. You can set it up on a local probe or remote probe only, not on a cluster probe.
- There are several limitations 1459 for this sensor type.
- Paessler Website: Paessler sFlow Tester
- Knowledge Base: How can I change the default groups and channels for xFlow and Packet Sniffer sensors?
- Knowledge Base: Where is the volume line in graphs?
- For a general introduction to the technology behind flow monitoring, please see manual section **Monitoring Bandwidth via Flows** 3099.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Limitations of This Sensor Type

There are some limitations that you want to consider before using this sensor type:

- Only sFlow version 5 datagrams are supported
- Only IPv4 flows are supported
- Only the "raw packet header" format is supported
- Only the "Flow sample" format is supported. "Extended flow" and "Counter" formats cannot be processed
- PRTG processes only samples where the source ID matches the ifIndex of the input interface (avoiding double counted traffic) and ascending sequence numbers.
- Sample packets have to be of ethernet type "IP" (with optional VLAN tag)
- Sampled packets of type TCP and UDP are supported

We recommend that you use the sFlow tester for debugging. Please download it here: Paessler sFlow Tester

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SFLOW SPECIFIC SETTINGS

Receive sFlow Packets on UDP Port	Enter the UDP port number on which the flow packets are received. It must match the one you have configured in the sFlow export options of your hardware router device. Default value is **6343**. Please enter an integer value. When configuring export, ensure you select the appropriate sFlow version 5.
Sender IP	Enter the IP address of the sending device you want to receive the sFlow from. Enter an IP address to receive data from a specific device only, or leave the field empty to receive data from any device on the specified port.
Receive sFlow Packets on IP	Select the IP address(es) on which PRTG listens to sFlow packets. The list of IP addresses shown here is specific to your setup. To select an IP address, add a check mark in front of the respective line. The IP address selected here must match the one configured in the sFlow export options of your hardware router device.

SFLOW SPECIFIC SETTINGS

When configuring export, ensure you select the appropriate sFlow version 5.

Log Stream Data to Disk (for Debugging)

Define if you want the probe to write a logfile of the stream and packet data to the data folder (see **Data Storage** 3226). Choose between:

- **None (recommended)**: Do not write additional logfiles. Recommended for normal use cases.
- **Only for the 'Other' channel**: Only write logfiles of data that is not filtered otherwise and therefore accounted to the default **Other** channel.
- **All stream data**: Write logfiles for all data received.

Use with caution! When enabled, huge data files can be created. Please use for a short time and for debugging purposes only.

CHANNEL CONFIGURATION

Channel Selection

Define the categories the sensor accounts the traffic to. There are different groups of traffic available. Choose between:

- **Web**: Internet web traffic.
- **File Transfer**: Traffic caused by FTP.
- **Mail**: Internet mail traffic.
- **Chat**: Traffic caused by chat and instant messaging.
- **Remote Control**: Traffic caused by remote control applications, such as RDP, SSH, Telnet, and VNC.
- **Infrastructure**: Traffic caused by network services, such as DHCP, DNS, Ident, ICMP, and SNMP.
- **NetBIOS**: Traffic caused by NetBIOS communication.
- **Citrix**: Traffic caused by Citrix applications.
- **Other Protocols**: Traffic caused by various other protocols via UDP and TCP.

For each traffic group, you can select how many channels will be used for each group, that is, how detailed the sensor divides the traffic. For each group, choose between:

CHANNEL CONFIGURATION

- **No**: Do not account traffic of this group in its own channel. All traffic of this group is accounted to the default channel named **Other**.
- **Yes**: Count all traffic of this group and summarize it into one channel.
- **Detail**: Count all traffic of this group and further divide it into different channels. The traffic appears in several channels as shown in the **Content** column.
  Extensive use of this option can cause load problems on your probe system. We recommend setting specific, well-chosen filters for the data you really want to analyze.

You can change the default configuration for groups and channels. For details, please see this Knowledge Base article: How can I change the default groups and channels for xFlow and Packet Sniffer sensors?

FILTERING

Include Filter	Define if you want to filter any traffic. If you leave this field empty, all traffic will be included. To include specific traffic only, define filters using a special syntax. For detailed information, please see **Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors** 3175 section.
Exclude Filter	First, the filters defined in the **Include Filter** field are considered. From this subset, you can explicitly exclude traffic, using the same syntax. For detailed information, please see **Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors** 3175 section.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

SENSOR DISPLAY

Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

PRIMARY TOPLIST

Primary Toplist	Define which will be your primary toplist. It will be shown in maps when adding a toplist object. Choose from: ▪ **Top Talkers** ▪ **Top Connections** ▪ **Top Protocols** ▪ [Any custom toplists you have added]

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply. If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply. If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

Toplists

For all flow and packet sniffer sensors there are **Toplists** available on the **Overview** tab of a sensor's detail page. Using toplists, you can review traffic data of small time periods in great detail. For more information, please see **Toplists** 2806 section.

More

Paessler Website: Paessler sFlow Tester

- https://www.paessler.com/tools/sflowtester

Knowledge Base: How can I change the default groups and channels for xFlow and Packet Sniffer sensors?

- https://kb.paessler.com/en/topic/60203

Knowledge Base: Where is the volume line in graphs?

- https://kb.paessler.com/en/topic/61272

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

Related Topics

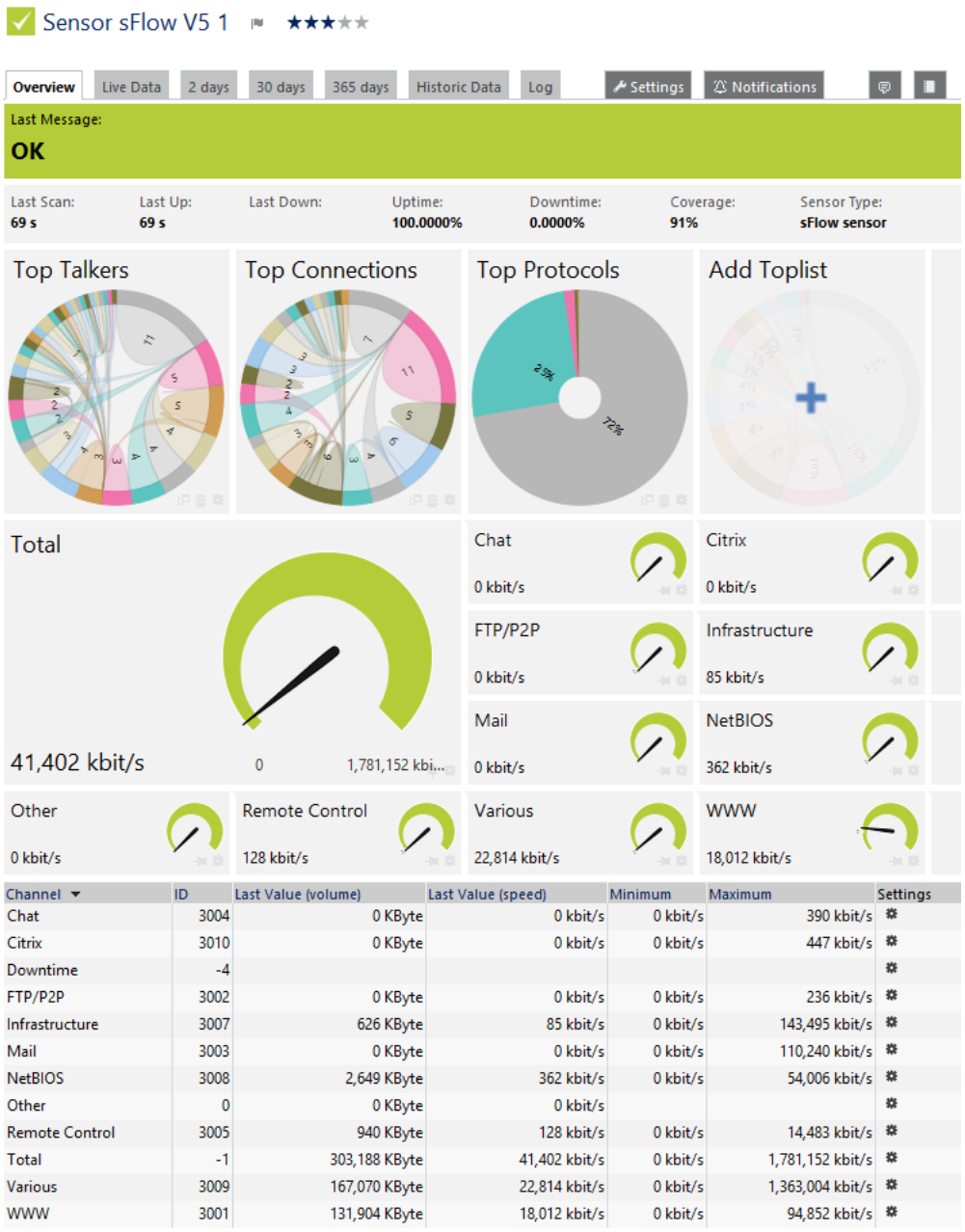
- **Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors** 3175
- **Channel Defintions for xFlow, IPFIX, and Packet Sniffer Sensors** 3180

7.8.102 sFlow (Custom) Sensor

The sFlow (Custom) sensor receives traffic data from an sFlow V5 compatible device and shows the traffic by type. Please make sure the device matches the sFlow version V5! There are several filter options available to divide traffic into different channels.

- This sensor can show traffic by type individually according to your needs.

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Channel	ID	Last Value (volume)	Last Value (speed)	Minimum	Maximum	Settings
Chat	3004	0 KByte	0 kbit/s	0 kbit/s	390 kbit/s	
Citrix	3010	0 KByte	0 kbit/s	0 kbit/s	447 kbit/s	
Downtime	-4					
FTP/P2P	3002	0 KByte	0 kbit/s	0 kbit/s	236 kbit/s	
Infrastructure	3007	626 KByte	85 kbit/s	0 kbit/s	143,495 kbit/s	
Mail	3003	0 KByte	0 kbit/s	0 kbit/s	110,240 kbit/s	
NetBIOS	3008	2,649 KByte	362 kbit/s	0 kbit/s	54,006 kbit/s	
Other	0	0 KByte	0 kbit/s			
Remote Control	3005	940 KByte	128 kbit/s	0 kbit/s	14,483 kbit/s	
Total	-1	303,188 KByte	41,402 kbit/s	0 kbit/s	1,781,152 kbit/s	
Various	3009	167,070 KByte	22,814 kbit/s	0 kbit/s	1,363,004 kbit/s	
WWW	3001	131,904 KByte	18,012 kbit/s	0 kbit/s	94,852 kbit/s	

sFlow (Custom) Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/sflow.png

Remarks

- You must enable sFlow V5 export on the monitored device for this sensor to work. The device must send the flow data stream to the IP address of the PRTG probe system on which the sensor is set up (either a local or remote probe).
- The sensor accepts RAW data.

- This sensor type cannot be used in cluster mode. You can set it up on a local probe or remote probe only, not on a cluster probe.
- There are several limitations[1471] for this sensor type.
- Paessler Website: Paessler sFlow Tester
- Knowledge Base: Where is the volume line in graphs?
- For a general introduction to the technology behind flow monitoring, please see manual section **Monitoring Bandwidth via Flows**[3099].

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Limitations of This Sensor Type

There are some limitations that you want to consider before using this sensor type:

- Only sFlow version 5 datagrams are supported
- Only IPv4 flows are supported
- Only the "raw packet header" format is supported
- Only the "Flow sample" format is supported. "Extended flow" and "Counter" formats cannot be processed
- PRTG processes only samples where the source ID matches the ifIndex of the input interface (avoiding double counted traffic) and ascending sequence numbers.
- Sample packets have to be of ethernet type "IP" (with optional VLAN tag)
- Sampled packets of type TCP and UDP are supported

We recommend that you use the sFlow tester for debugging. Please download it here: Paessler sFlow Tester

Limited to 50 Sensor Channels

PRTG does not support more than 50 sensor channels officially. Depending on the data used with this sensor type, you might exceed the maximum number of supported sensor channels. In this case, PRTG will try to display all sensor channels. However, please be aware that you will experience limited usability and performance.

Add Sensor

The **Add Sensor** dialog appears when you manually[288] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SFLOW SPECIFIC SETTINGS

Receive sFlow Packets on UDP Port	Enter the UDP port number on which the flow packets are received. It must match the one you have configured in the sFlow export options of your hardware router device. Default value is **6343**. Please enter an integer value. When configuring export, ensure you select the appropriate sFlow version 5.
Sender IP	Enter the IP address of the sending device you want to receive the sFlow from. Enter an IP address to receive data from a specific device only, or leave the field empty to receive data from any device on the specified port.

SFLOW SPECIFIC SETTINGS

Receive sFlow Packets on IP	Select the IP address(es) on which PRTG listens to sFlow packets. The list of IP addresses shown here is specific to your setup. To select an IP address, add a check mark in front of the respective line. The IP address selected here must match the one configured in the sFlow export options of your hardware router device. When configuring export, ensure you select the appropriate sFlow version 5.
Log Stream Data to Disk (for Debugging)	Define if you want the probe to write a logfile of the stream and packet data to the data folder (see **Data Storage** 3226). Choose between: ▪ **None (recommended)**: Do not write additional logfiles. Recommended for normal use cases. ▪ **Only for the 'Other' channel**: Only write logfiles of data that is not filtered otherwise and therefore accounted to the default **Other** channel. ▪ **All stream data**: Write logfiles for all data received. Use with caution! When enabled, huge data files can be created. Please use for a short time and for debugging purposes only.

Channel Definition	Enter a channel definition to divide the traffic into different channels. Write each definition in one line. For detailed information, please see **Channel Defintions for xFlow and Packet Sniffer Sensors** 3180 section. All traffic for which no channel is defined will be accounted to the default channel named **Other**. Extensive use of many filters can cause load problems on your probe system. We recommend defining specific, well-chosen filters for the data you really want to analyze.

FILTERING

Include Filter	Define if you want to filter any traffic. If you leave this field empty, all traffic will be included. To include specific traffic only, define filters using a special syntax. For detailed information, please see **Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors** 3175 section.

FILTERING

Exclude Filter	First, the filters defined in the **Include Filter** field are considered. From this subset, you can explicitly exclude traffic, using the same syntax. For detailed information, please see **Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors** 3175 section.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

PRIMARY TOPLIST

Primary Toplist	Define which will be your primary toplist. It will be shown in maps when adding a toplist object. Choose from: ▪ **Top Talkers** ▪ **Top Connections**

PRIMARY TOPLIST

- **Top Protocols**
- [Any custom toplists you have added]

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.

SCANNING INTERVAL

- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** Custom channel types can be set on sensor level only.

Toplists

For all flow and packet sniffer sensors there are **Toplists** available on the **Overview** tab of a sensor's detail page. Using toplists, you can review traffic data of small time periods in great detail. For more information, please see **Toplists** 2806 section.

More

Paessler Website: Paessler sFlow Tester

- https://www.paessler.com/tools/sflowtester

Knowledge Base: Where is the volume line in graphs?

- https://kb.paessler.com/en/topic/61272

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

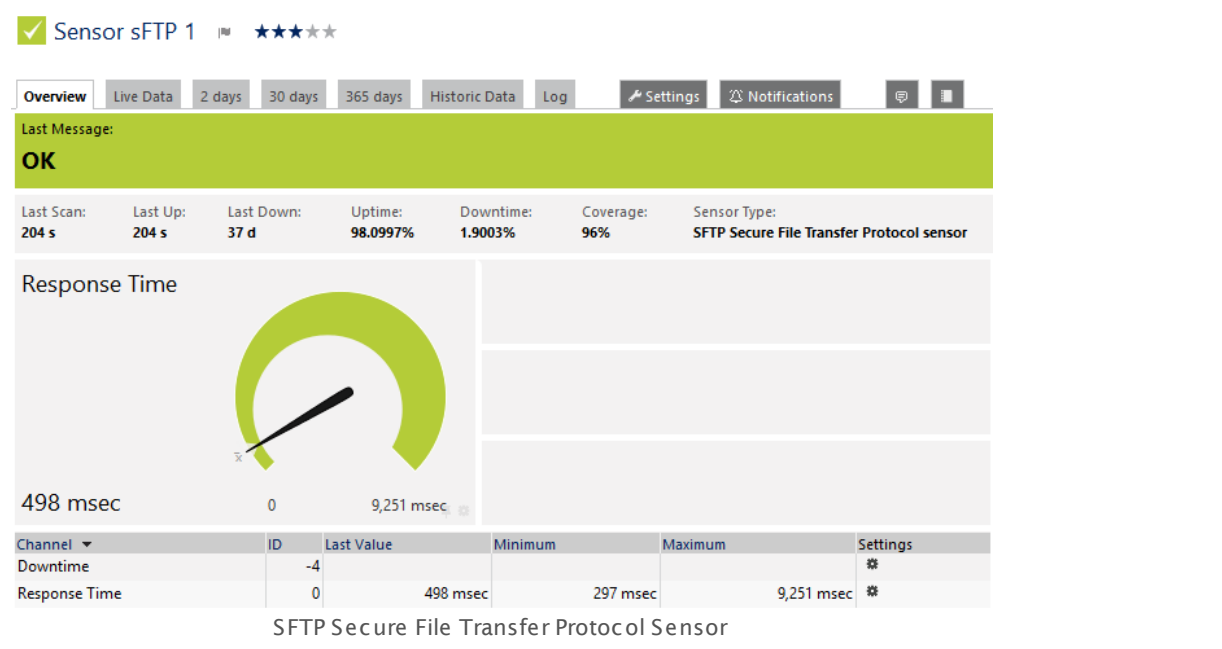
Related Topics

- Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors 3175
- Channel Defintions for xFlow, IPFIX, and Packet Sniffer Sensors 3180

7.8.103 SFTP Secure File Transfer Protocol Sensor

The sFTP Secure File Transfer Protocol sensor monitors FTP servers of a Linux/Unix system using SSH File Transfer Protocol (FTP over SSH).

- It tries to connect and shows the response time of the server.



SFTP Secure File Transfer Protocol Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/sftp_secure_file_transfer_protocol.png

Remarks

- For this sensor type you must define credentials for Linux/Solaris/Mac OS (SSH/WBEM) systems on the device you want to use the sensor on.
- This sensor type cannot support all Linux/Unix and Mac OS distributions.
- For a general introduction to SSH monitoring, please see manual section **Monitoring via SSH** 3095.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SSH SPECIFIC

Connection Timeout (Sec.)	Define a timeout in seconds for the connection. This is the time the sensor will wait to establish a connection to the host. Keep this value as low as possible. The maximum value is **900** seconds (15 minutes). Please enter an integer value.
Shell Timeout (Sec.)	Define a timeout in seconds for the shell response. This is the time in seconds the sensor will wait for the shell to return a response after it has sent its specific command (for example, cat /proc/loadavg). The maximum value is **300** seconds (5 minutes). Please enter an integer value.
SSH Port	Define which port this sensor uses for the SSH connection. Choose between:

SSH SPECIFIC

	▪ **Inherit port number from parent device (default)**: Use the port number as defined in the **Credentials for Linux/Solaris/ Mac OS (SSH/WBEM) Systems** 365 section of the device this sensor is created on. ▪ **Enter custom port number**: Define a custom port number below and do not use the port number from the parent device settings.
Use Port Number	This field is only visible if you choose **Enter custom port number** above. Enter the port number (between 1 and 65535) that this sensor will use for the SSH connection. Please enter an integer value.
SSH Engine	Select the method you want to use to access data with this SSH sensor 3095. We strongly recommend that you use the default engine! For some time you still can use the legacy mode to ensure compatibility with your target systems. Choose between: ▪ **Inherit from parent device (default)**: Use the SSH engine that you have defined in the parent device settings or higher in the object hierarchy 118. If you did not change it, this is the recommended default engine. ▪ **Default**: This is the default monitoring method for SSH sensors. It provides best performance and security. It is set by default in objects that are higher in the hierarchy so usually you can keep the **Inherit from parent device (default)** option. ▪ **Compatibility Mode (deprecated)**: Try this legacy method only if the default mode does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions and is deprecated. We will remove this legacy option soon, so please try to get your SSH sensors running with the default SSH engine. ⓘ The option you select here overrides the selection of the SSH engine in a higher object (which is a parent device, group, probe, or root).
Result Handling	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result.

SSH SPECIFIC

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section Data Storage 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt") in case of error**: Store the last result of the sensor only if it throws an error.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. ⓘ Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.104 SIP Options Ping Sensor

The SIP Options Ping sensor monitors the connectivity for a Session Initiation Protocol (SIP) server using SIP options "Ping". You can use it to monitor Voice over IP (VoIP) services. The sensor sends "auth" and "options" requests to the SIP server. It can alert in case of an error.

It can show the following:

- Response time of the SIP server
- Response code: You can individually define the status for each individual response code by editing the lookup 3183 file **prtg.standardlookups.sip.statuscode**

SIP Options Ping Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/sip_options_ping.png

Remarks

- Requires 1491 .NET 4.0 or higher on the probe system.
- An SIP server might return a "480 Service temporarily unavailable" error until at least one reachable SIP client is connected to the server.
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.
- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.

Requirement: .NET Framework

This sensor type requires the Microsoft .NET Framework to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the remote probe 3196. If the framework is missing, you cannot create this sensor.

Required .NET version (with latest updates): .NET 4.0 (Client Profile is sufficient), .NET 4.5, or .NET 4.6.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/60543

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

BASIC SENSOR SETTINGS

	You can add additional tags to the sensor if you like. Other tags are automatically inherited[124] from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SIP SPECIFIC

Port	Enter the number of the port to which this sensor connects. Please enter an integer value. The default UDP port is **5060**.
Username	Enter the username of the SIP account this sensor will log on to after a connection to the SIP server has been established. Please enter a string.
Password	Enter the password of the SIP account this sensor will log on to after a connection to the SIP server has been established. Please enter a string.
Timeout (Sec.)	Enter the timeout for the connection to the SIP server. Please enter an integer value. The maximum value is 300.
Retry Count	If the connection to the SIP server fails, the sensor tries to connect again. Enter the maximum number of retries. After reaching the maximum count, the sensor will show a red **Down** status[163]. Please enter an integer value.

DEBUG OPTIONS

Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result.

DEBUG OPTIONS

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section Data Storage 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: Which .NET version does PRTG require?

- https://kb.paessler.com/en/topic/60543

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

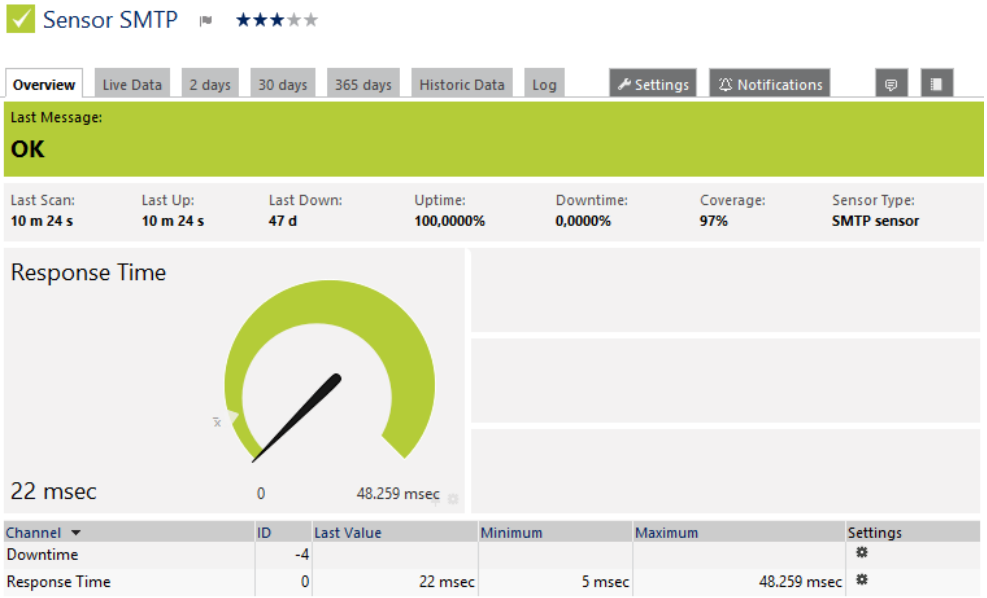
Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.105 SMTP Sensor

The SMTP sensor monitors a mail server using Simple Mail Transfer Protocol (SMTP) and can optionally send a test email with every check.

- It shows the response time of the server.



SMTP Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/smtp.png

Remarks

- This sensor type does not support Secure Remote Password (SRP) ciphers.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you manually add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SMTP SPECIFIC

Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).
Port	Enter the number of the port that the sensor uses to send an email via SMTP. For non-secure connections usually port 25 is used and for SSL/TLS connections, port 465 or 587. The actual setting depends on the server you connect to. Please enter an integer value. We recommend that you use the default value. If you do not get a connection, please try another port number.

AUTHENTICATION

Type	Select whether to use an authentication method for the SMTP connection. Choose between: ▪ **None**: Do not use any authentication method. ▪ **Username and password**: Authenticate at the SMTP server via username and password.
Username	This field is only visible if you enable SMTP authentication above. Enter a username for SMTP authentication. Please enter a string.
Password	This field is only visible if you enable SMTP authentication above. Enter a password for SMTP authentication. Please enter a string.
HELO Ident	Enter a server name for the HELO part of the email protocol. For some mail servers, the HELO identifier must be the valid principal host domain name for the client host. See SMTP RFC 2821.

TRANSPORT-LEVEL SECURITY

Sensor Specific	Define the security level for the sensor connection. Choose between: ▪ **Use Transport-Level Security if available using StartTLS (default)**: Choose this option to try to connect to the server using TLS and StartTLS. If the server does not support this, the sensor will try to connect without encryption. ▪ **Use Transport-Level Security if available**: Choose this option to try to connect to the server using TLS. If the server does not support this, the sensor will try to connect without encryption. ▪ **Enforce Transport-Level Security using StartTLS**: Choose this option to try connecting to the server using TLS and StartTLS. If the server does not support this, the sensor will show a **Down** status 163. ▪ **Enforce Transport-Level Security**: Choose this option to try to connect to the server using TLS. If the server does not support this, the sensor will show a **Down** status 163. If the sensor connects to a server via StartTLS, the connection is established unencrypted first. After the connection is established, the sensor sends a certain command (StartTLS) over the unencrypted connection to negotiate a secure connection via the SSL/TLS protocol.

TRANSPORT-LEVEL SECURITY

If the sensor uses TLS without StartTLS, the negotiation of a secure connection happens immediately (implicitly) so that no commands are sent in unencrypted plain text. If there is no secure connection possible, no communication will take place.

MONITORING

Send Email	Define if PRTG sends an email when connecting to the SMTP server. Choose between: ▪ **None**: Do not send an email, just connect to the SMTP server. ▪ **Send Email**: Send an email through the SMTP server. If there is an error when sending the email, an error message will be triggered and the sensor will change to a **Down** status.
From	Specify the address that the sent emails contain in the from field. Please enter a valid email address.
To	Specify the address that PRTG sends the emails to. If you define more than one recipient, separate the individual email addresses with commas. Please enter a valid email address.
Topic	Specify the subject that the sent emails contain. Please enter a string or leave the field empty.
Content	Specify the body that the sent emails contain. Please enter a string or leave the field empty.
Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section Data Storage 3226.

MONITORING

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply. If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply. If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

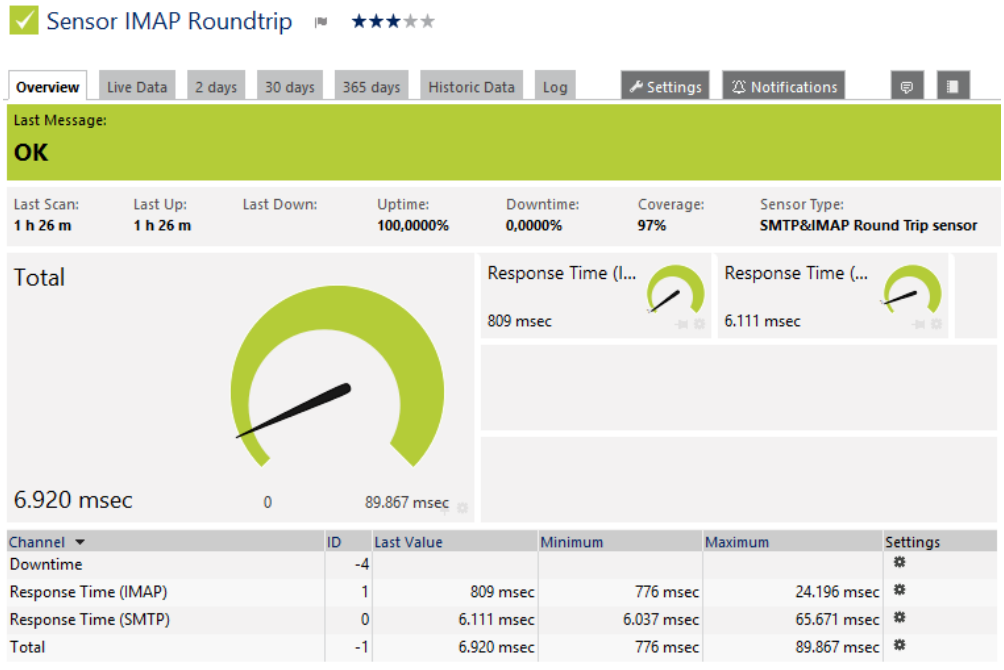
7.8.106 SMTP&IMAP Round Trip Sensor

The SMTP&IMAP Round Trip sensor monitors the time it takes for an email to reach an Internet Message Access Protocol (IMAP) mailbox after being sent using Simple Mail Transfer Protocol (SMTP). It sends an email using the parent device as SMTP server and then scans a dedicated IMAP mailbox until this email comes in.

The SMTP&IMAP Round Trip sensor will delete these emails automatically from the mailbox as soon as PRTG retrieves them. Emails will only remain in the mailbox particularly if a timeout or a restart of the PRTG server occurred during sensor runtime.

The sensor shows the following:

- Response time of SMTP server
- Response time of IMAP server
- Sum of both response times



SMTP&IMAP Round Trip Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/smtp_imap_round_trip.png

Remarks

- Please use dedicated email accounts with this sensor type. If you use more sensors of this type, please make sure that each sensor uses its own email accounts.
  - This sensor type does not support Secure Remote Password (SRP) ciphers.
- For a general introduction to the technology behind round trip monitoring, please see **Monitoring Email Round Trip** 3109 section.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

We recommend that you add this sensor to an SMTP server device only, because the settings of this sensor type are optimized for this scenario.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

EMAIL SETTINGS

From	Specify the address that the sent emails contain in the from field. Please enter a valid email address.
To	Specify the address that PRTG sends the emails to. Please enter a valid email address.
HELO Ident	Enter a server name for the HELO part of the mail protocol. For some mail servers the HELO identifier must be the valid principal host domain name for the client host. See SMTP RFC 2821.

STEP 1: SEND EMAIL WITH PARENT DEVICE AS SMTP SERVER

In this step, you configure how PRTG sends the emails. As SMTP server, the sensor uses the **IP Address/DNS Name** property's value of the device on which you add this sensor.

Port	Enter the number of the port that the sensor uses to send an email via SMTP. For non-secure connections, usually port 25 is used and for SSL/TLS connections, port 465 or 587. The actual setting depends on the server you are connecting to. Please enter an integer value. We recommend that you use the default value. If you do not get a connection, please try another port number.
Timeout for SMTP Connection (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).
SMTP Authentication Type	Define if you want to use authentication for the SMTP connection. Choose between: ▪ **None**: Do not use any authentication method. ▪ **Username/Password**: Authenticate at the SMTP server via username and password.
Username	This field is only visible if you enable SMTP authentication above. Enter a username for SMTP authentication. Please enter a string.
Password	This field is only visible if you enable SMTP authentication above. Enter a password for SMTP authentication. Please enter a string.

STEP 1: SEND EMAIL WITH PARENT DEVICE AS SMTP SERVER

Additional Text for Email Subject	The subject part of the round trip email is created automatically by PRTG. It consists of the string "PRTG Roundtrip Mail:" followed by a unique GUID to correctly identify the email in the IMAP mailbox (for example, PRTG Roundtrip Mail: {5E858D9C-AC70-466A-9B2A-55630165D276}). Use this field to place your custom text before the automatically created text.

TRANSPORT-LEVEL SECURITY

Sensor Specific

Define the security level for the sensor connection. Choose between:

- **Use Transport-Level Security if available using StartTLS (default)**: Choose this option to try to connect to the server using TLS and StartTLS. If the server does not support this, the sensor will try to connect without encryption.
- **Use Transport-Level Security if available**: Choose this option to try to connect to the server using TLS. If the server does not support this, the sensor will try to connect without encryption.
- **Enforce Transport-Level Security using StartTLS**: Choose this option to try connecting to the server using TLS and StartTLS. If the server does not support this, the sensor will show a **Down** status 163.
- **Enforce Transport-Level Security**: Choose this option to try to connect to the server using TLS. If the server does not support this, the sensor will show a **Down** status 163.

If the sensor connects to a server via StartTLS, the connection is established unencrypted first. After the connection is established, the sensor sends a certain command (StartTLS) over the unencrypted connection to negotiate a secure connection via the SSL/TLS protocol.

If the sensor uses TLS without StartTLS, the negotiation of a secure connection happens immediately (implicitly) so that no commands are sent in unencrypted plain text. If there is no secure connection possible, no communication will take place.

STEP 2: CHECK AN IMAP MAILBOX UNTIL EMAIL ARRIVES

In this step, you configure how the sent emails will be received.

STEP 2: CHECK AN IMAP MAILBOX UNTIL EMAIL ARRIVES

IP Address/DNS Name	Specify the IMAP server. Enter a valid IP address or DNS name.
Mailbox	Specify the IMAP mailbox you want to check. Enter the IMAP mailbox or folder name.
Port	Specify the port that the sensor uses for the IMAP connection. For non-secure connections usually port 143 is used and for SSL/TLS connections, port 993 . The actual setting depends on the server you connect to. Please enter an integer value. We recommend that you use the default value. If you do not get a connection, please try another port number.
Connection Interval (Sec.)	Enter the number of seconds the sensor will wait between two connections to the IMAP server. PRTG will repeatedly check the mailbox in this interval until the email arrives. Please enter an integer value.
Maximum Trip Time (Sec.)	Enter the number of seconds an email may take to arrive in the IMAP mailbox. PRTG will repeatedly check the mailbox in the interval specified above until the email arrives. If it does not arrive within the maximum trip time, the sensor will trigger an error message. Please enter an integer value.
Username	Enter a username for IMAP authentication. Please enter a string.
Password	Enter a password for IMAP authentication. Please enter a string.
Search Method	Define how to search for the roundtrip email in the mailbox. Choose between: ▪ **Search email directly (default)**: Send a SEARCH command to find the roundtrip email directly on the IMAP server. ▪ **Search through all available emails**: Iterate over all available message in the mailbox on the IMAP server to find the roundtrip email.

TRANSPORT-LEVEL SECURITY

Sensor Specific	Define the security level for the sensor connection. Choose between:

TRANSPORT-LEVEL SECURITY

- **Use Transport-Level Security if available using StartTLS (default)**: Choose this option to try to connect to the server using TLS and StartTLS. If the server does not support this, the sensor will try to connect without encryption.
- **Use Transport-Level Security if available**: Choose this option to try to connect to the server using TLS. If the server does not support this, the sensor will try to connect without encryption.
- **Enforce Transport-Level Security using StartTLS**: Choose this option to try connecting to the server using TLS and StartTLS. If the server does not support this, the sensor will show a **Down** status 163.
- **Enforce Transport-Level Security**: Choose this option to try to connect to the server using TLS. If the server does not support this, the sensor will show a **Down** status 163.

If the sensor connects to a server via StartTLS, the connection is established unencrypted first. After the connection is established, the sensor sends a certain command (StartTLS) over the unencrypted connection to negotiate a secure connection via the SSL/TLS protocol.

If the sensor uses TLS without StartTLS, the negotiation of a secure connection happens immediately (implicitly) so that no commands are sent in unencrypted plain text. If there is no secure connection possible, no communication will take place.

DEBUG OPTIONS

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result**: Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section **Data Storage** 3226.

DEBUG OPTIONS

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply. If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply. If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

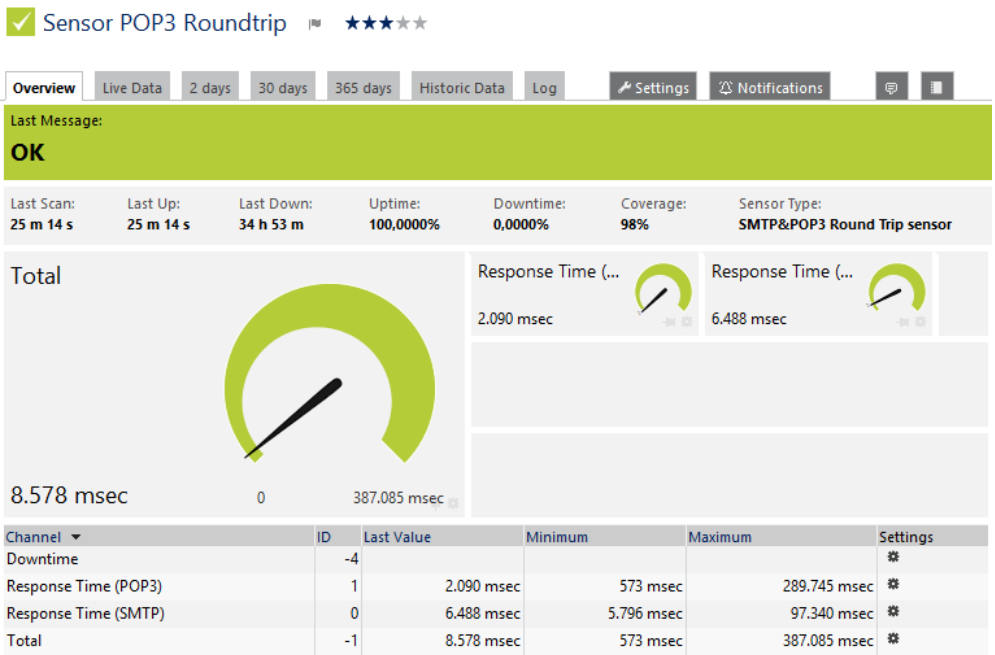
7.8.107 SMTP&POP3 Round Trip Sensor

The SMTP&POP3 Round Trip sensor monitors the time it takes for an email to reach a Post Office Protocol version 3 (POP3) mailbox after being sent using Simple Mail Transfer Protocol (SMTP). It sends an email using the parent device as SMTP server and then scans a dedicated POP3 mailbox until the email comes in.

The SMTP&POP3 Round Trip sensor will delete these emails automatically from the mailbox as soon as PRTG retrieves them. Emails will only remain in the mailbox particularly if a timeout or a restart of the PRTG server occurred during sensor runtime.

The sensor shows the following:

- Response time of SMTP server
- Response time of POP3 server
- Sum of both response times



SMTP&POP3 Round Trip Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/smtp_pop3_round_trip.png

Remarks

- Please use dedicated email accounts with this sensor type. If you use more sensors of this type, please make sure that each sensor uses its own email accounts.
  - This sensor type does not support Secure Remote Password (SRP) ciphers.
- For a general introduction to the technology behind round trip monitoring, please see Monitoring Email Round Trip 3109 section.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

We recommend that you add this sensor on an SMTP server device only, because the settings of this sensor type are optimized for this scenario.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

EMAIL SETTINGS

From	Specify the address that the sent emails will contain in the from field. Please enter a valid email address.
To	Specify the address that PRTG sends the emails to. Please enter a valid email address.
HELO Ident	Enter a server name for the HELO part of the mail protocol. For some mail servers the HELO identifier must be the valid principal host domain name for the client host. See SMTP RFC 2821.

STEP 1: SEND EMAIL WITH PARENT DEVICE AS SMTP SERVER

In this step, you configure how PRTG sends the emails. As SMTP server, the sensor uses the **IP-Address/DNS Name** property's value of the device on which you add this sensor.

Port	Enter the number of the port that the sensor uses to send an email via SMTP. For non-secure connections usually port 25 is used and for SSL/TLS connections, port 465 or 587 . The actual setting depends on the server you connect to. Please enter an integer value. We recommend that you use the default value. If you do not get a connection, please try another port number.
Timeout for SMTP Connection (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).
SMTP Authentication Type	Define if you want to use an authentication for the SMTP connection. Choose between: ▪ **None**: Do not use any authentication method. ▪ **Username/Password**: Authenticate at the SMTP server via username and password.
Username	This field is only visible if you enable SMTP authentication above. Enter a username for SMTP authentication. Please enter a string.

STEP 1: SEND EMAIL WITH PARENT DEVICE AS SMTP SERVER

Password	This field is only visible if you enable SMTP authentication above. Enter a password for SMTP authentication. Please enter a string.
Additional Text for Email Subject	The subject part of the round trip email is created automatically by PRTG. It consists of the string "PRTG Roundtrip Mail:" followed by a unique GUID to correctly identify the email in the POP3 mailbox (for example, PRTG Roundtrip Mail: {5E858D9C-AC70-466A-9B2A-55630165D276}). Use this field to place your custom text before the automatically created text.

TRANSPORT-LEVEL SECURITY

Sensor Specific

Define the security level for the sensor connection. Choose between:

- **Use Transport-Level Security if available using StartTLS (default)**: Choose this option to try to connect to the server using TLS and StartTLS. If the server does not support this, the sensor will try to connect without encryption.
- **Use Transport-Level Security if available**: Choose this option to try to connect to the server using TLS. If the server does not support this, the sensor will try to connect without encryption.
- **Enforce Transport-Level Security using StartTLS**: Choose this option to try connecting to the server using TLS and StartTLS. If the server does not support this, the sensor will show a **Down** status 163.
- **Enforce Transport-Level Security**: Choose this option to try to connect to the server using TLS. If the server does not support this, the sensor will show a **Down** status 163.

If the sensor connects to a server via StartTLS, the connection is established unencrypted first. After the connection is established, the sensor sends a certain command (StartTLS) over the unencrypted connection to negotiate a secure connection via the SSL/TLS protocol.

If the sensor uses TLS without StartTLS, the negotiation of a secure connection happens immediately (implicitly) so that no commands are sent in unencrypted plain text. If there is no secure connection possible, no communication will take place.

STEP 2: CHECK A POP3 MAILBOX UNTIL EMAIL ARRIVES

In this step, you configure how the sent emails will be received.

IP Address/DNS Name	Specify the POP3 server. Enter a valid IP address or DNS name.
Port	Specify the port that the sensor uses for the POP3 connection. For non-secure connections usually port 110 is used and port 995 for SSL/TLS connections. The actual setting depends on the server you are connecting to. Please enter an integer value. We recommend that you use the default value. If you do not get a connection, please try another port number.
Connection Interval (Sec.)	Enter the number of seconds the sensor will wait between two connections to the IMAP server. PRTG will repeatedly check the mailbox in this interval until the email arrives. Please enter an integer value.
Maximum Trip Time (Sec.)	Enter the number of seconds an email may take to arrive in the IMAP mailbox. PRTG will repeatedly check the mailbox in the interval specified above until the email arrives. If it does not arrive within the maximum trip time, the sensor will trigger an error message. Please enter an integer value.
POP3 Authentication Type	Select the kind of authentication for the POP3 connection. Choose between: ▪ **Without Login**: Monitor the connection to the POP3 server only. ▪ **Username and Password**: Log on to the POP3 server with username and password (simple login, non-secure). ▪ **128-bit MD5 hash value (APOP)**: Send the password in an encrypted form using APOP. This option must be supported by the POP3 server you're connecting to.
Username	This field is only visible if you select an option with login above. Enter a username for POP3 authentication. Please enter a string.
Password	This field is only visible if you select an option with login above. Enter a username for POP3 authentication. Please enter a string.

TRANSPORT-LEVEL SECURITY

Sensor Specific

Define the security level for the sensor connection. Choose between:

- **Use Transport-Level Security if available using StartTLS (default)**: Choose this option to try to connect to the server using TLS and StartTLS. If the server does not support this, the sensor will try to connect without encryption.
- **Use Transport-Level Security if available**: Choose this option to try to connect to the server using TLS. If the server does not support this, the sensor will try to connect without encryption.
- **Enforce Transport-Level Security using StartTLS**: Choose this option to try connecting to the server using TLS and StartTLS. If the server does not support this, the sensor will show a **Down** status 163.
- **Enforce Transport-Level Security**: Choose this option to try to connect to the server using TLS. If the server does not support this, the sensor will show a **Down** status 163.

If the sensor connects to a server via StartTLS, the connection is established unencrypted first. After the connection is established, the sensor sends a certain command (StartTLS) over the unencrypted connection to negotiate a secure connection via the SSL/TLS protocol.

If the sensor uses TLS without StartTLS, the negotiation of a secure connection happens immediately (implicitly) so that no commands are sent in unencrypted plain text. If there is no secure connection possible, no communication will take place.

DEBUG OPTIONS

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result**: Do not store the sensor result.

DEBUG OPTIONS

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section **Data Storage** 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

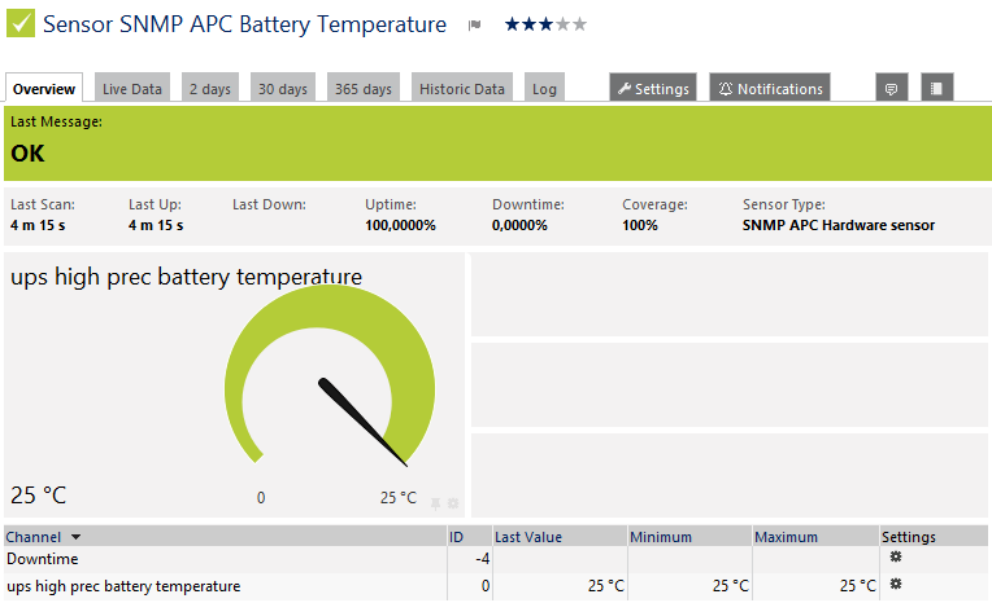
7.8.108 SNMP APC Hardware Sensor

The SNMP APC Hardware sensor monitors performance counters on an APC UPS device using Simple Network Management Protocol (SNMP).

It can show the following:

- Actual voltage of battery
- Capacity of battery
- Temperature of battery
- Remaining runtime of battery
- Input and output frequency
- Input and output voltage
- Output load

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



SNMP APC Hardware Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_apc_hardware.png

Remarks

- Knowledge Base: How can I monitor additional counters with the SNMP APC Hardware sensor?
- Knowledge Base: How can I monitor an APC UPS that does not support SNMP?
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the performance counters you want to monitor. PRTG creates one sensor for each counter you select in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

APC UPS SPECIFIC

Library OIDs	Select the performance counters you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

APC UPS SPECIFIC

Selected Interface	Shows the name of the interface (performance counter) that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Unit String	Define the unit of the numerical data that the sensor monitors at the given OID. Please enter a string.
Multiplication	If you want to multiply the received data with a certain value, enter the quotient here. Please enter an integer value.
Division	If you want to divide the received data by a certain value, enter the divisor here. Please enter an integer value.
If Value Changes	Define what this sensor will do when the sensor value changes. You can choose between: ▪ **Ignore changes (default)**: The sensor takes no action on change. ▪ **Trigger 'change' notification**: The sensor sends an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification 2791 whenever the sensor value changes.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: How can I monitor additional counters with the SNMP APC Hardware sensor?

- https://kb.paessler.com/en/topic/60367

Knowledge Base: How can I monitor an APC UPS that does not support SNMP?

- https://kb.paessler.com/en/topic/63674

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.109 SNMP Buffalo TS System Health Sensor

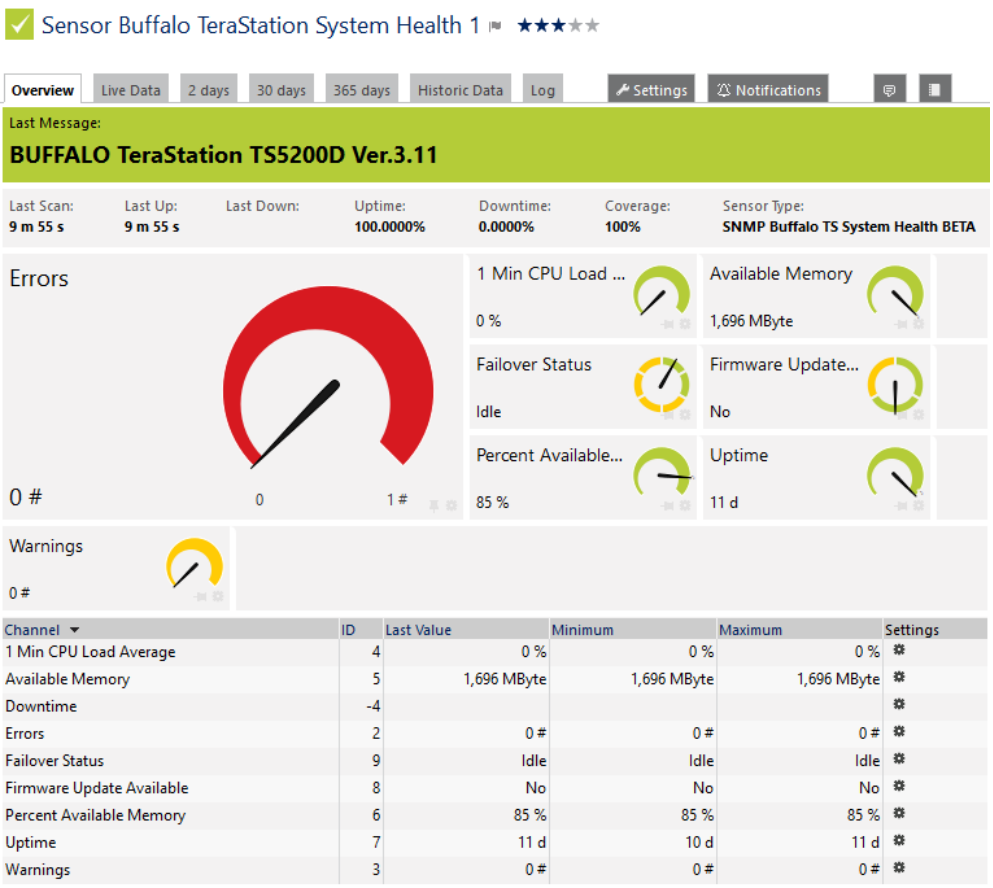
The SNMP Buffalo TS System Health sensor monitors the system health of a Buffalo TeraStation Network Attached Storage (NAS) using Simple Network Management Protocol (SNMP). Supported TeraStation systems are the 1000, 3000, 5000, and 7000 series.

It can show the following:

- Number of errors
- Number of warnings
- Available memory in total and percent
- CPU usage
- Uptime
- Failover status: idle, busy, starting main, starting backup, initializing, stopping
- Firmware update availability: yes, no, unknown
- RPSU status: fine, broken, unknown

The channels are created at run-time, depending on your Buffalo TeraStation NAS and firmware version. Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

Run an **Auto-Discovery** 249 with the device template **Buffalo TeraStation NAS** to automatically create **SNMP Custom Table sensors** 1689 with additional useful information about your Buffalo TeraStation, for example, array status, disk smart status, disk status, and iSCSI status. This device template will also create SNMP sensors 387 for traffic, memory, and load average on your TeraStation.



SNMP Buffalo TS System Health Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_buffalo_ts_system_health.png

Remarks

- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.
- This sensor type has predefined limits for several metrics. You can change these limits individually in the channel settings. For detailed information about channel limits, please refer to the manual section **Sensor Channels Settings** 2782.
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.
- Currently, this sensor type is in beta status. The methods of operating can change at any time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.

BETA

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.110 SNMP Cisco ADSL Sensor

The SNMP Cisco ADSL sensor monitors Asymmetric Digital Subscriber Line (ADSL) statistics of a Cisco router using Simple Network Management Protocol (SNMP).

It shows the following:

- Speed of downlink
- Speed of uplink
- Remote and local attenuation
- Remote and local SNR (signal-to-noise ratio)
- Remote and local power output

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

Remarks

- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

For devices with multiple performance counters, multiple sensors are created at once in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

CISCO ADSL SETTINGS

Line Index	Select the performance counters you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

SENSOR DISPLAY

Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies [2822] in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector [210] to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** [360] or in the superior **Group Settings** [334].

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

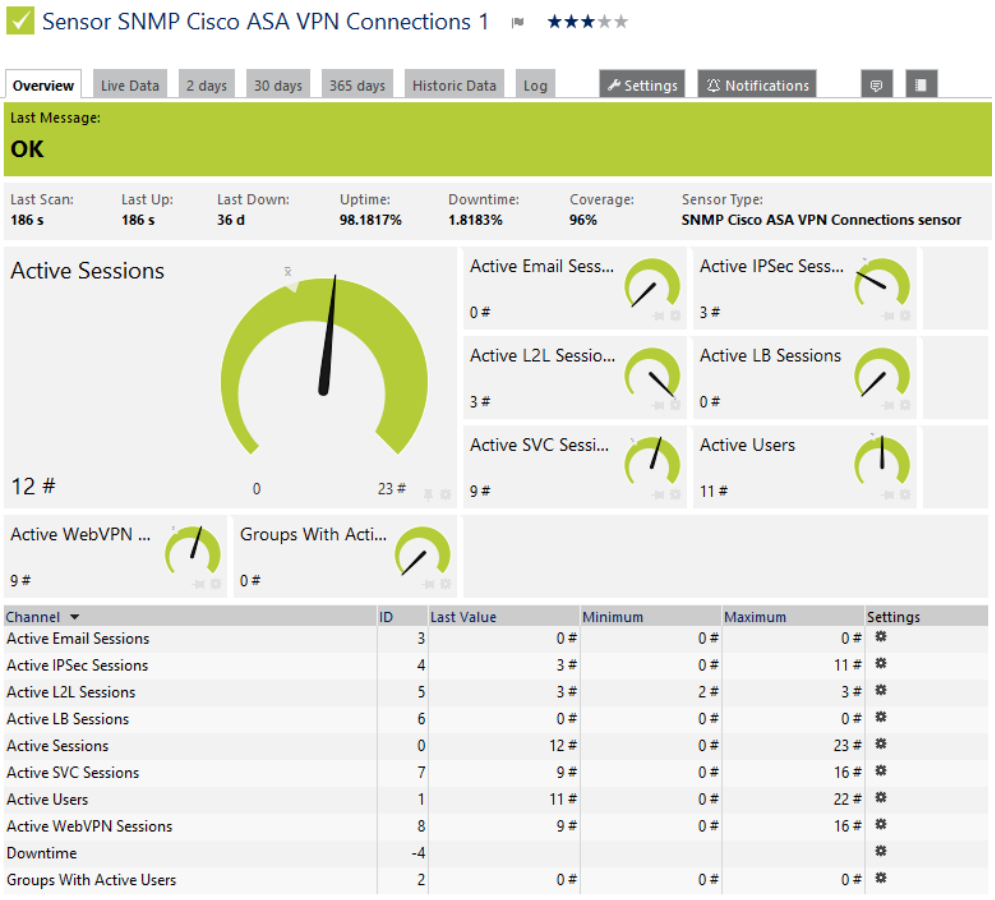
For more general information about settings, please see the **Object Settings** 188 section.

7.8.111 SNMP Cisco ASA VPN Connections Sensor

The SNMP Cisco ASA VPN Connections sensor monitors the Virtual Private Network (VPN) connections on a Cisco Adaptive Security Appliance using Simple Network Management Protocol (SNMP).

It can show the following:

- Active email sessions
- Active Internet Protocol Security (IPsec) sessions
- Active L2L sessions
- Active LB sessions
- Active sessions in total
- Active SVC sessions
- Active users
- Groups with active users



SNMP Cisco ASA VPN Connections Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_cisco_asa_vpn_connections.png

Remarks

- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2945, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

CREDENTIALS FOR SNMP DEVICES

SNMP Version	Select the SNMP version for the device connection. Choose between: ▪ **v1**: Use the simple v1 protocol for SNMP connections. This protocol only offers clear-text data transmission, but it is usually supported by all devices. SNMP v1 does not support 64-bit counters which may result in invalid data when monitoring traffic via SNMP.

CREDENTIALS FOR SNMP DEVICES

- **v2c (recommended)**: Use the more advanced v2c protocol for SNMP connections. This is the most common SNMP version. Data is still transferred as clear-text, but it supports 64-bit counters.
- **v3**: Use the v3 protocol for SNMP connections. It provides secure authentication and data encryption.

When using SNMP v3 you can only monitor a limited number of sensors per second due to internal limitations. The limit is somewhere between 1 and 50 sensors per second (depending on the SNMP latency of your network). This means that using an interval of 60 seconds limits you to between 60 and 3000 SNMP v3 sensors for each probe. If you experience an increased Interval Delay or Open Requests with the **Probe Health Sensor** 1378, distribute the load over multiple probes 3196. SNMP v1 and v2 do not have this limitation.

Community String

This setting is only visible if you select SNMP version **v1** or **v2c** above. Enter the community string of your devices. This is a kind of "clear-text password" for simple authentication. We recommend that you use the default value.

Authentication Type

This setting is only visible if you select SNMP version **v3** above. Choose between:

- **MD5**: Use Message-Digest Algorithm 5 (MD5) for authentication.
- **SHA**: Use Secure Hash Algorithm (SHA) for authentication.

The type you choose must match the authentication type of your device.

If you do not want to use authentication, but you need SNMP v3, for example, because your device requires context, you can leave the field **Password** empty. In this case, SNMP_SEC_LEVEL_NOAUTH is used and authentication deactivated entirely.

User

This setting is only visible if you select SNMP version **v3** above. Enter a username for secure authentication. This value must match the username of your device.

Password

This setting is only visible if you select SNMP version **v3** above. Enter a password for secure authentication. This value must match the password of your device.

Encryption Type

This setting is only visible if you select SNMP version **v3** above. Select an encryption type. Choose between:

- **DES**: Use Data Encryption Standard (DES) as encryption algorithm.

CREDENTIALS FOR SNMP DEVICES

- **AES**: Use Advanced Encryption Standard (AES) as encryption algorithm.

AES 192 and AES 256 are not supported by Net-SNMP because they lack RFC specification.

The type that you choose must match the encryption type of your device.

Data Encryption Key	This setting is only visible if you select SNMP version **v3** above. Enter an encryption key here. If you provide a key in this field, SNMP data packets are encrypted using the encryption algorithm selected above, which provides increased security. The key that you enter here must match the encryption key of your device. If the key you enter in this field does not match the key configured on the target SNMP device, you will not get an error message about this! Please enter a string or leave the field empty.
Context Name	This setting is only visible if you select SNMP version **v3** above. Enter a context name only if it is required by the configuration of the device. Context is a collection of management information accessible by an SNMP device. Please enter a string.
SNMP Port	Enter the port for the SNMP communication. We recommend that you use the default value.
SNMP Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than the value you enter here, the request is aborted and an error message triggered.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

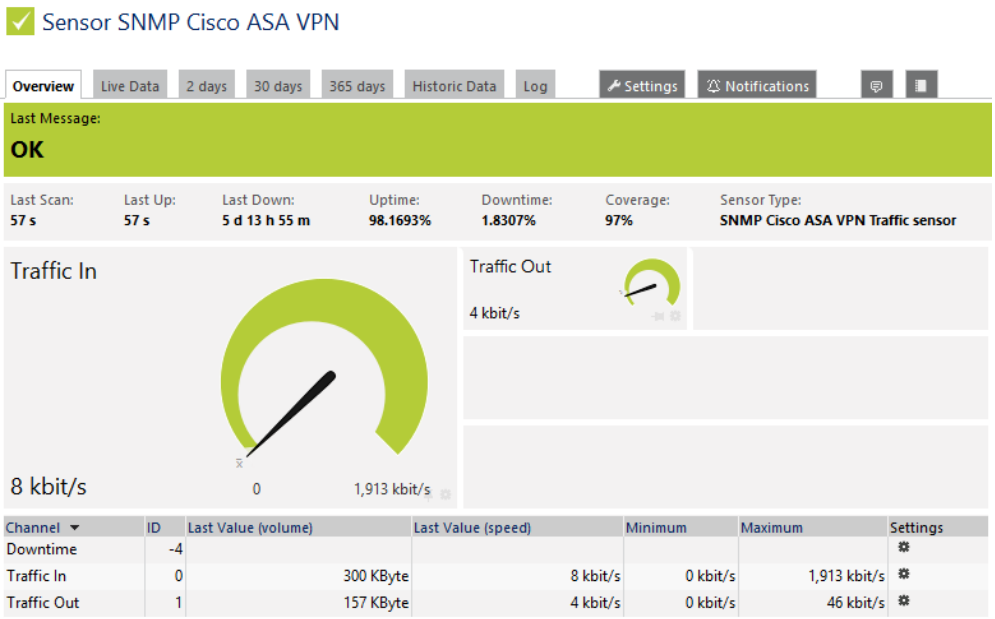
For more general information about settings, please see the **Object Settings** 188 section.

7.8.112 SNMP Cisco ASA VPN Traffic Sensor

The SNMP Cisco ASA VPN Traffic sensor monitors the traffic of an Internet Protocol Security (IPsec) Virtual Private Network (VPN) connection on a Cisco Adaptive Security Appliance using Simple Network Management Protocol (SNMP).

It shows the following:

- Incoming traffic
- Outgoing traffic



SNMP Cisco ASA VPN Traffic Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_cisco_asa_vpn_traffic.png

Remarks

- This sensor type is indented to monitor permanent connections. It will show an error if a connection is interrupted.
- This sensor can monitor IPsec connections only!
- Knowledge Base: I get the error PE123 when using the SNMP Cisco ASA VPN Traffic sensor. What can I do?
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the connections you want to monitor. PRTG creates one sensor for each connection you select in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

ASA VPN SPECIFIC

Connections	Select the IPsec VPN connections you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items. This sensor type can only monitor VPN connections based on IPsec. This means, for example, that connections using "Cisco AnyConnect" are not listed here.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.

BASIC SENSOR SETTINGS

Parent Tags	Shows **Tags** [124] that this sensor inherits [124] from its parent device, group, and probe [118]. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** [124], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited [124] from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

ASA VPN SPECIFIC

Remote IP	Shows the IP address of the connection this sensor monitors. This value is shown for reference purposes only. We strongly recommend that you only change it if Paessler support explicitly asks you to do so. Wrong usage can result in incorrect monitoring data! This sensor type can only monitor VPN connections based on IPsec.
Sensor Behavior	Define the status of the sensor [163] if there is no active connection available. Choose between: ▪ **Show 'Down' status if no connection is active (recommended)** ▪ **Show 'Warning' status if no connection is active** ▪ **Stay in 'Up' status if no connection is active**

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

CREDENTIALS FOR SNMP DEVICES

SNMP Version	Select the SNMP version for the device connection. Choose between: ▪ **v1**: Use the simple v1 protocol for SNMP connections. This protocol only offers clear-text data transmission, but it is usually supported by all devices. SNMP v1 does not support 64-bit counters which may result in invalid data when monitoring traffic via SNMP.

CREDENTIALS FOR SNMP DEVICES

- **v2c (recommended)**: Use the more advanced v2c protocol for SNMP connections. This is the most common SNMP version. Data is still transferred as clear-text, but it supports 64-bit counters.
- **v3**: Use the v3 protocol for SNMP connections. It provides secure authentication and data encryption.

When using SNMP v3 you can only monitor a limited number of sensors per second due to internal limitations. The limit is somewhere between 1 and 50 sensors per second (depending on the SNMP latency of your network). This means that using an interval of 60 seconds limits you to between 60 and 3000 SNMP v3 sensors for each probe. If you experience an increased Interval Delay or Open Requests with the **Probe Health Sensor** 1378, distribute the load over multiple probes 3196. SNMP v1 and v2 do not have this limitation.

Community String

This setting is only visible if you select SNMP version **v1** or **v2c** above. Enter the community string of your devices. This is a kind of "clear-text password" for simple authentication. We recommend that you use the default value.

Authentication Type

This setting is only visible if you select SNMP version **v3** above. Choose between:

- **MD5**: Use Message-Digest Algorithm 5 (MD5) for authentication.
- **SHA**: Use Secure Hash Algorithm (SHA) for authentication.

The type you choose must match the authentication type of your device.

If you do not want to use authentication, but you need SNMP v3, for example, because your device requires context, you can leave the field **Password** empty. In this case, SNMP_SEC_LEVEL_NOAUTH is used and authentication deactivated entirely.

User

This setting is only visible if you select SNMP version **v3** above. Enter a username for secure authentication. This value must match the username of your device.

Password

This setting is only visible if you select SNMP version **v3** above. Enter a password for secure authentication. This value must match the password of your device.

Encryption Type

This setting is only visible if you select SNMP version **v3** above. Select an encryption type. Choose between:

- **DES**: Use Data Encryption Standard (DES) as encryption algorithm.

CREDENTIALS FOR SNMP DEVICES

- **AES**: Use Advanced Encryption Standard (AES) as encryption algorithm.

AES 192 and AES 256 are not supported by Net-SNMP because they lack RFC specification.

The type that you choose must match the encryption type of your device.

Data Encryption Key	This setting is only visible if you select SNMP version **v3** above. Enter an encryption key here. If you provide a key in this field, SNMP data packets are encrypted using the encryption algorithm selected above, which provides increased security. The key that you enter here must match the encryption key of your device. If the key you enter in this field does not match the key configured on the target SNMP device, you will not get an error message about this! Please enter a string or leave the field empty.
Context Name	This setting is only visible if you select SNMP version **v3** above. Enter a context name only if it is required by the configuration of the device. Context is a collection of management information accessible by an SNMP device. Please enter a string.
SNMP Port	Enter the port for the SNMP communication. We recommend that you use the default value.
SNMP Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than the value you enter here, the request is aborted and an error message triggered.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Knowledge Base: I get the error PE123 when using the SNMP Cisco ASA VPN Traffic sensor. What can I do?

- https://kb.paessler.com/en/topic/59643

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.113 SNMP Cisco ASA VPN Users Sensor

The SNMP Cisco ASA VPN Users sensor monitors account connections to a Virtual Private Network (VPN) on a Cisco Adaptive Security Appliance via Simple Network Management Protocol (SNMP).

It can show the following:

- Number of currently connected accounts
- If a specific user account is currently offline or online

SNMP Cisco ASA VPN Users Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_cisco_asa_vpn_users.png

Remarks

- Please do not use the sensor to monitor more than 50 VPN users, especially if they are all connected simultaneously. For more information, see this Knowledge Base article: My Cisco ASA VPN Users sensor shows a user limit error. Why? What can I do?

- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

CREDENTIALS FOR SNMP DEVICES

SNMP Version	Select the SNMP version for the device connection. Choose between: ▪ **v1**: Use the simple v1 protocol for SNMP connections. This protocol only offers clear-text data transmission, but it is usually supported by all devices. SNMP v1 does not support 64-bit counters which may result in invalid data when monitoring traffic via SNMP.

CREDENTIALS FOR SNMP DEVICES

- **v2c (recommended)**: Use the more advanced v2c protocol for SNMP connections. This is the most common SNMP version. Data is still transferred as clear-text, but it supports 64-bit counters.
- **v3**: Use the v3 protocol for SNMP connections. It provides secure authentication and data encryption.

When using SNMP v3 you can only monitor a limited number of sensors per second due to internal limitations. The limit is somewhere between 1 and 50 sensors per second (depending on the SNMP latency of your network). This means that using an interval of 60 seconds limits you to between 60 and 3000 SNMP v3 sensors for each probe. If you experience an increased Interval Delay or Open Requests with the **Probe Health Sensor** 1378, distribute the load over multiple probes 3196. SNMP v1 and v2 do not have this limitation.

Community String

This setting is only visible if you select SNMP version **v1** or **v2c** above. Enter the community string of your devices. This is a kind of "clear-text password" for simple authentication. We recommend that you use the default value.

Authentication Type

This setting is only visible if you select SNMP version **v3** above. Choose between:

- **MD5**: Use Message-Digest Algorithm 5 (MD5) for authentication.
- **SHA**: Use Secure Hash Algorithm (SHA) for authentication.

The type you choose must match the authentication type of your device.

If you do not want to use authentication, but you need SNMP v3, for example, because your device requires context, you can leave the field **Password** empty. In this case, SNMP_SEC_LEVEL_NOAUTH is used and authentication deactivated entirely.

User

This setting is only visible if you select SNMP version **v3** above. Enter a username for secure authentication. This value must match the username of your device.

Password

This setting is only visible if you select SNMP version **v3** above. Enter a password for secure authentication. This value must match the password of your device.

Encryption Type

This setting is only visible if you select SNMP version **v3** above. Select an encryption type. Choose between:

- **DES**: Use Data Encryption Standard (DES) as encryption algorithm.

CREDENTIALS FOR SNMP DEVICES

- **AES**: Use Advanced Encryption Standard (AES) as encryption algorithm.

AES 192 and AES 256 are not supported by Net-SNMP because they lack RFC specification.

The type that you choose must match the encryption type of your device.

Data Encryption Key	This setting is only visible if you select SNMP version **v3** above. Enter an encryption key here. If you provide a key in this field, SNMP data packets are encrypted using the encryption algorithm selected above, which provides increased security. The key that you enter here must match the encryption key of your device. If the key you enter in this field does not match the key configured on the target SNMP device, you will not get an error message about this! Please enter a string or leave the field empty.
Context Name	This setting is only visible if you select SNMP version **v3** above. Enter a context name only if it is required by the configuration of the device. Context is a collection of management information accessible by an SNMP device. Please enter a string.
SNMP Port	Enter the port for the SNMP communication. We recommend that you use the default value.
SNMP Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than the value you enter here, the request is aborted and an error message triggered.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Knowledge Base: My Cisco ASA VPN Users sensor shows a user limit error. Why? What can I do?

- https://kb.paessler.com/en/topic/64053

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

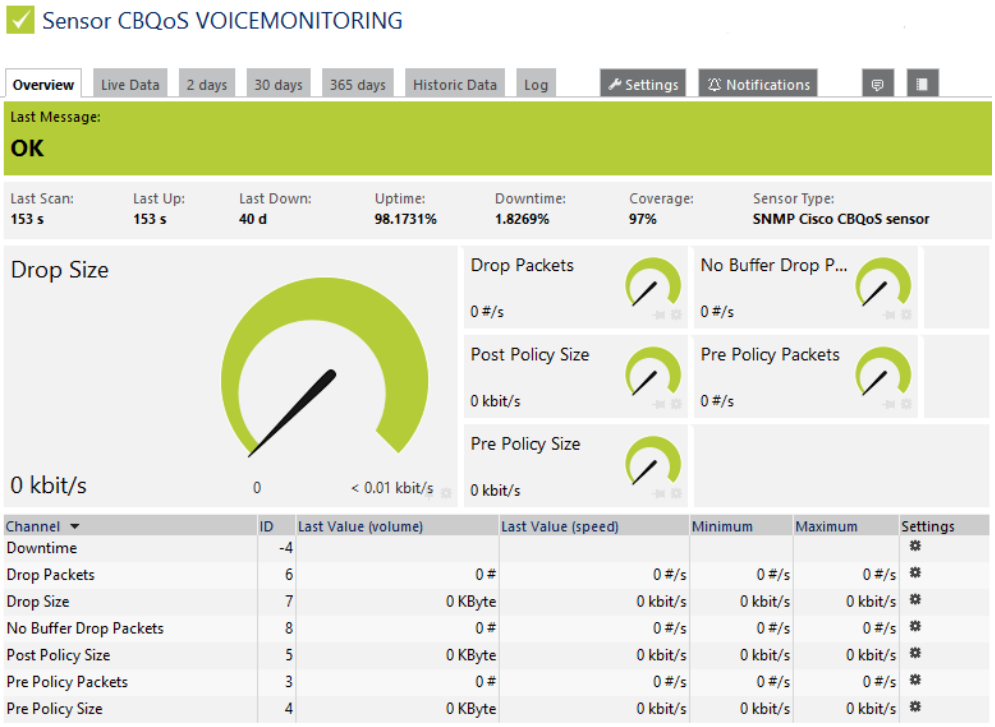
7.8.114 SNMP Cisco CBQoS Sensor

The SNMP Cisco CBQoS sensor monitors network parameters using Cisco's Class Based Quality of Service (CBQoS) via Simple Network Management Protocol (SNMP). It supports the classes Class Map, Match Statement, and Queueing.

The sensor can show the following depending on the particular class type:

- Current and maximum queue depth
- Pre policy packets
- Pre and post policy size
- Drop packets and size
- Drop packets without buffer
- Fragment packets and size.

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



SNMP Cisco CBQoS Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_cisco_cbqos.png

Remarks

- For a general introduction to the technology behind SNMP, please see the manual section Monitoring via SNMP 3087.

- For a general introduction to the technology behind Quality of Service monitoring, please see manual section **Monitoring Quality of Service** 3104.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the CBQoS entries you want to monitor. To monitor Quality of Service (QoS) via compatible devices, PRTG creates one sensor for each CBQoS entry you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

CLASS BASED QOS SPECIFIC

CBQoS Entries	Select the measurements you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.

BASIC SENSOR SETTINGS

Parent Tags	Shows **Tags** [124] that this sensor inherits [124] from its parent device, group, and probe [118]. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** [124], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited [124] from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

CLASS BASED QOS SPECIFIC

Object Type Interface	Shows further information about the parameter that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Description	
BitMask	
ObjectID	
ConfigID	

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

SENSOR DISPLAY

	You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

SCANNING INTERVAL

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

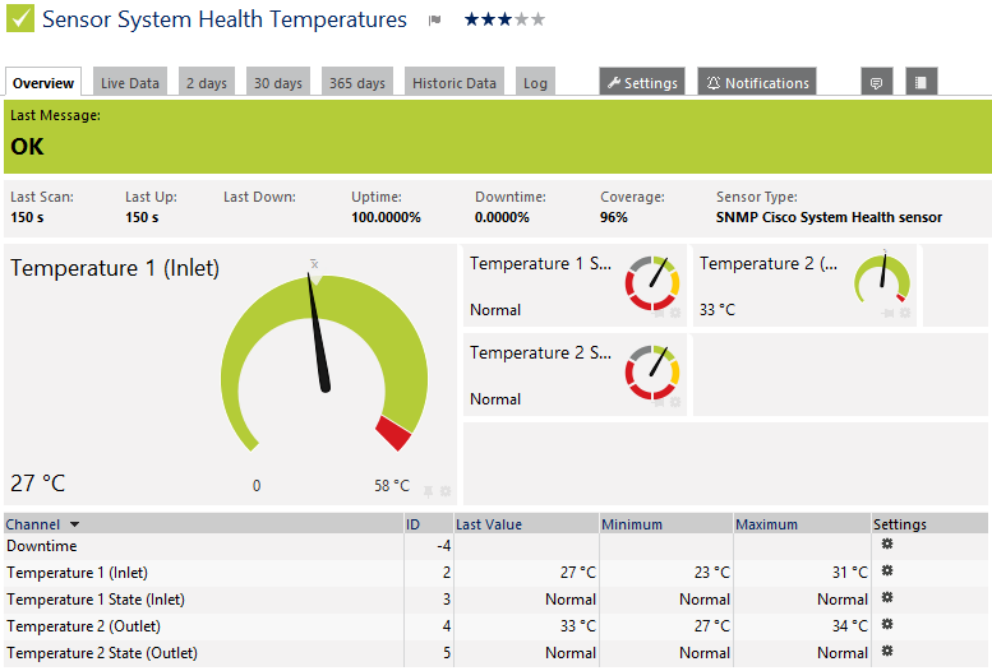
7.8.115 SNMP Cisco System Health Sensor

The SNMP Cisco System Health sensor monitors the system health of a Cisco device via Simple Network Management Protocol (SNMP).

It can show the following depending on the available components of your device:

- CPU load in percent
- Available memory in absolute and percentage values
- Status of power supplies
- Current temperature and temperature status

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



SNMP Cisco System Health Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_cisco_system_health.png

Remarks

- This sensor type has predefined limits for several metrics. You can change these limits individually in the channel settings. For detailed information about channel limits, please refer to the manual section **Sensor Channels Settings** 2782.
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.

- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the components you want to monitor. To monitor the system health of a Cisco device, PRTG creates one sensor for each measurement you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

CISCO SYSTEM HEALTH SPECIFIC

Measurement	Select the measurements you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.

BASIC SENSOR SETTINGS

Parent Tags	Shows **Tags** [124] that this sensor inherits [124] from its parent device, group, and probe [118]. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** [124], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited [124] from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

CISCO SYSTEM HEALTH SPECIFIC

Measurement	Shows the ID of the measurement that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

DEBUG OPTIONS

Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result.

DEBUG OPTIONS

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section **Data Storage** 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

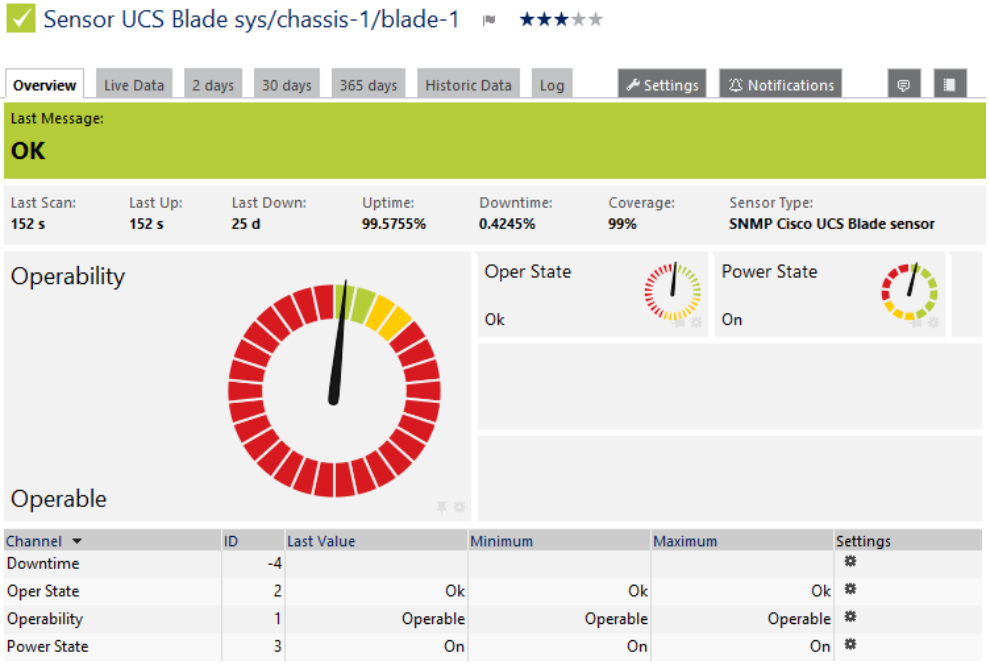
For more general information about settings, please see the **Object Settings** 188 section.

7.8.116 SNMP Cisco UCS Blade Sensor

The SNMP Cisco UCS Blade sensor monitors the health status of a Cisco Unified Computing System (UCS) blade server via Simple Network Management Protocol (SNMP).

It can show the following states:

- Operability
- Oper state
- Power state



SNMP Cisco UCS Blade Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_cisco_ucs_blade.png

Remarks

- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the blade servers you want to monitor. PRTG creates one sensor for each blade you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SENSOR SETTINGS

Blade Server	Select the blades you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	Enter one or more **Tags**, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SETTINGS

Blade Server Channel Mask Model Serial Number	Shows information about the blade server that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel.

SENSOR DISPLAY

	▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. ⓘ This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.

SCANNING INTERVAL

- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies [2822] in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector [210] to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** [360] or in the superior **Group Settings** [334].

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

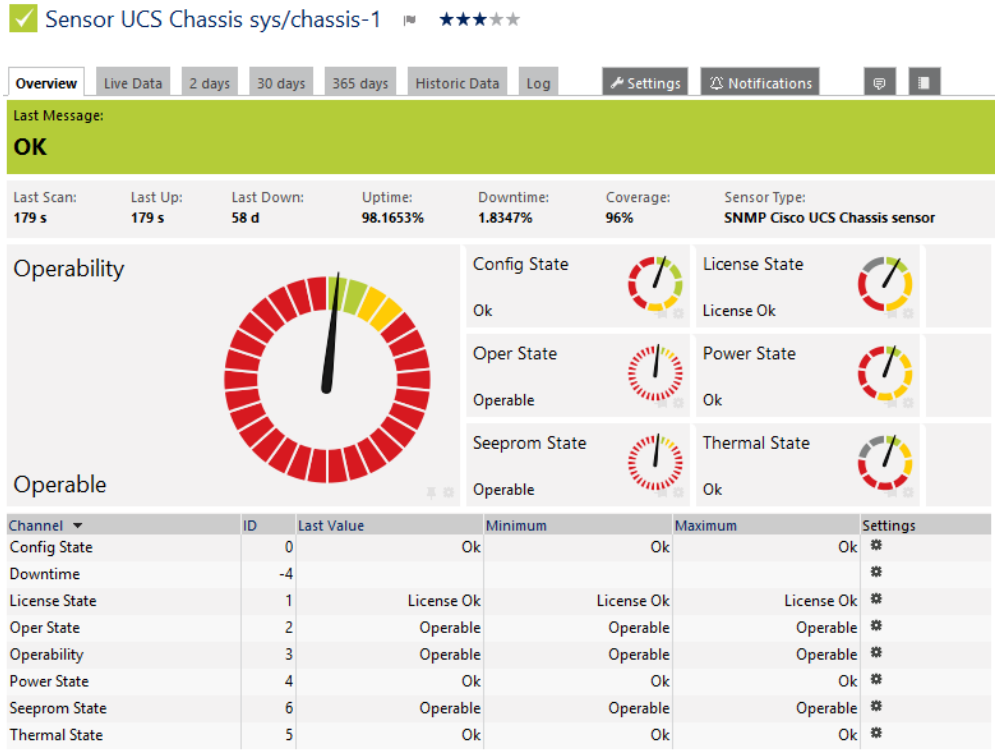
7.8.117 SNMP Cisco UCS Chassis Sensor

The SNMP Cisco UCS Chassis sensor monitors the health status of the chassis of a Cisco Unified Computing System (UCS) device via Simple Network Management Protocol (SNMP).

It can show the states of the following properties:

- Configuration
- License
- Oper
- Operability
- Power
- Thermal
- Serial electronic erasable programmable read-only memory (SEEPROM)

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



SNMP Cisco UCS Chassis Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_cisco_ucs_chassis.png

Remarks

- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the chassis you want to monitor. PRTG creates one sensor for each chassis you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SENSOR SETTINGS

Chassis	Select the chassis you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SETTINGS

Chassis	Shows the chassis that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. ⓘ You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor.

SENSOR DISPLAY

- **Show channels independently (default)**: Show an own graph for each channel.
- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.118 SNMP Cisco UCS Physical Disk Sensor

The SNMP Cisco UCS Physical Disk sensor monitors a physical disk of a Cisco Unified Computing System (UCS) device via Simple Network Management Protocol (SNMP).

It can show the following:

- Operability status of the disk
- Connection status of the disk

SNMP Cisco UCS Physical Disk Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_cisco_ucs_physical_disk.png

Remarks

- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

In order to monitor physical disks in a UCS device, PRTG will create one sensor for each disk you choose. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

UCS PHYSICAL DISK

Disks	Select the disks you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items. This list only shows working disks with the current status **Up** or **Warning**.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

BASIC SENSOR SETTINGS

	You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

UCS PHYSICAL DISK

Disk	Shows the disk that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Display Name	Shows the display name of the physical disk that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.

SCANNING INTERVAL

- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies [2822] in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector [210] to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** [360] or in the superior **Group Settings** [334].

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

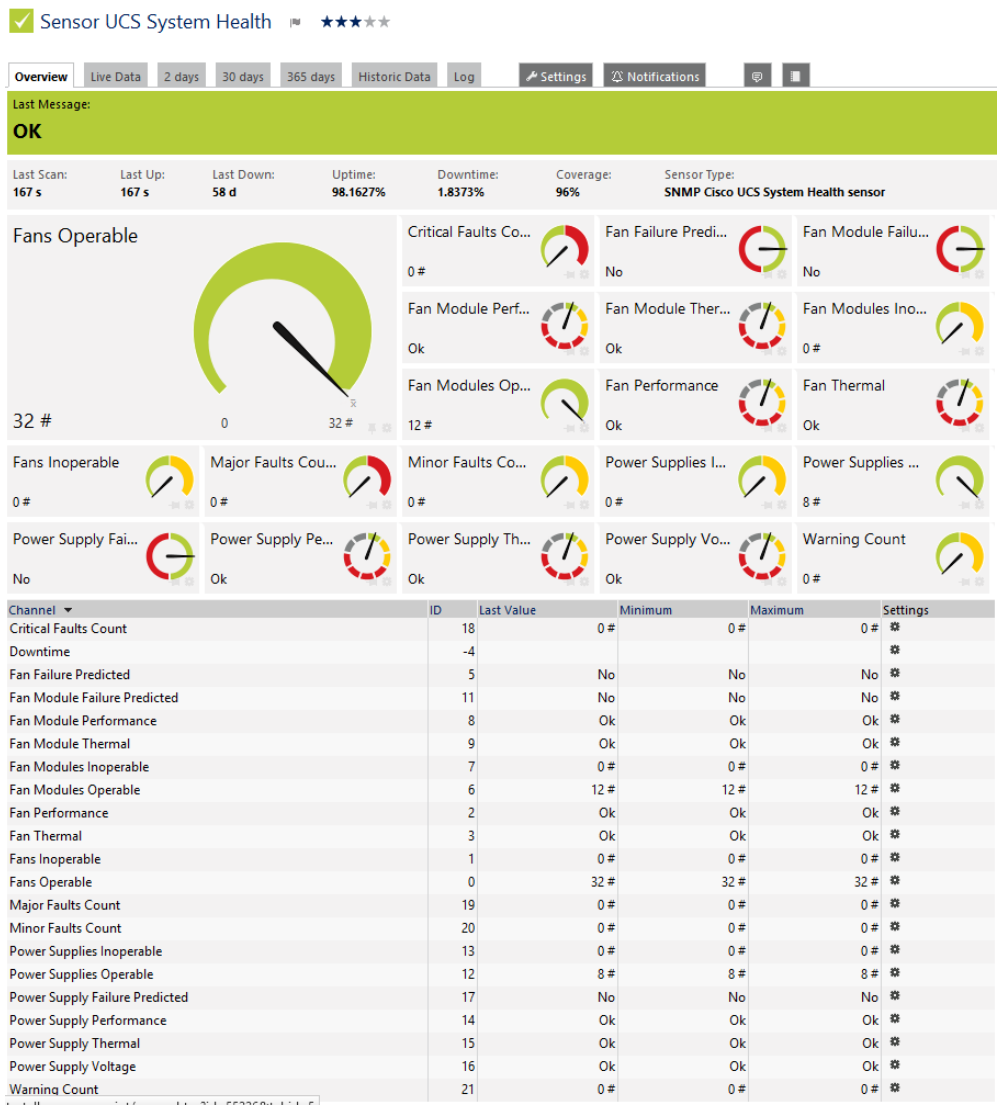
7.8.119 SNMP Cisco UCS System Health Sensor

The SNMP Cisco UCS System Health sensor monitors the system health of a Cisco Unified Computing System (UCS) device via Simple Network Management Protocol (SNMP).

It can show the following:

- Number of operable and inoperable fans
- Status of fan performance, fan thermal, and fan voltage
- Number of operable and inoperable fan modules
- Status of fan module performance, fan module thermal, and fan module voltage
- Number of operable and inoperable power supplies
- Status of power supply performance, power supply thermal, and power supply voltage
- Number of minor, major, and critical faults (which are not yet acknowledged in the UCS logs)
- Number of warnings (which are not yet acknowledged in the UCS logs)

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



SNMP Cisco UCS System Health Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_cisco_ucs_system_health.png

Remarks

- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.120 SNMP CPU Load Sensor

The SNMP CPU Load sensor monitors the system load using Simple Network Management Protocol (SNMP).

- It shows the load of several CPUs in percent.

Channel	ID	Last Value	Minimum	Maximum	Settings
Downtime	-4				
Processor 1	2	12 %	0 %	92 %	
Processor 10	11	9 %	0 %	96 %	
Processor 11	12	11 %	1 %	99 %	
Processor 12	13	11 %	1 %	100 %	
Processor 13	14	16 %	1 %	74 %	
Processor 14	15	10 %	1 %	81 %	
Processor 15	16	13 %	1 %	81 %	
Processor 16	17	11 %	1 %	87 %	
Processor 17	18	14 %	1 %	87 %	
Processor 18	19	12 %	1 %	100 %	
Processor 19	20	15 %	1 %	97 %	
Processor 2	3	9 %	0 %	99 %	
Processor 20	21	12 %	1 %	100 %	
Processor 21	22	18 %	1 %	85 %	
Processor 22	23	9 %	1 %	100 %	

SNMP CPU Load Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_cpu_load.png

Remarks

- It might not work to query data from a probe device via SNMP (querying localhost, 127.0.0.1, or ::1). Add this device to PRTG [275] with the IP address that it has in your network and create the SNMP sensor on this device instead.
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** [3087].

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

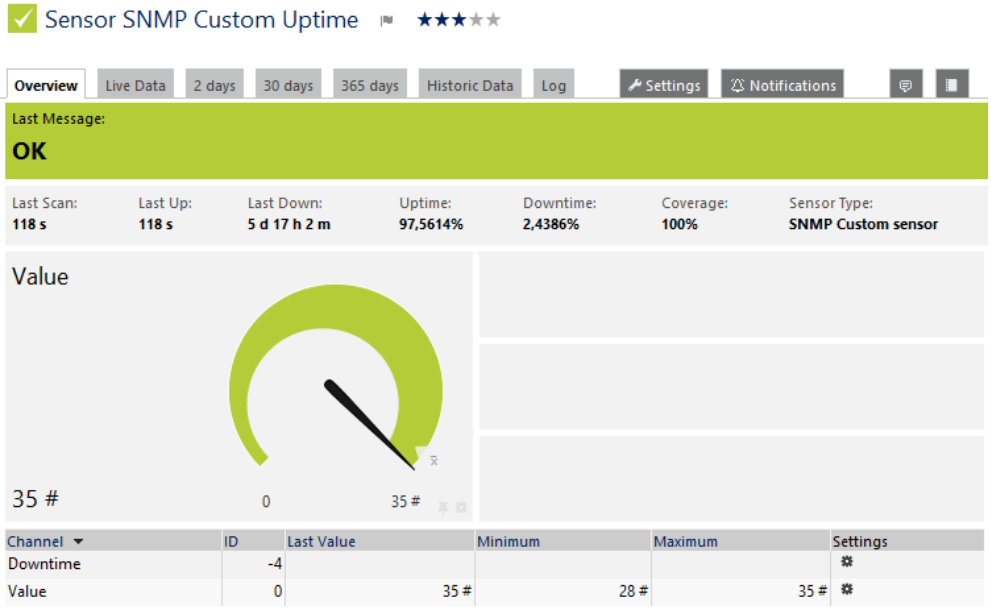
Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.121 SNMP Custom Sensor

The SNMP Custom sensor monitors a single parameter, that is returned by a specific Object Identifier (OID) using Simple Network Management Protocol (SNMP).

- This sensor shows a single numerical value (int64) for a given OID. Each OID always refers to a specific parameter of a certain SNMP device.



SNMP Custom Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_custom.png

Remarks

- It might not work to query data from a probe device via SNMP (querying localhost, 127.0.0.1, or ::1). Add this device to PRTG 275 with the IP address that it has in your network and create the SNMP sensor on this device instead.
- Knowledge Base: How do I find out what OID I need to use for a custom sensor?
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

OID VALUES

Channel Name	Enter a name for the channel in which the sensor shows the results for the given OID. Please enter a string. You can change this value later in the respective channel settings 2782 of this sensor.
Value Type	Select the expected numeric type of the results at the given OID. Choose between: ▪ **Gauge (unsigned Integer)**: Integer values, without an operational sign, such as 10 or 120. ▪ **Gauge (signed integer)**: For integer values, including an operational sign, such as -12 or 120. ▪ **Gauge (float)**: For float values, such as -5.80 or 8.23. ▪ **Delta (Counter)**: For counter values. PRTG will calculate the difference between the last and the current value. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	Enter one or more **Tags**, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

OID VALUES

OID Value	Enter the OID of the SNMP object you want to receive numerical data from. Most OIDs begin with 1.3.6.1. However, entering OIDs starting with 1.0, or 1.1, or 1.2 is also allowed. If you want to disable the validation of your entry entirely, add the string **norfccheck:** to the beginning of your OID, for example, **norfccheck:2.0.0.0.1**.
Unit String	Define the unit of the numerical data that this sensor receives from the given OID. Please enter a string.
Value Type	Shows the value type of the numerical data, that this sensor receives from the given OID. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Multiplication	If you want to multiply the received data with a certain value, enter the multiplier here. Please enter an integer value. Otherwise, use the default value 1 to not change the received value.
Division	If you want to divide the received data by a certain value, enter the divisor here. Please enter an integer value. Otherwise, use the default value 1 to not change the received value.
If Value Changes	Define what this sensor will do when the sensor value changes. You can choose between:

OID VALUES

- **Ignore changes (default)**: The sensor takes no action on change.
- **Trigger 'change' notification**: The sensor sends an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification 2791 whenever the sensor value changes.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.
- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply. If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply. If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Video Tutorial: How to Set Up an SNMP Custom Sensor

- https://www.paessler.com/support/videos/prtg-advanced/snmp-custom-and-library-sensor

Knowledge Base: How do I find out what OID I need to use for a custom sensor?

- https://kb.paessler.com/en/topic/903

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

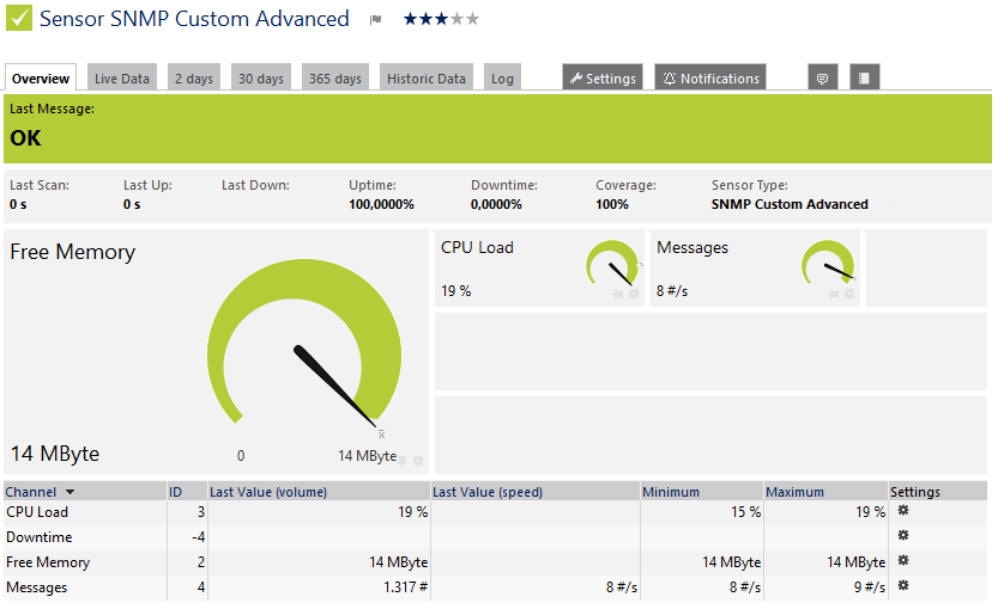
For more general information about settings, please see the **Object Settings** 188 section.

7.8.122 SNMP Custom Advanced Sensor

The SNMP Custom Advanced sensor monitors numerical values returned for Object Identifiers (OIDs) using Simple Network Management Protocol (SNMP).

- The sensor displays numerical values for given OIDs that refer to this specific SNMP device. Up to 10 OIDs and corresponding numerical values are possible.

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



SNMP Custom Advanced Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_custom_advanced.png

Remarks

- It might not work to query data from a probe device via SNMP (querying localhost, 127.0.0.1, or ::1). Add this device to PRTG 275 with the IP address that it has in your network and create the SNMP sensor on this device instead.
- Knowledge Base: How do I find out what OID I need to use for a custom sensor?
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

OID VALUES

Value Type	Select the expected numeric type of the results at the given OID. Choose between: ▪ **Gauge (unsigned Integer)**: For integer values, such as 10 or 120. ▪ **Gauge (signed integer)**: For integer values, such as -12 or 120. ▪ **Gauge (float)**: For float values, such as -5.80 or 8.23. ▪ **Delta (Counter)**: For counter values. PRTG will calculate the difference between the last and the current value. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Sensor Channel #2 – #10	You can create up to 10 different sensor channels for this sensor. You have to define at least one data channel, so you will see all available settings for Sensor Channel #1 without enabling it manually. Additionally you can define Sensor Channel #2 up to Sensor Channel #10. To do so, choose between: ▪ **Disable**: The sensor will not create this channel. ▪ **Enable**: The sensor will create this channel. Specify name, OID, value type, and unit for this channel below. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew. It is not possible to enable or disable sensor channels after creation of this sensor!

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

OID VALUES

Sensor Channel #x Name	Enter a name for the channel in which the sensor shows the results at the given OID. Please enter a string.
Sensor Channel #x OID	Enter the OID of the SNMP object you want to receive numerical data from. Most OIDs begin with 1.3.6.1. However, entering OIDs starting with 1.0, or 1.1, or 1.2 is also allowed. If you want to disable the validation of your entry during your typing entirely, add the string **norfccheck:** to the beginning of your OID, for example, **norfccheck:2.0.0.0.1**.
Sensor Channel #x Value Type	Shows the value type of the numerical data that this sensor receives from the given OID. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Sensor Channel #x Unit	Define the unit of the numerical data that this sensor receives from the given OID. Choose between:

OID VALUES

- BytesBandwidth
- BytesMemory
- BytesDisk
- Temperature
- Percent
- TimeResponse
- TimeSeconds
- TimeHours
- Count
- CPU
- BytesFile
- SpeedDisk
- SpeedNet
- Custom
- Value Lookup

For more information about the available units, please refer to the PRTG **Application Programming Interface (API) Definition** 3174 for custom sensors.

To use lookups 3183 with this channel, choose the unit **Value Lookup** and select your lookup file below. Do not use the unit **Custom** for using lookups with this sensor and do not use the channel settings 2782 to define a lookup file!

Sensor Channel #x Custom Unit

This setting is only visible if you select the **Custom** unit option above. Define a unit for the channel value. Please enter a string.

Sensor Channel #x Value Lookup

This setting is only visible if you select the **Value Lookup** option above. Choose a lookup 3183 file that you want to use with this channel.

Sensor Channel #y

This field shows the option you chose for this channel in the **Add Sensor** 1658 dialog, **Enable** or **Disable**. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

If you created this channel, you can define the settings of this channel as described above.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: How do I find out what OID I need to use for a custom sensor?

- https://kb.paessler.com/en/topic/903

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

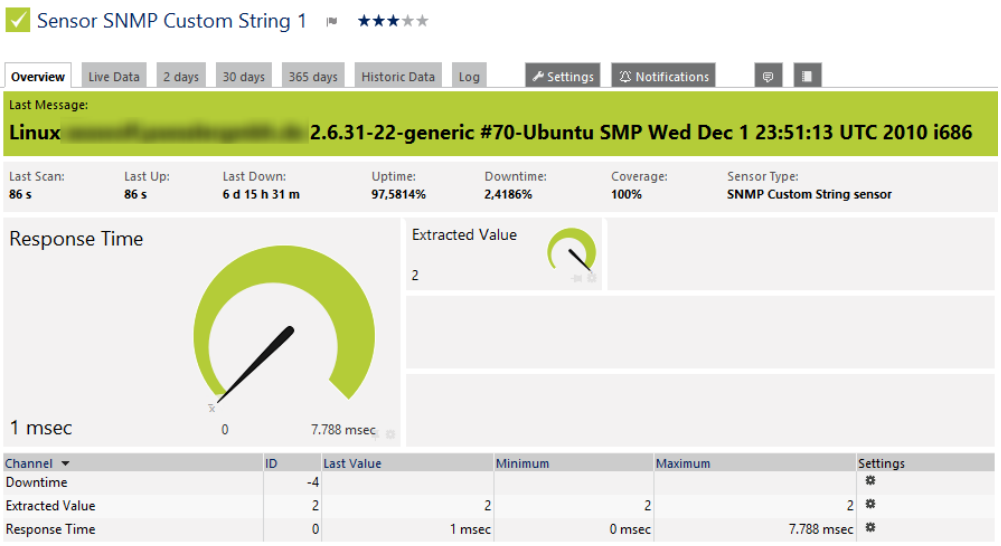
For more general information about settings, please see the **Object Settings** 188 section.

7.8.123 SNMP Custom String Sensor

The SNMP Custom String sensor monitors a string returned by a specific Object Identifier (OID) using Simple Network Management Protocol (SNMP). It can check for keywords. If you want to set limits to the sensor channel value, you can also extract a numeric value contained in the string.

This sensor shows the following:

- Response time of the monitored device
- Optionally a value extracted from the string
- In the sensor message, the sensor shows the string you search [1670] for and which is the reason for a current **Warning** or **Down** status [163].



SNMP Custom String Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_custom_string.png

Remarks

- It might not work to query data from a probe device via SNMP (querying localhost, 127.0.0.1, or ::1). Add this device to PRTG [275] with the IP address that it has in your network and create the SNMP sensor on this device instead.
- Knowledge Base: How do I find out what OID I need to use for a custom sensor?
- Example: Number Extraction with Regular Expression [1677]
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** [3087].

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

OID VALUES

OID Value	Enter the OID of the SNMP object you want to receive a string from. Most OIDs begin with 1.3.6.1. However, entering OIDs starting with 1.0, or 1.1, or 1.2 is also allowed. If you want to disable the validation of your entry entirely, add the string **norfccheck:** at the beginning of your OID, for example, **norfccheck:2.0.0.0.1**.
Maximum Length of String	Define the maximum allowed length of the string to be received from the SNMP object at the given OID. If the string is longer than this value, the sensor shows a **Down** status 163. Please enter an integer value or leave the field empty.
If Value Changes	Define what this sensor will do when the sensor value changes. You can choose between: ▪ **Ignore changes (default)**: The sensor takes no action on change. ▪ **Trigger 'change' notification**: The sensor sends an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification 2791 whenever the sensor value changes.

KEYWORD SEARCH

Response Must Include (Error State)	Define which string must be part of the data that is received from the SNMP object at the given OID. You can either enter plain text or a **Regular Expression** 3193. If the data does not include the search pattern, the sensor shows a **Down** status 163. Please enter a string or leave the field empty.
For Keyword Search Use	Define in which format you have entered the search expression in the field above. ▪ **Plain Text**: Search for the string as plain text. The characters asterisk * and question mark ? work here as placeholder, whereas * stands for no or any number of characters and ? stands for exactly one character (as known from Windows search). You cannot disable this behavior, so the literal search for these characters is not possible with plain text search. ▪ **Regular Expression**: Use the search pattern as a **Regular Expression** 3193.

KEYWORD SEARCH

Response Must Not Include (Error State)	Define which string must not be part of the data that is received form the SNMP object at the given OID. You can either enter plain text or a **Regular Expression** [3193]. If the data does include the search pattern, the sensor shows a **Down** status [163]. Please enter a string or leave the field empty.
For Keyword Search Use	Define in which format you have entered the search expression in the field above. ▪ **Plain Text**: Search for the string as plain text. The characters asterisk * and question mark ? work here as placeholder, whereas * stands for no or any number of characters and ? stands for exactly one character (as known from Windows search). You cannot disable this behavior, so the literal search for these characters is not possible with plain text search. ▪ **Regular Expression**: Use the search pattern as a **Regular Expression** [3193].
Response Must Include (Warning State)	Define which string must be part of the data that is received from the SNMP object at the given OID. You can either enter plain text or a **Regular Expression** [3193]. If the data does not include the search pattern, the sensor shows a **Warning** status [163]. Please enter a string or leave the field empty.
For Keyword Search Use	Define in which format you have entered the search expression in the field above. ▪ **Plain Text**: Search for the string as plain text. The characters asterisk * and question mark ? work here as placeholder, whereas * stands for no or any number of characters and ? stands for exactly one character (as known from Windows search). You cannot disable this behavior, so the literal search for these characters is not possible with plain text search. ▪ **Regular Expression**: Use the search pattern as a **Regular Expression** [3193].
Response Must Not Include (Warning State)	Define which string must not be part of the data that is received form the SNMP object at the given OID. You can either enter plain text or a **Regular Expression** [3193]. If the data does include the search pattern, the sensor shows a **Warning** status [163]. Please enter a string or leave the field empty.
For Keyword Search Use	Define in which format you have entered the search expression in the field above.

KEYWORD SEARCH

- **Plain Text**: Search for the string as plain text. The characters asterisk * and question mark ? work here as placeholder, whereas * stands for no or any number of characters and ? stands for exactly one character (as known from Windows search). You cannot disable this behavior, so the literal search for these characters is not possible with plain text search.
- **Regular Expression**: Use the search pattern as a **Regular Expression** 3193.

EXTENDED PROCESSING

Interpret Result as

Define the type of the received string. Choose between:

- **String (default)**: Handle the result as common string.
- **Hexadecimal bytes (as in MAC addresses)**: Handle the result as hexadecimal bytes. For example, choose this option when monitoring MAC addresses.
- **Decimal bytes (as in IP addresses)**: Handle the result as decimal bytes. For example, choose this option when monitoring IP addresses.

Extract Number Using Regular Expression

Define if you want to filter out a numeric value from the string received from the SNMP object at the given OID. You can convert this into a float value to use it with channel limits (see **Sensor Channels Settings** 2782).

- **No extraction**: Do not extract a float value. Use the result as a string value.
- **Extract a numeric value using a regular expression**: Use a regular expression to identify a numeric value in the string and convert it to a float value. Define below. See also the example 1677 below.

Regular Expression

This setting is only visible if you enable number extraction above. Enter a **Regular Expression** 3193 to identify the numeric value you want to extract from the string returned by the SNMP object at the given OID. You can use capturing groups here. Make sure the expression returns numbers only (including decimal and thousands separators). The result will be further refined by the settings below.

EXTENDED PROCESSING

Index of Capturing Group	This setting is only visible if you enable number extraction above. If your regular expression uses capturing groups, please specify which one will be used to capture the number. Please enter an integer value or leave the field empty.
Decimal Separator	This setting is only visible if you enable number extraction above. Define which character is used as decimal separator for the number extracted above. Please enter a string or leave the field empty.
Thousands Separator	This setting is only visible if you enable number extraction above. Define which character is used as thousands separator for the number extracted above. Please enter a string or leave the field empty.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

Example: Number Extraction with Regular Expression

If you want to extract a number in the response string using a regular expression, please note that the index for captures in this sensor is based on 1 (**not on 0**). Furthermore, capturing groups are not created automatically. The example below will illustrate this issue.

Consider the following string as returned by a request for CPU usage:

```
5 Sec (3.49%), 1 Min (3.555%), 5 Min (3.90%)
```

Assuming you would like to filter for the number 3.555, i.e., the percentage in the second parentheses. Then enter the following regex in the **Regular Expression** field:

```
(\d+\.\d+).*?(\d+\.\d+).*?(\d+\.\d+)
```

As **Index of Capturing Group** enter 3. This will extract the desired number 3.555.

The index has to be 3 in this case because the capturing groups here are the following:

- Group 1 contains "3.49%), 1 Min (3.555), 5 Min (3.90"

- Group 2 contains "3.49"
- Group 3 contains "3.555"
- Group 4 contains "3.90"

Please keep in mind this note about index and capturing groups when using number extraction.

It is not possible to match an empty string with the PRTG regex sensor search.

More

Knowledge Base: How do I find out what OID I need to use for a custom sensor?

- https://kb.paessler.com/en/topic/903

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

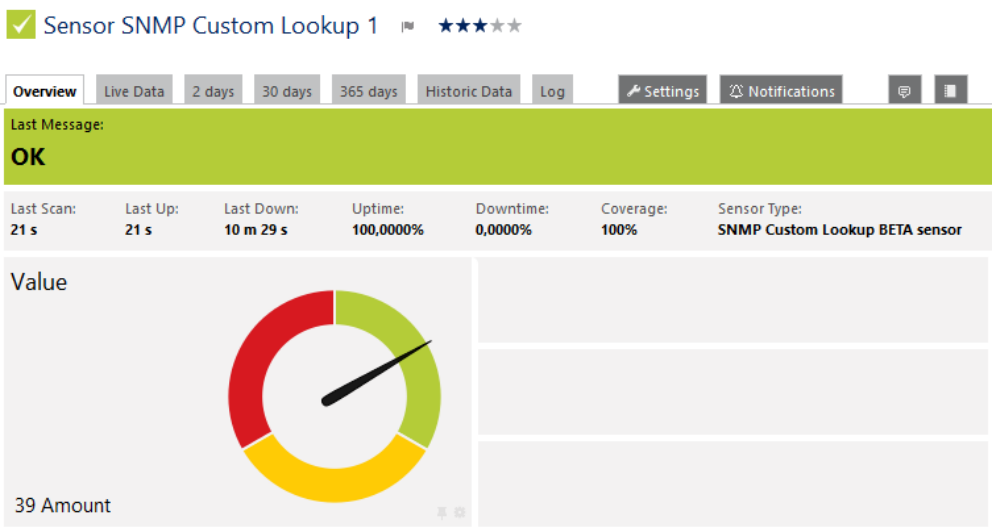
Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.124 SNMP Custom String Lookup Sensor

The SNMP Custom String Lookup sensor monitors a string that a specific Object Identifier (OID) returns via Simple Network Management Protocol (SNMP). It can map the string directly to a sensor status [163] by using a defined lookup file [3183]. Basically, this sensor type does a "reverse lookup". You have to define all potential return strings in the lookup file as text values, each in one lookup entry. Graphs and data tables show the value to which the string is mapped, usually an integer (lookup type [3190] **SingleInt**). See section **Example** [1686] below.

- This sensor shows a retrieved string value and its status, as defined in the corresponding lookup file.



SNMP Custom Lookup Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_custom_lookup.png

Remarks

- See manual section **SNMP Custom String Lookup Sensor—Example** [1686] for a sample lookup definition for this sensor type.
- It might not work to query data from a probe device via SNMP (querying localhost, 127.0.0.1, or ::1). Add this device to PRTG [275] with the IP address that it has in your network and create the SNMP sensor on this device instead.
- Knowledge Base: How do I find out what OID I need to use for a custom sensor?
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** [3183].
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** [3087].
- BETA Currently, this sensor type is in beta status. The methods of operating can change at any time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

OID VALUES

Channel Name	Enter a name for the channel in which the sensor shows the results at the given OID. Please enter a string. You can change this value later in the respective channel settings 2782 of this sensor.
Lookup	Select a lookup file that you stored in the **\lookups\custom** subfolder of your PRTG installation. This lookup file must contain all potential strings that the monitored OID can return.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	Enter one or more **Tags**[124], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited[124] from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

OID VALUES

OID Value	Enter the OID of the SNMP object you want to receive a string from. Most OIDs begin with 1.3.6.1. However, entering OIDs starting with 1.0, or 1.1, or 1.2 is also allowed. If you want to disable the validation of your entry entirely, add the string **norfccheck:** at the beginning of your OID, for example, **norfccheck:2.0.0.0.1**.
Lookup	Shows the lookup file that this sensor uses. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
If Value Changes	Define what this sensor will do when the sensor value changes. You can choose between: ▪ **Ignore changes (default)**: The sensor takes no action on change. ▪ **Trigger 'change' notification**: The sensor sends an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification[2791] whenever the sensor value changes.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

Example

You have to provide all possible return strings for this sensor in one lookup file. For example, consider an OID that can return one of the three strings Good, Deficient, or Bad. Then you have to define a lookup file 3183 for this sensor that contains all these possible string values as text, each text value in one lookup entry:

```
<?xml version="1.0" encoding="UTF-8"?>
<ValueLookup id="mylookupfile" desiredValue="0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:
       <Lookups>
              <SingleInt state="Ok" value="0">
              Good
              </SingleInt>
              <SingleInt state="Warning" value="1">
              Deficient
              </SingleInt>
              <SingleInt state="Error" value="2">
              Bad
              </SingleInt>
    </Lookups>
</ValueLookup>
```

If a retrieved string matches one of the text values, the sensor maps it into the defined integer value ("reverse lookup") that is shown, for example, in data graphs. Depending on the integer, the sensor shows the according status and converts the integer back to the original string to show it as channel value. If the OID returns a string that the lookup definition does not contain, the sensor shows a **Down** status with a corresponding error message.

For example, you create an SNMP Custom String Lookup sensor, apply the example lookup definition from above (store it into the **\lookups\custom** subfolder of your PRTG installation), and the given OID returns the string Good. Then the sensor maps Good into the integer value 0, shown in the live graph of the sensor, for example. According to the status definition state="Ok", the sensor status is **Up** in this case. The integer 0 is converted back to the string Good which is shown as channel value.

The string match is not case sensitive.

Please use the lookup type **SingleInt** for this sensor. BitFields and ranges are not supported!

If you imported an SNMP library 1915 (this is an oidlib file) that contains lookups 3183 (you can see this in section **Lookup** in the MIB Importer), you can define your own sensor states for returning values. Use the **lookupname** of the imported SNMP library as **id** parameter in a custom lookup definition. This overrides the lookups which an oidlib might contain with your own status definitions. See section **Define Lookups—Customizing Lookups** 3188 for details about this mechanism.

More

Knowledge Base: How do I find out what OID I need to use for a custom sensor?

- https://kb.paessler.com/en/topic/903

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

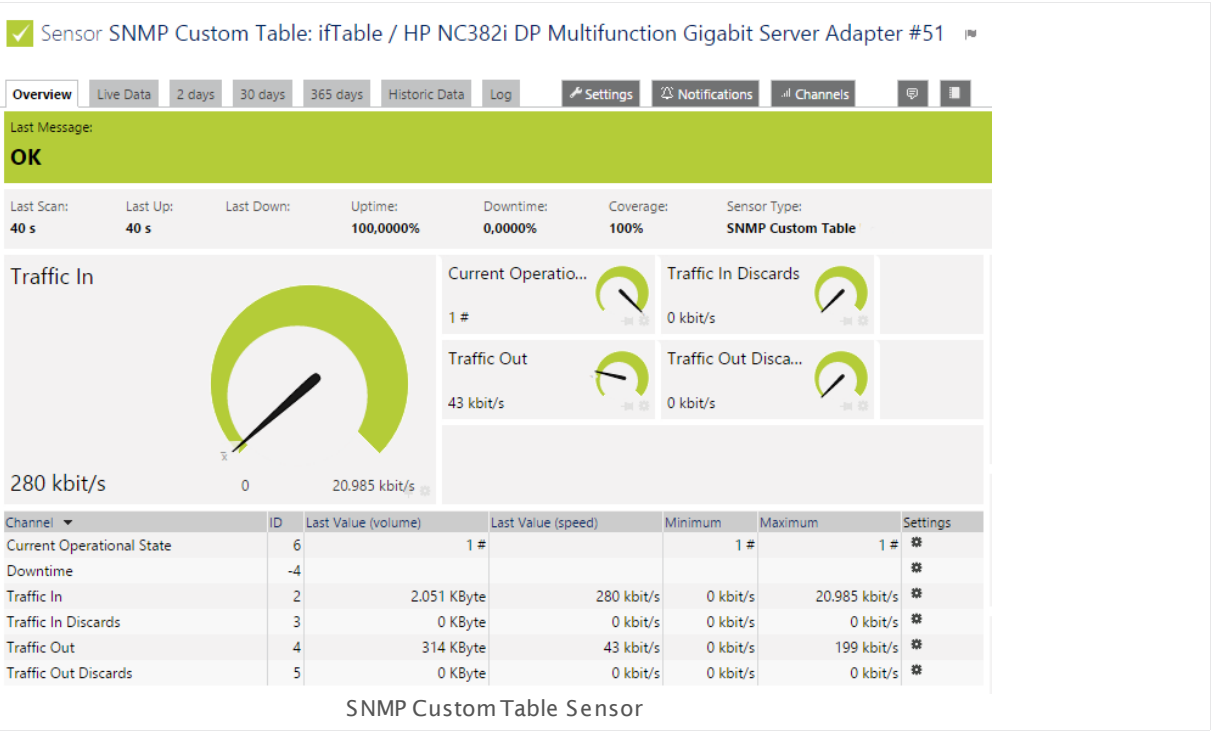
For more general information about settings, please see the **Object Settings** 188 section.

7.8.125 SNMP Custom Table Sensor

The SNMP Custom Table Sensor monitors entries from a table that is provided via Simple Network Management Protocol (SNMP). You can create one new sensor per table row. For each sensor, you can define up to ten channels. Each channel shows the value of one defined table column.

- It can show numerical values in up to 10 channels per table row.

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



SNMP Custom Table Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_custom_table.png

Remarks

- It might not work to query data from a probe device via SNMP (querying localhost, 127.0.0.1, or ::1). Add this device to PRTG 275 with the IP address that it has in your network and create the SNMP sensor on this device instead.
- Knowledge Base: How do I find out what OID I need to use for a custom sensor?
- Knowledge Base: What can I monitor with the SNMP Custom Table Sensor?
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

PRTG creates one SNMP Table sensor for each table row that you select in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SNMP TABLE

Table OID

Enter the OID of the SNMP table you want to monitor. The OID needs to point directly to an object that represents an SNMP table. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Without entering an OID, you cannot proceed to the sensor and sensor channel creation.

BASIC SENSOR SETTINGS

Sensor Name

Enter a meaningful name to identify the sensor. You can use the placeholders [tablename] and [rowidentifier]. They will be replaced with the name of the table and the identifying value of the chosen row respectively. You can choose the column that provides the row identifier in the **Identification Column** option below.

You can also enter a valid OID which is part of a different SNMP table, for example, [1.3.6.1.2.1.2.2.1.2], to query information that is not contained in the current table. The same index as in the original table will be added to the OID.

TABLE SPECIFIC

Table

Choose the relevant table rows in which you find the data that you want to monitor. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

PRTG shows you the table that the OID you entered before returns. To better find what you want to monitor, especially in large tables, use the search function in the upper right corner.

Identification Column

Define the identification column for the SNMP Table sensor(s) you want to create. The sensor uses this column to uniquely identify each table row. This column should preferably be unique because it will allow the sensor to keep track of changing indexes.

The value of the column that you choose as the identification column will replace the **[rowidentifier]** in the sensor name. This allows you to distinguish sensors that are created for the same SNMP table.

One new sensor is created for each table row you choose.

Sensor Channel #2 – #10

You can create up to 10 different sensor channels for this sensor. You have to define at least one data channel, so you will see all available settings for Sensor Channel #1 without enabling it manually. Additionally you can define Sensor Channel #2 up to Sensor Channel #10. To do so, choose between:

- **Disable**: The sensor will not create this channel.
- **Enable**: Create an additional channel and define all its characteristics below, its name, column, value type, and unit.

It is not possible to enable or disable sensor channels after the creation of this sensor!

All sensor channels that you define while creating an SNMP Table sensor will be the same for all sensors for each table row.

Value Type

Select the expected type of the results in this channel. Choose between:

- **Gauge (unsigned Integer)**: For integer values, such as 10 or 120.
- **Gauge (signed integer)**: For integer values, such as -12 or 120.
- **Gauge (float)**: For float values, such as -5.80 or 8.23.

TABLE SPECIFIC

- **Delta (Counter)**: For counter values. PRTG will calculate the difference between the last and the current value.

Please see below[1693] for the other channel settings that can be changed also after the sensor has been created.

This sensor monitors numerical values only. Make sure that you do not select columns that return strings because they lead to a Down status[163]. For example, if you monitor an **ifTable**, we recommend that you do not select an **ifDescr** column because this will result in an error.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings**[360] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree[151], as well as in alarms[190], logs[198], notifications[2829], reports[2862], maps[2885], libraries[2845], and tickets[200].
Parent Tags	Shows **Tags**[124] that this sensor inherits[124] from its parent device, group, and probe[118]. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags**[124], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited[124] from objects further up in the device tree. These are visible above as **Parent Tags**.

BASIC SENSOR SETTINGS

Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SNMP TABLE

Table OID	Shows the OID of the SNMP table that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

TABLE SPECIFIC

Identifier	This is the value of the column that you selected as the **Identification Column** during the sensor creation. It is also displayed in the sensor name to distinguish it from other sensors you created for the same table with other table rows. You can change the identifier if you want to.
Identification Column	Shows the table column that you chose as the identification column. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Sensor Channel #x Name	Enter a name for the channel in which the sensor shows the desired result. Please enter a string.
Sensor Channel #x Column	Select the table column that together with the table row points to the value that you want to monitor in this channel. You can choose between the available columns of the table that you monitor.
Sensor Channel #x Value Type	Shows the value type of the data that this sensor receives in this channel. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Sensor Channel #x Unit	Define the unit of the data that this sensor receives in this channel. Choose between: ▪ BytesBandwidth ▪ BytesMemory

TABLE SPECIFIC

- BytesDisk
- Temperature
- Percent
- TimeResponse
- TimeSeconds
- TimeHours
- Count
- CPU
- BytesFile
- SpeedDisk
- SpeedNet
- Custom
- Value Lookup

For more information about the available units, please refer to the PRTG **Application Programming Interface (API) Definition** 3174 for custom sensors.

To use lookups 3183 with this channel, choose the unit **Value Lookup** and select your lookup file below. Do not use the unit **Custom** for using lookups with this sensor and do not use the channel settings 2782 to define a lookup file!

Sensor Channel #x Custom Unit	This setting is only visible if you select the **Custom** unit option above. Define a unit for the channel value. Please enter a string.
Sensor Channel #x Value Lookup	This setting is only visible if you select the **Value Lookup** option above. Select a lookup 3183 file that you want to use with this channel.
Sensor Channel #x+1	Shows if you enabled or disabled a channel. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: What can I monitor with the SNMP Custom Table Sensor?

- https://kb.paessler.com/en/topic/68539

Knowledge Base: How to monitor a no-break (UPS) device complying to the UPS-MIB (RFC 1628)

- https://kb.paessler.com/en/topic/72117

Knowledge Base: How do I find out what OID I need to use for a custom sensor?

- https://kb.paessler.com/en/topic/903

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

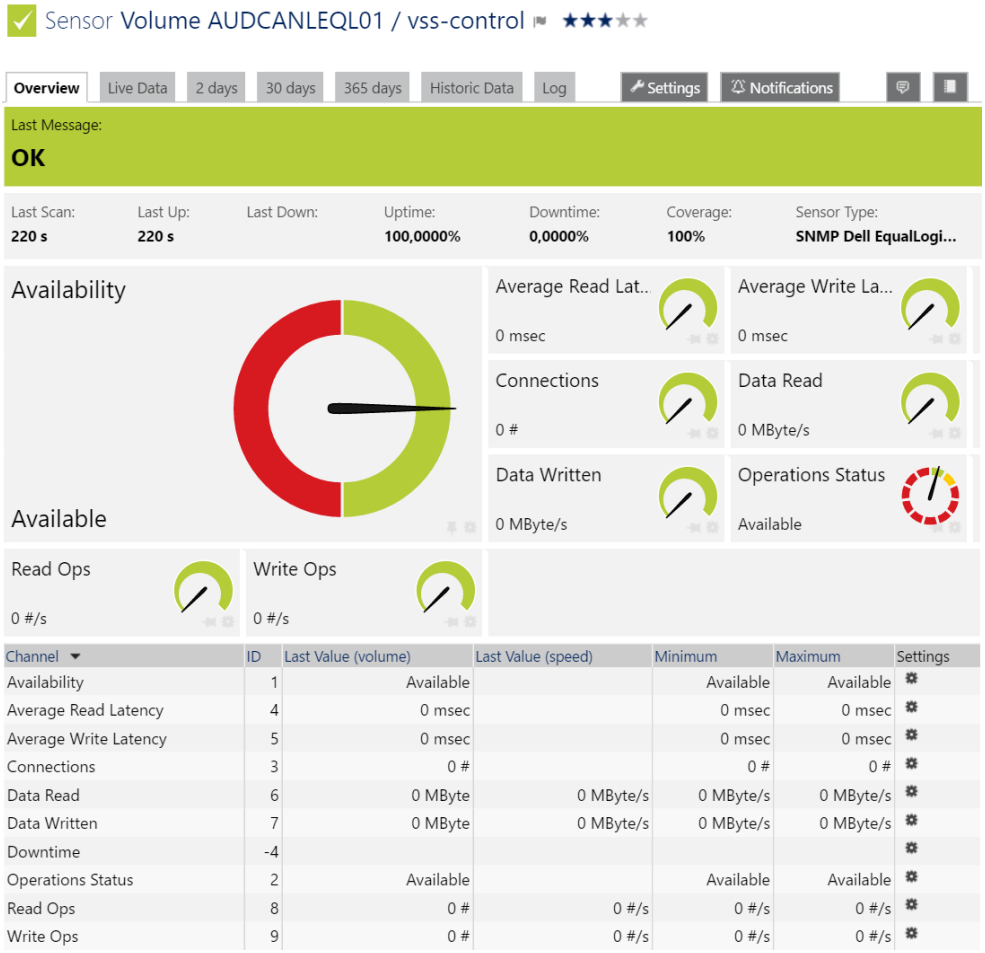
For more general information about settings, please see the **Object Settings** 188 section.

7.8.126 SNMP Dell EqualLogic Logical Disk Sensor

The SNMP Dell EqualLogic Logical Disk sensor monitors a volume of a Dell EqualLogic storage system via Simple Network Management Protocol (SNMP).

The sensor provides the following information:

- Availability
- Average read/write latency
- Number of connections
- Amount of read/written data
- Operational status
- Number of IOPS (Input/Output operations per second)



Channel	ID	Last Value (volume)	Last Value (speed)	Minimum	Maximum	Settings
Availability	1	Available		Available	Available	
Average Read Latency	4	0 msec		0 msec	0 msec	
Average Write Latency	5	0 msec		0 msec	0 msec	
Connections	3	0 #		0 #	0 #	
Data Read	6	0 MByte	0 MByte/s	0 MByte/s	0 MByte/s	
Data Written	7	0 MByte	0 MByte/s	0 MByte/s	0 MByte/s	
Downtime	-4					
Operations Status	2	Available		Available	Available	
Read Ops	8	0 #	0 #/s	0 #/s	0 #/s	
Write Ops	9	0 #	0 #/s	0 #/s	0 #/s	

SNMP Dell EqualLogic Logical Disk Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_dell_equallogic_logical_disk.png

Remarks

- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the volume(s) from the storage system that you want to monitor. PRTG creates one sensor for each volume you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

DELL EQUALLOGIC SPECIFIC

Volume	Select the volume(s) you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DELL EQUALLOGIC SPECIFIC

Volume	Shows the volume that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Member ID	Shows the identifier of the array member. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Volume ID	Shows the ID of the volume that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Volume Description	Shows the description of the volume that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

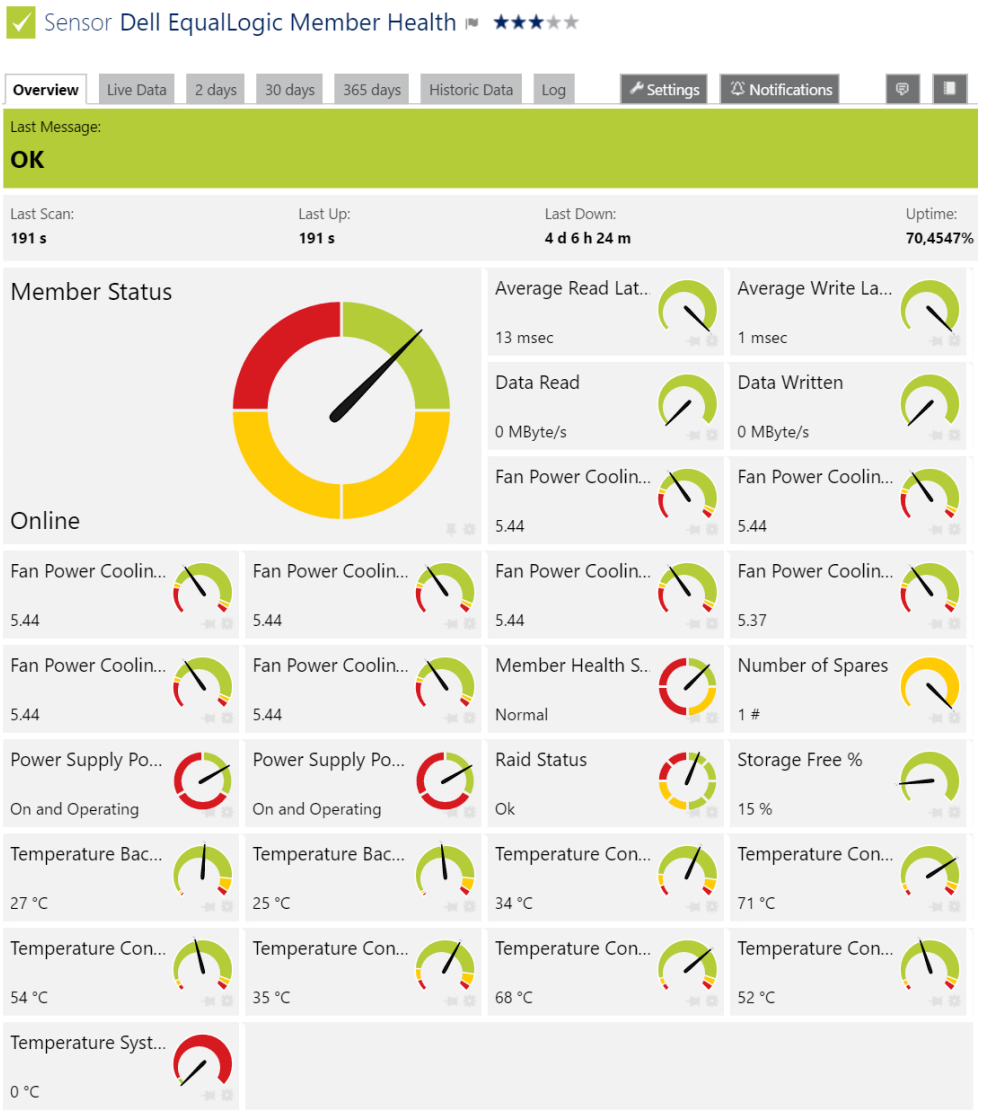
For more general information about settings, please see the **Object Settings** 188 section.

7.8.127 SNMP Dell EqualLogic Member Health Sensor

The SNMP Dell EqualLogic Member Health sensor monitors the health of an array member of an EqualLogic storage system via Simple Network Management Protocol (SNMP).

The sensor provides the following information:

- Member status
- Cooling power of the fan module in rpm (rotations per minute)
- Power supply status of cooling system
- Temperature of the backplane
- Temperature measured by temperature control module
- System temperature
- Member health status
- RAID status
- Average read/write latency in milliseconds or as percentage of the largest value
- Free storage capacity
- Amount of data handled per second
- Number of spare drives available



SNMP Dell EqualLogic Member Health Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_dell_equallogic_member_health.png

Remarks

- This sensor type works with SNMP v2c and SNMP v3. It does not support SNMP v1. Please ensure you set the correct **SNMP Version** in the **Credentials for SNMP Devices** settings of the parent device or inherit it from objects higher in the hierarchy [118].
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** [3183].
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** [3087].

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the disk(s) on the drive you want to monitor. PRTG creates one sensor for each disk you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

DELL EQUALLOGIC SPECIFIC

Array Member	Select the array member(s) you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.

BASIC SENSOR SETTINGS

Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DELL EQUALLOGIC SPECIFIC

Array Member	Shows the name of the member this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Group ID	Shows the group ID of the disk that this sensor monitors.. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Member ID	Shows the group member ID of the disk that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

SENSOR DISPLAY

	You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

SCANNING INTERVAL

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

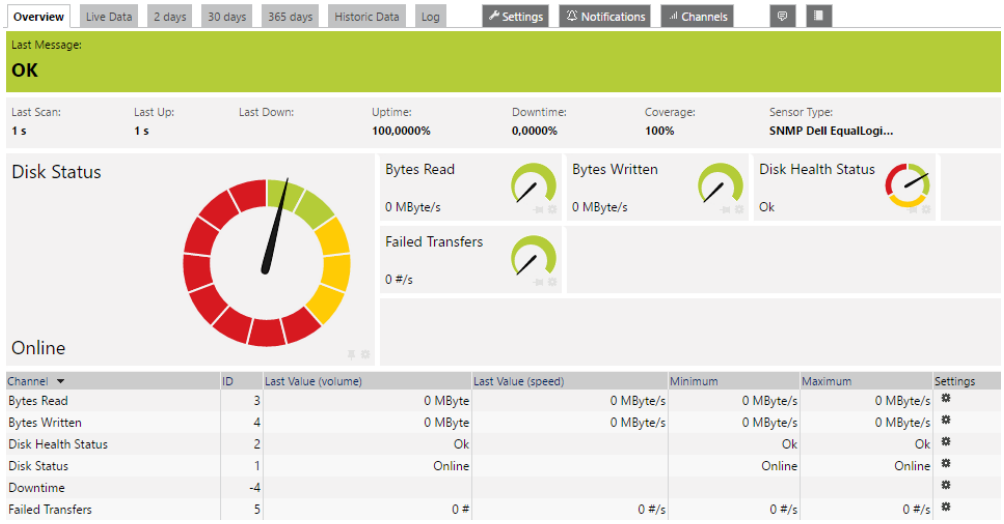
For more general information about settings, please see the **Object Settings** 188 section.

7.8.128 SNMP Dell EqualLogic Physical Disk Sensor

The SNMP Dell EqualLogic Physical Disk sensor monitors a disk in a Dell EqualLogic storage system via Simple Network Management Protocol (SNMP).

The sensor provides the following information:

- Disk status
- Bytes read/written
- Failed transfers
- Health status of disk



SNMP Dell EqualLogic Physical Disk Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_dell_equallogic_physical_disk.png

Remarks

- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the array member(s) of the Dell EqualLogic storage system you want to monitor. PRTG creates one sensor for each disk you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

DELL EQUALLOGIC SPECIFIC

Disk	Select the disk(s) you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

BASIC SENSOR SETTINGS

	You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DELL EQUALLOGIC SPECIFIC

Disk	Shows the disk that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Group ID	Shows the group ID of the disk that this sensor monitors.. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Member ID	Shows the group member ID of the disk that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Disk Slot	Shows the slot number of disk that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Serial Number	Shows the serial number of the disk that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Manufactured	Shows the production date of the disk that this sensor monitors. If this field is empty, the disk does not provide information about the date (this depends on the manufacturer). Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

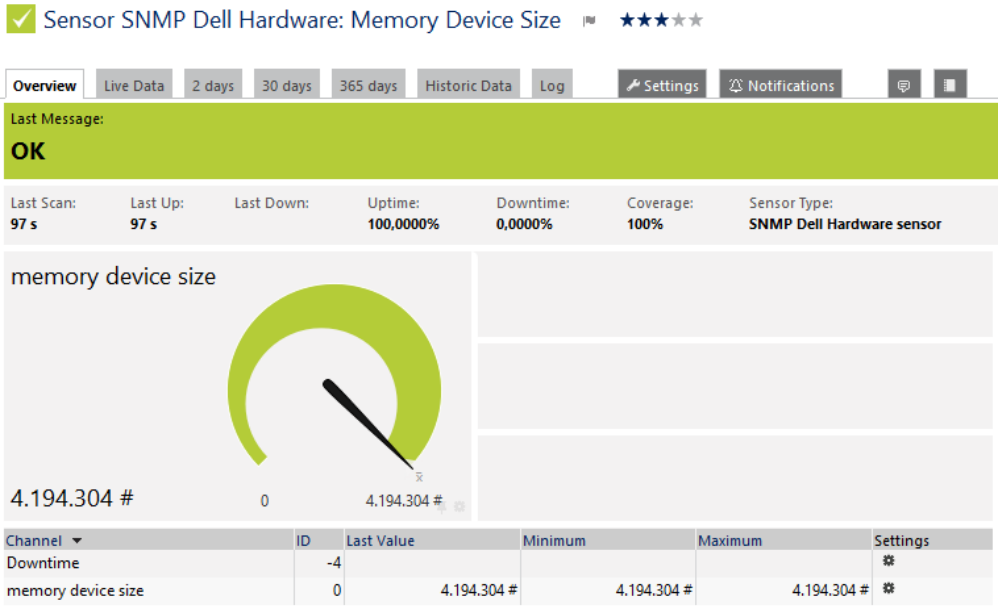
7.8.129 SNMP Dell Hardware Sensor

The SNMP Dell Hardware sensor monitors performance counters on a Dell hardware device using Simple Network Management Protocol (SNMP). The data that you can monitor with this sensor depends on the available performance counters on the target system.

This sensor shows a value returned by a specific Dell hardware OID, for example:

- Data about the system management software
- Data about system status
- Information about chassis and BIOS
- Various hardware parameters
- Other valuable data

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



SNMP Dell Hardware Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_dell_hardware.png

Remarks

- Requires 1730 the Dell OpenManage Server Administrator to be installed on the monitored Dell device.
- Knowledge Base: What do I need to monitor Dell servers?
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Requirement: Dell OpenManage Server Administrator

This sensor needs the Dell OpenManage Server Administrator tool to be installed on the Dell hardware device to monitor it. Please make sure that you enable SNMP in the OpenManage Server Administrator. For details, please see section **More** 1736 below.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the Dell performance counter you want to monitor. PRTG creates one sensor for each OID you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

DELL HARDWARE SPECIFIC

Library OIDs	Select the performance counters you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items. Choose the counters that you want to monitor with caution! We recommend that you select only a few counters in this dialog. Use the search function in the table head to filter for specific counters. Selecting too many library OIDs might result in thousands of sensors or in an aborted sensor creation.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DELL HARDWARE SPECIFIC

Selected Interface	Shows the name of the interface (performance counter) that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Unit String	Define the unit of the numerical data that the sensor receives at the given OID. Please enter a string.
Multiplication	If you want to multiply the received data with a certain value, enter the multiplier here. Please enter an integer value.
Division	If you want to divide the received data by a certain value, enter the divisor here. Please enter an integer value.
If Value Changes	Define what this sensor will do when the sensor value changes. You can choose between: ▪ **Ignore changes (default)**: The sensor takes no action on change.

- **Trigger 'change' notification**: The sensor sends an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification 2791 whenever the sensor value changes.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply. If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply. If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: What do I need to monitor Dell servers?

- https://kb.paessler.com/en/topic/45333

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

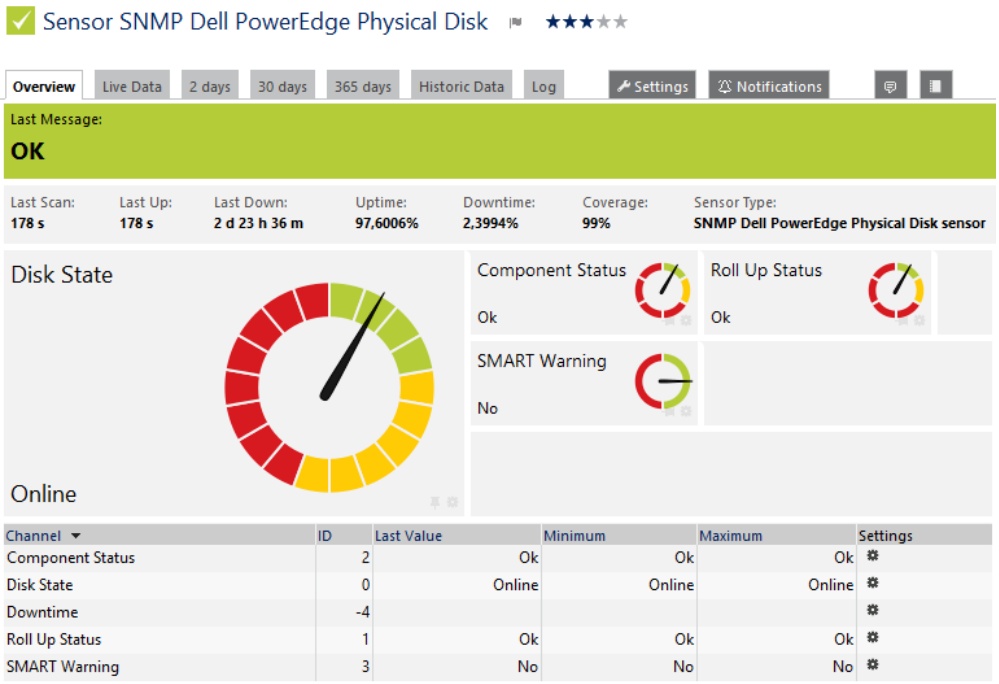
For more general information about settings, please see the **Object Settings** 188 section.

7.8.130 SNMP Dell PowerEdge Physical Disk Sensor

The SNMP Dell PowerEdge Physical Disk sensor monitors a physical disk in a Dell PowerEdge server using Simple Network Management Protocol (SNMP).

It can show the following:

- Disk status
- Roll up status
- Component status
- If there is currently a warning regarding the Self-Monitoring, Analysis and Reporting Technology (S.M.A.R.T.) status



SNMP Dell PowerEdge Physical Disk Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_dell_poweredge_physical_disk.png

Remarks

- Requires 1749 iDRAC 7 or the Dell OpenManage Server Administrator to be installed on the monitored server.
- Knowledge Base: What do I need to monitor Dell servers?
- Knowledge Base: I can't add Dell PowerEdge sensors to PRTG. What can I do?
- Knowledge Base: Why does my Dell PowerEdge System Health sensor show a power unit status error after iDRAC update?

- Knowledge Base: My Dell PowerEdge sensor fails to validate disks and I can't add it. What can I do?
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Requirement: Dell OpenManage Server Administrator or iDRAC 7

This sensor needs the Dell OpenManage Server Administrator tool to be installed on the Dell PowerEdge server to monitor it. Please make sure that you enable SNMP in the OpenManage Server Administrator. For details, please see section **More** below.

You can also monitor Dell PowerEdge servers with this sensor type via Integrated Dell Remote Access Controller (iDRAC) 7.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the disks you want to monitor. PRTG creates one sensor for each disk you select in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

DELL POWEREDGE PHYSICAL DISK SETTINGS

Disk	Select the disks you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DELL POWEREDGE PHYSICAL DISK SETTINGS

Disk	Shows the name of the disk that this sensor is monitoring. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Data Source	Shows the interface that is used to get monitoring data. This is either Dell OpenManage Server Administrator (OMSA) or Integrated Dell Remote Access Controller (iDRAC).

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: What do I need to monitor Dell servers?

- https://kb.paessler.com/en/topic/45333

Knowledge Base: I can't add Dell PowerEdge sensors to PRTG. What can I do?

- https://kb.paessler.com/en/topic/68040

Knowledge Base: My Dell PowerEdge sensor fails to validate disks and I can't add it. What can I do?

- https://kb.paessler.com/en/topic/61784

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

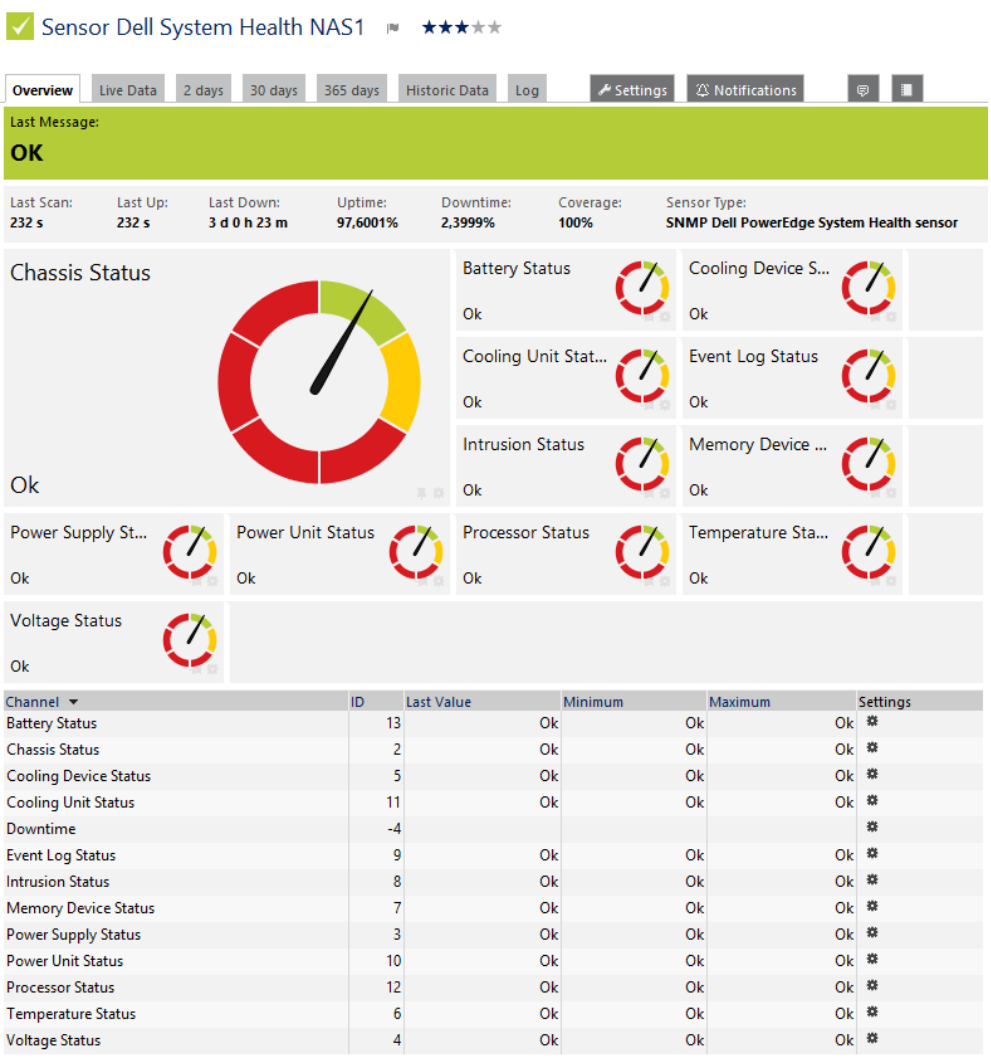
7.8.131 SNMP Dell PowerEdge System Health Sensor

The SNMP Dell PowerEdge System Health sensor monitors the system health of a Dell PowerEdge server using Simple Network Management Protocol (SNMP).

It can show the states of the following components, depending on their availability:

- Global system
- Power supply
- Temperature
- Cooling device
- Memory device
- Voltage

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Channel	ID	Last Value	Minimum	Maximum	Settings
Battery Status	13	Ok	Ok	Ok	
Chassis Status	2	Ok	Ok	Ok	
Cooling Device Status	5	Ok	Ok	Ok	
Cooling Unit Status	11	Ok	Ok	Ok	
Downtime	-4				
Event Log Status	9	Ok	Ok	Ok	
Intrusion Status	8	Ok	Ok	Ok	
Memory Device Status	7	Ok	Ok	Ok	
Power Supply Status	3	Ok	Ok	Ok	
Power Unit Status	10	Ok	Ok	Ok	
Processor Status	12	Ok	Ok	Ok	
Temperature Status	6	Ok	Ok	Ok	
Voltage Status	4	Ok	Ok	Ok	

SNMP Dell PowerEdge System Health Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_dell_poweredge_system_health.png

Remarks

- Requires 1749 iDRAC 7 or the Dell OpenManage Server Administrator to be installed on the monitored server.
- Knowledge Base: What do I need to monitor Dell servers?
- Knowledge Base: I can't add Dell PowerEdge sensors to PRTG. What can I do?
- Knowledge Base: Why does my Dell PowerEdge System Health sensor show a power unit status error after iDRAC update?
- This sensor type has predefined limits for several metrics. You can change these limits individually in the channel settings. For detailed information about channel limits, please refer to the manual section **Sensor Channels Settings** 2782.

- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Requirement: Dell OpenManage Server Administrator or iDRAC 7

This sensor needs the Dell OpenManage Server Administrator tool to be installed on the Dell PowerEdge server to monitor it. Please make sure that you enable SNMP in the OpenManage Server Administrator. For details, please see section **More** below.

You can also monitor Dell PowerEdge servers with this sensor type via Integrated Dell Remote Access Controller (iDRAC) 7.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the Dell PowerEdge chassis you want to monitor. PRTG creates one sensor for each chassis you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

DELL POWEREDGE SYSTEM HEALTH SPECIFIC

Chassis	Select the chassis you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DELL POWEREDGE SYSTEM HEALTH SPECIFIC

Chassis	Shows the chassis that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Channel Mask	Shows the channel mask that describes which sensors are available. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Data Source	Shows the interface that is used to get monitoring data. This is either Dell OpenManage Server Administrator (OMSA) or Integrated Dell Remote Access Controller (iDRAC).

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: What do I need to monitor Dell servers?

- https://kb.paessler.com/en/topic/45333

Knowledge Base: I can't add Dell PowerEdge sensors to PRTG. What can I do?

- https://kb.paessler.com/en/topic/68040

Knowledge Base: Why does my Dell PowerEdge System Health sensor show a power unit status error after iDRAC update?

- https://kb.paessler.com/en/topic/72855

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

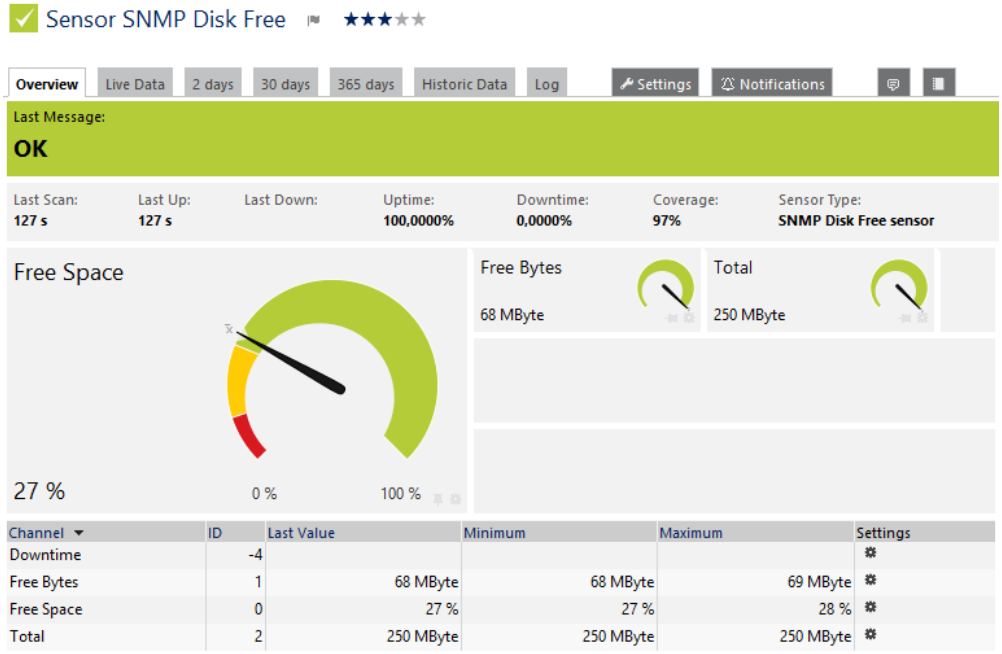
For more general information about settings, please see the **Object Settings** 188 section.

7.8.132 SNMP Disk Free Sensor

The SNMP Disk Free sensor monitors the free disk space on a logical disk via Simple Network Management Protocol (SNMP).

It can show the following:

- Free disk space in percent
- Free disk space in bytes
- Total disk space



SNMP Disk Free Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_disk_free.png

Remarks

- This sensor uses more generic Object Identifier (OID) values compared to the **SNMP Linux Disk Free Sensor** 1924.
- It might not work to query data from a probe device via SNMP (querying localhost, 127.0.0.1, or ::1). Add this device to PRTG 275 with the IP address that it has in your network and create the SNMP sensor on this device instead.
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the disk(s) you want to monitor. PRTG creates one sensor for each disk you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

DISK FREE SETTINGS

Disk	Select one or more disks you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	Enter one or more **Tags**, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DISK FREE SETTINGS

Disk	Shows the name of the disk that this sensor is monitoring. This value is shown for reference purposes only. We strongly recommend that you only change it if Paessler support explicitly asks you to do so. Wrong usage can result in incorrect monitoring data!

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. ⓘ You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel.

SENSOR DISPLAY

	▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. ⓘ This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.

SCANNING INTERVAL

- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

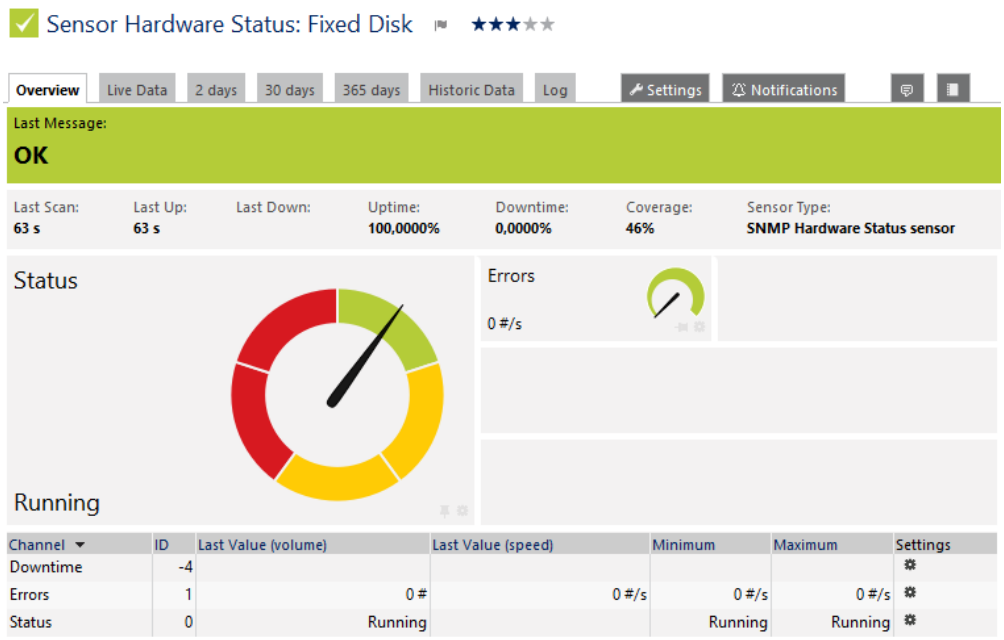
For more general information about settings, please see the **Object Settings** 188 section.

7.8.133 SNMP Hardware Status Sensor

The SNMP Hardware Status sensor monitors the status of a hardware component of a server via Simple Network Management Protocol (SNMP).

It shows the following:

- Current status of the monitored hardware component
- Number of errors per time period



SNMP Hardware Status Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_hardware_status.png

Remarks

- It might not work to query data from a probe device via SNMP (querying localhost, 127.0.0.1, or ::1). Add this device to PRTG 275 with the IP address that it has in your network and create the SNMP sensor on this device instead.
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the hardware components you want to monitor. PRTG creates one sensor for each component you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

HARDWARE SPECIFIC

Hardware Component	Select the hardware components you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	Enter one or more **Tags**, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

HARDWARE SPECIFIC

Hardware Component	
Product ID	Shows further information about the hardware component. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Description	
Type	

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.

SCANNING INTERVAL

- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. ⓘ To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

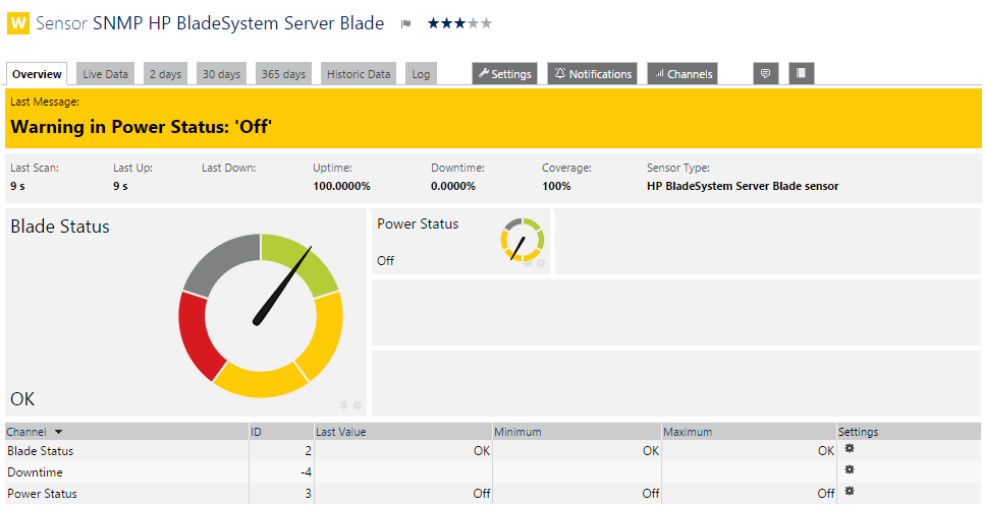
Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.134 SNMP HP BladeSystem Blade Sensor

The SNMP HP BladeSystem Blade Sensor monitors the status of an HP BladeSystem via Simple Network Management Protocol (SNMP). It can show the following:

- Blade status (OK, degraded, unknown, failed, other)
- Power status (OK, on, off, power stagged off, unknown, other)



HP BladeSystem Server Blade Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/hp_bladesystem_server_blade.png

Remarks

- Make sure you add this sensor to a device whose IP/DNS name points to the HP BladeSystem Enclosure hosting the Onboard Administrator!
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the server blades you want to monitor. PRTG creates one sensor for each blade you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

HP BLADESYSTEM SPECIFIC

Server Blade	Select the blades you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.

BASIC SENSOR SETTINGS

Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

HP BLADESYSTEM SPECIFIC

Server Blade	Shows the server blade that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. ⓘ Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

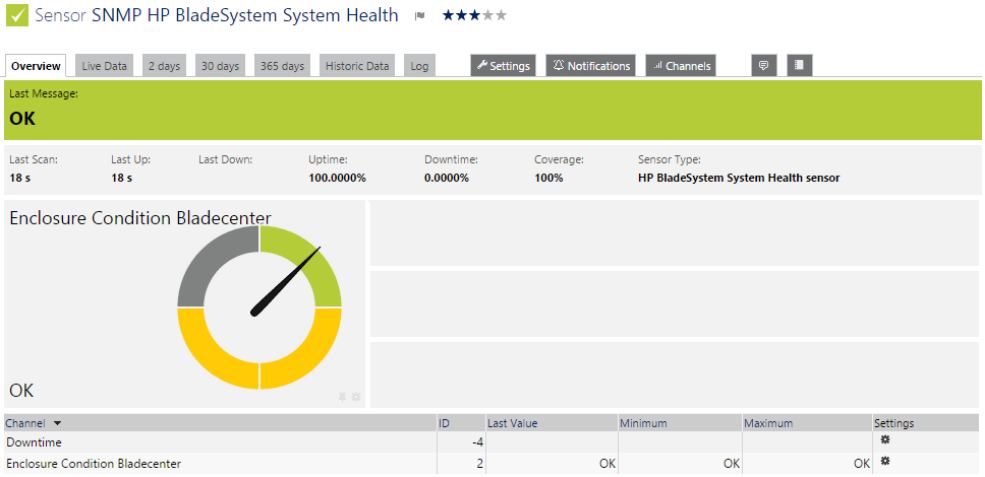
Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.135 SNMP HP BladeSystem Enclosure System Health Sensor

The SNMP HP BladeSystem Enclosure System Health sensors monitors the system health of an HP BladeSystem device via Simple Network Management Protocol (SNMP). It can show the following:

- Enclosure condition of the BladeCenter (OK, degraded, failed, unknown, other)



HP BladeSystem System Health Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/hp_bladesystem_system_health.png

Remarks

- Make sure you add this sensor to a device whose IP/DNS name points to the HP BladeSystem Enclosure hosting the Onboard Administrator!
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.

SCANNING INTERVAL

- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

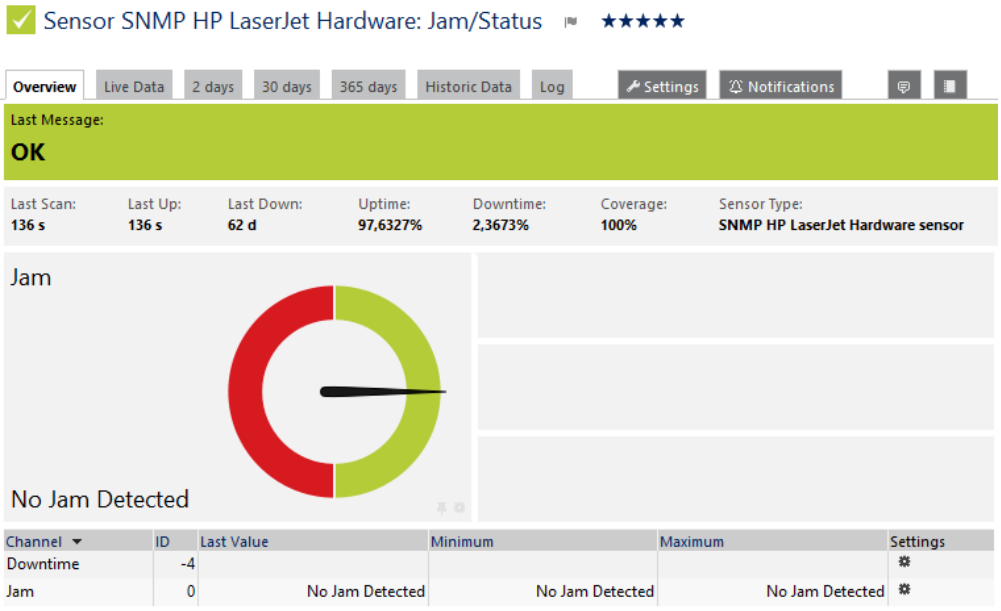
For more general information about settings, please see the **Object Settings** 188 section.

7.8.136 SNMP HP LaserJet Hardware Sensor

The SNMP HP LaserJet Hardware sensor monitors performance counters on a HP LaserJet hardware device using Simple Network Management Protocol (SNMP).

It can show the following, depending on what category you monitor:

- Status of toner
- Status of paper
- Paper jam status



SNMP HP LaserJet Hardware Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_hp_laserjet_hardware.png

Remarks

- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the categories you want to monitor. PRTG creates one sensor for each category you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

DELL HARDWARE SPECIFIC

Library OIDs	Select the categories you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items. The following performance counters for your printer are available: ▪ **Toner/Status** ▪ **Paper/Status** ▪ **Jam/Status**

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	Enter one or more **Tags**[124], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited[124] from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

HP LASERJET SPECIFIC

Selected Interface	Shows the name of the category (performance counter) that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
If Value Changes	Define what this sensor will do when the sensor value changes. You can choose between: ▪ **Ignore changes (default)**: The sensor takes no action on change. ▪ **Trigger 'change' notification**: The sensor sends an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification[2791] whenever the sensor value changes.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. ⓘ You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

SENSOR DISPLAY

Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

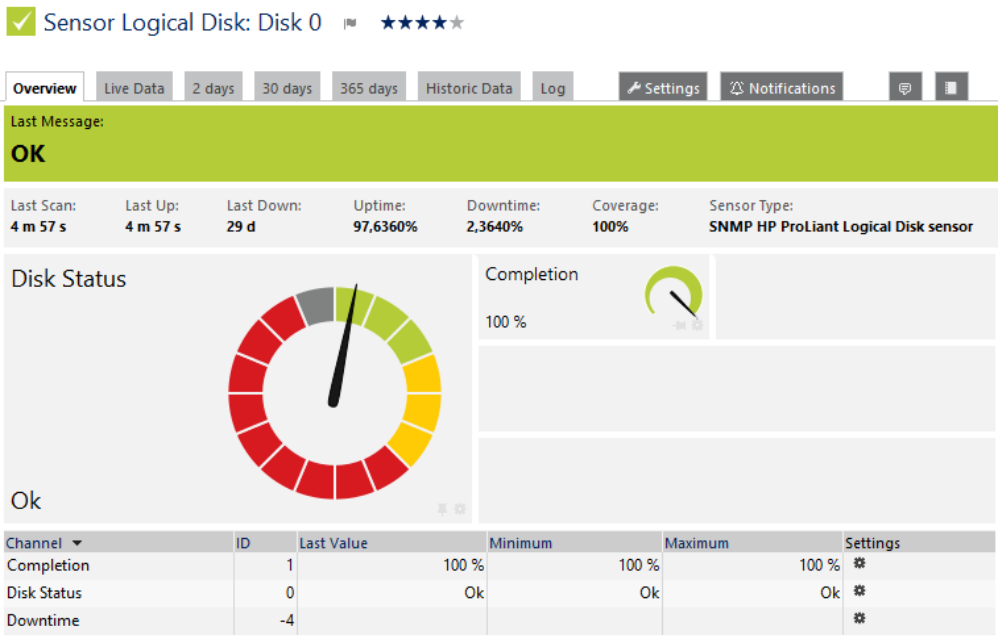
For more general information about settings, please see the **Object Settings** 188 section.

7.8.137 SNMP HP ProLiant Logical Disk Sensor

The SNMP HP ProLiant Logical Disk sensor monitors a logical disk in an HP server via Simple Network Management Protocol (SNMP).

It can show the following:

- Disk status
- Completion in percent: This is only important when the disk status is "Reconstructing" or "Expanding" and illustrates the progress of this task.



SNMP HP ProLiant Logical Disk Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_hp_proliant_logical_disk.png

Remarks

- Requires 1801 HP Insight Management Agents and HP Insight Management WBEM Providers to be installed on the target device.
- Knowledge Base: Monitor HP ProLiant via SNMP?
- If the sensor shows a "cannot find such device types" error message, use an HP iLO interface 1801 as parent device for this sensor (if available).
- This sensor type supports monitoring HP Integrated Lights-Out (iLO) as of iLO version 3. We recommend that you use **iLO 4** because this version applies its own dedicated SNMP counters while iLO 3 only forwards SNMP counters from the particular operating system.
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.

- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Requirement: HP System Management Tools

This sensor needs a specific HP system management tool to be installed on the target device, so it reports data via SNMP: HP Insight Management Agents for Windows Server 2003/2008. To receive SNMP data from RAID controllers, you additionally need HP Insight Management WBEM Providers. For more details and download links please refer to the subsection **More** below.

Some of the HP Object Identifiers (OIDs) that this sensor type uses are only accessible via the HP Integrated Lights-Out (iLO) interface. If this sensor throws an error that it cannot find "such device types", please create a device in PRTG that points to the address of the HP iLO interface (if available) and add the sensor to this device. We recommend that you use the Agentless Management feature with configured SNMP. You can set this up in the iLO configuration interface under **Administration | Management | SNMP Settings**.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the disks in the HP server you want to monitor. PRTG creates one sensor for each disk you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

HP PROLIANT LOGICAL DISK SETTINGS

Disk	Select the disks you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

HP PROLIANT LOGICAL DISK SETTINGS

Disk	Shows the name of the disk that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

SENSOR DISPLAY

	You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

SCANNING INTERVAL

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: Monitor HP ProLiant via SNMP

- https://kb.paessler.com/en/topic/33133

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

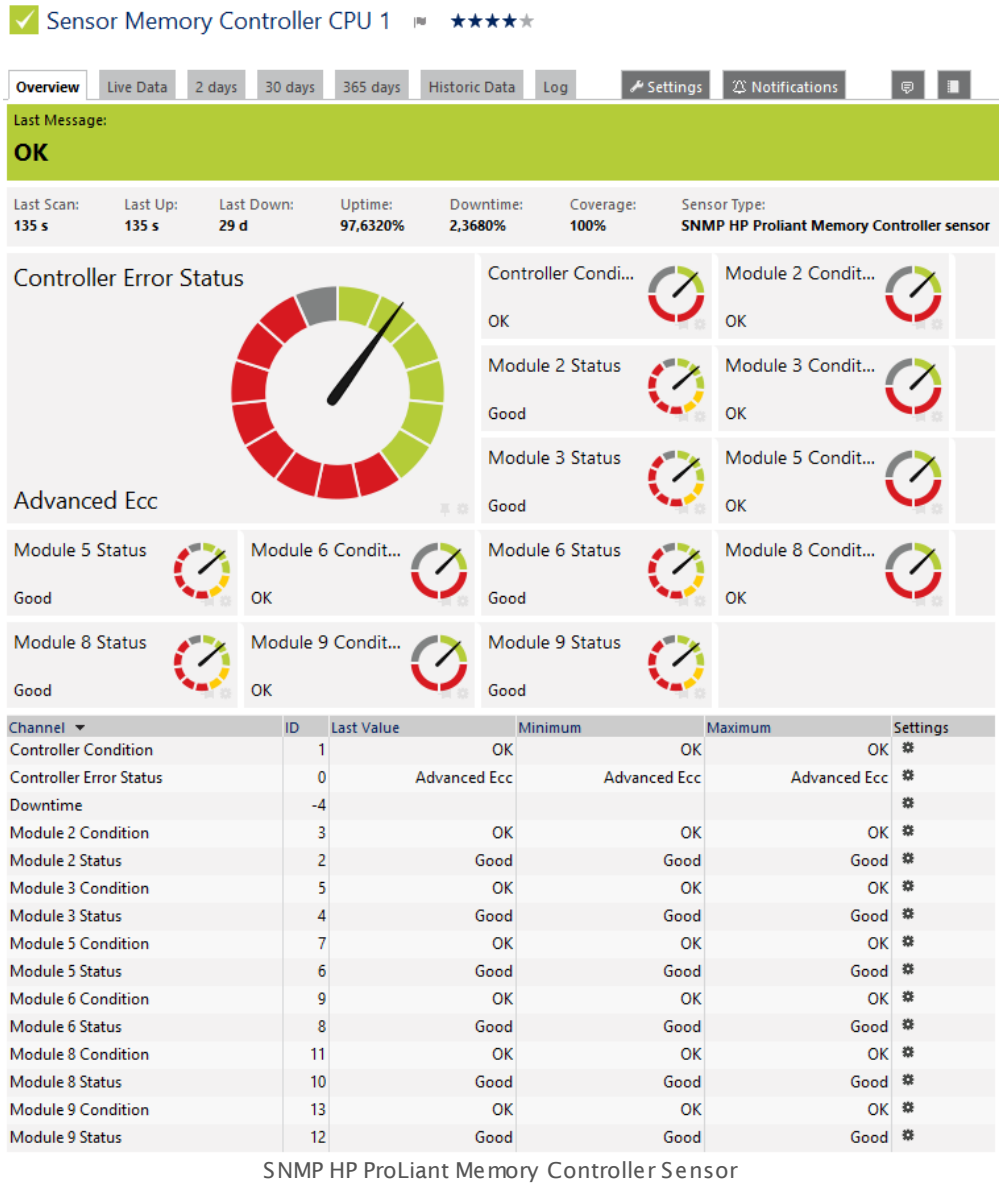
For more general information about settings, please see the **Object Settings** 188 section.

7.8.138 SNMP HP ProLiant Memory Controller Sensor

The SNMP HP ProLiant Memory Controller sensor monitors a memory controller in an HP server via Simple Network Management Protocol (SNMP).

It shows the following:

- Error status of the controller
- Condition of the controller
- States and conditions of available modules.



Channel	ID	Last Value	Minimum	Maximum	Settings
Controller Condition	1	OK	OK	OK	
Controller Error Status	0	Advanced Ecc	Advanced Ecc	Advanced Ecc	
Downtime	-4				
Module 2 Condition	3	OK	OK	OK	
Module 2 Status	2	Good	Good	Good	
Module 3 Condition	5	OK	OK	OK	
Module 3 Status	4	Good	Good	Good	
Module 5 Condition	7	OK	OK	OK	
Module 5 Status	6	Good	Good	Good	
Module 6 Condition	9	OK	OK	OK	
Module 6 Status	8	Good	Good	Good	
Module 8 Condition	11	OK	OK	OK	
Module 8 Status	10	Good	Good	Good	
Module 9 Condition	13	OK	OK	OK	
Module 9 Status	12	Good	Good	Good	

SNMP HP ProLiant Memory Controller Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_hp_proliant_memory_controller.png

Remarks

- Requires 1810 HP Insight Management Agents and HP Insight Management WBEM Providers to be installed on the target device.
- Knowledge Base: Which lookup values are supported by the SNMP HP ProLiant Memory Controller Sensor?
- Knowledge Base: Monitor HP ProLiant via SNMP?
- If modules are inserted at a later point, you have to add this sensor anew.
- If the sensor shows a "cannot find such device types" error message, use an HP iLO interface 1801 as parent device for this sensor (if available).
- This sensor type supports monitoring HP Integrated Lights-Out (iLO) as of iLO version 3. We recommend that you use **iLO 4** because this version applies its own dedicated SNMP counters while iLO 3 only forwards SNMP counters from the particular operating system.
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Requirement: HP System Management Tools

This sensor needs a specific HP system management tool to be installed on the target device, so it reports data via SNMP: HP Insight Management Agents for Windows Server 2003/2008. To receive SNMP data from RAID controllers, you additionally need HP Insight Management WBEM Providers. For more details and download links please refer to the subsection **More** below.

Some of the HP Object Identifiers (OIDs) that this sensor type uses are only accessible via the HP Integrated Lights-Out (iLO) interface. If this sensor throws an error that it cannot find "such device types", please create a device in PRTG that points to the address of the HP iLO interface (if available) and add the sensor to this device. We recommend that you use the Agentless Management feature with configured SNMP. You can set this up in the iLO configuration interface under **Administration | Management | SNMP Settings**.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the memory controllers in the HP server you want to monitor. PRTG creates one sensor for each controller you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

HP PROLIANT MEMORY CONTROLLER SETTINGS

Controller	Select the controllers you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

HP PROLIANT MEMORY CONTROLLER SETTINGS

Controller	Shows the name of the controller that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply. If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply. If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: Monitor HP ProLiant via SNMP

- https://kb.paessler.com/en/topic/33133

Knowledge Base: Which lookup values are supported by the SNMP HP ProLiant Memory Controller Sensor?

- https://kb.paessler.com/en/topic/44803

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.139 SNMP HP ProLiant Network Interface Sensor

The SNMP HP ProLiant Network Interface sensor monitors a network interface in an HP server via Simple Network Management Protocol (SNMP).

It can show the following:

- Traffic in
- Traffic out
- Number of transmitted and received good frames
- Number of transmitted and received bad frames
- Alignment errors
- FCS (Frame Check Sequence) errors
- Late and excessive collisions
- Carrier sense errors
- If frames are too long

Remarks

- Requires 1818 HP Insight Management Agents and HP Insight Management WBEM Providers to be installed on the target device.
- When adding the sensor, the status of each available network interface is shown. If this status is **Link Failure**, it is still possible to add a sensor for the respective interface. Though, most likely the sensor for this interface will not work correctly. The error message in this case will be "No Such Name (SNMP error # 2)".
- Knowledge Base: Monitor HP ProLiant via SNMP?
- If the sensor shows a "cannot find such device types" error message, use an HP iLO interface 1819 as parent device for this sensor (if available).
- This sensor type supports monitoring HP Integrated Lights-Out (iLO) as of iLO version 3. We recommend that you use **iLO 4** because this version applies its own dedicated SNMP counters while iLO 3 only forwards SNMP counters from the particular operating system.
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Requirement: HP System Management Tools

This sensor needs a specific HP system management tool to be installed on the target device, so it reports data via SNMP: HP Insight Management Agents for Windows Server 2003/2008. To receive SNMP data from RAID controllers, you additionally need HP Insight Management WBEM Providers. For more details and download links please refer to the subsection **More** below.

Some of the HP Object Identifiers (OIDs) that this sensor type uses are only accessible via the HP Integrated Lights-Out (iLO) interface. If this sensor throws an error that it cannot find "such device types", please create a device in PRTG that points to the address of the HP iLO interface (if available) and add the sensor to this device. We recommend that you use the Agentless Management feature with configured SNMP. You can set this up in the iLO configuration interface under **Administration | Management | SNMP Settings**.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the network interfaces in the HP server you want to monitor. PRTG creates one sensor for each interface you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

HP PROLIANT NETWORK INTERFACE SETTINGS

Network Interface	Select the interfaces you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items. If this status is **Link Failure**, it is still possible to add a sensor for the respective interface. Though, most likely the sensor for this interface will not work correctly. The error message in this case will be "No Such Name (SNMP error # 2)".

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

HP PROLIANT NETWORK INTERFACE SETTINGS

Network Interface	Shows the name of the interface that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. ⓘ You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how to show different channels for this sensor.

SENSOR DISPLAY

- **Show channels independently (default)**: Show an own graph for each channel.
- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic.
  You cannot use this option in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782). Manual scaling is not possible if you choose this option.
- **Show in and out traffic as positive and negative area chart**: Show channels for incoming and outgoing traffic as positive and negative area chart. This will visualize your traffic in a clear way.

  You cannot use this option in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782). Manual scaling is not possible if you choose this option.

  You cannot show a positive/negative chart for a channel if you choose to display its data in percent of maximum (available in the **Sensor Channels Settings** 2782).

Stack Unit	This setting is only available if you choose **Stack channels on top of each other** above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: Monitor HP ProLiant via SNMP

- https://kb.paessler.com/en/topic/33133

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.140 SNMP HP ProLiant Physical Disk Sensor

The SNMP HP ProLiant Physical Disk sensor monitors a physical disk in an HP server via Simple Network Management Protocol (SNMP).

It can show the following:

- Read and written sectors
- Hard and corrected read errors
- Hard and corrected write errors
- Disk status
- Drive condition
- Self-Monitoring, Analysis and Reporting Technology (S.M.A.R.T.) status
- If the threshold is passed

SNMP HP ProLiant Physical Disk Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_hp_proliant_physical_disk.png

Remarks

- Requires 1828 HP Insight Management Agents and HP Insight Management WBEM Providers to be installed on the target device.
- Knowledge Base: Monitor HP ProLiant via SNMP?
- If the sensor shows a "cannot find such device types" error message, use an HP iLO interface 1828 as parent device for this sensor (if available).
- This sensor type supports monitoring HP Integrated Lights-Out (iLO) as of iLO version 3. We recommend that you use **iLO 4** because this version applies its own dedicated SNMP counters while iLO 3 only forwards SNMP counters from the particular operating system.
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Requirement: HP System Management Tools

This sensor needs a specific HP system management tool to be installed on the target device, so it reports data via SNMP: HP Insight Management Agents for Windows Server 2003/2008. To receive SNMP data from RAID controllers, you additionally need HP Insight Management WBEM Providers. For more details and download links please refer to the subsection **More** below.

Some of the HP Object Identifiers (OIDs) that this sensor type uses are only accessible via the HP Integrated Lights-Out (iLO) interface. If this sensor throws an error that it cannot find "such device types", please create a device in PRTG that points to the address of the HP iLO interface (if available) and add the sensor to this device. We recommend that you use the Agentless Management feature with configured SNMP. You can set this up in the iLO configuration interface under **Administration | Management | SNMP Settings**.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the physical disks in the HP server you want to monitor. PRTG creates one sensor for each disk you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

HP PROLIANT PHYSICAL DISK SETTINGS

Disk	Select the disks you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

HP PROLIANT PHYSICAL DISK SETTINGS

Disk	Shows the identifier of the disk that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply. If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply. If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: Monitor HP ProLiant via SNMP

- https://kb.paessler.com/en/topic/33133

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

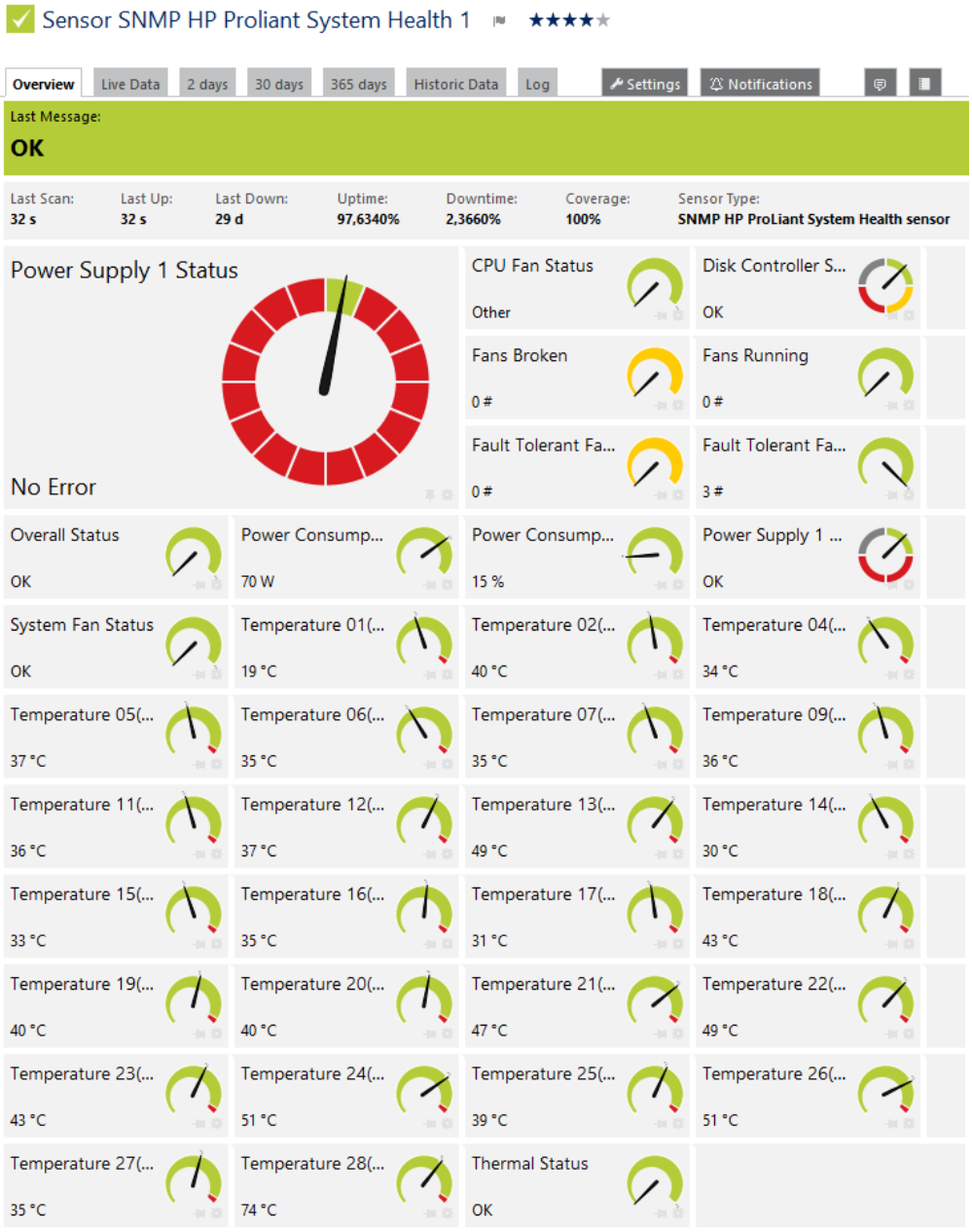
7.8.141 SNMP HP ProLiant System Health Sensor

The SNMP HP ProLiant System Health sensor monitors the system health of an HP ProLiant server via Simple Network Management Protocol (SNMP).

It can show the following:

- Overall status
- Thermal status
- System fan status
- CPU fan status
- Number of broken and running fans
- Number of broken and running fans that are fault tolerant
- Status and condition of the power supply
- Temperatures for various components of the server, for example, memory, power supply, CPU, system, and storage.
- Power consumption
- Disk controller status
- Integrated Management Log (IML) status: OK, Degraded, Failed, Other. This channel can help to determine the reason for a **Down** status of the sensor.

These channels are created at run-time, depending on the available measurement components. Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



SNMP HP ProLiant System Health Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_hp_proliant_system_health.png

Remarks

- Requires 1838 HP Insight Management Agents and HP Insight Management WBEM Providers to be installed on the target device.
- Knowledge Base: Monitor HP ProLiant via SNMP?
- This sensor has predefined limits for temperatures and broken frames. You can change these limits individually in the channel settings 2782.

- RAID controllers that have no hard disks assigned might cause a **Down** status 163. In this case, deactivate the respective controller(s) in the HP ProLiant BIOS to avoid sensor errors.
- If the sensor shows a "cannot find such device types" error message, use an HP iLO interface 1838 as parent device for this sensor (if available).
- This sensor type supports monitoring HP Integrated Lights-Out (iLO) as of iLO version 3. We recommend that you use **iLO 4** because this version applies its own dedicated SNMP counters while iLO 3 only forwards SNMP counters from the particular operating system.
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Requirement: HP System Management Tools

This sensor needs a specific HP system management tool to be installed on the target device, so it reports data via SNMP: HP Insight Management Agents for Windows Server 2003/2008. To receive SNMP data from RAID controllers, you additionally need HP Insight Management WBEM Providers. For more details and download links please refer to the subsection **More** below.

Some of the HP Object Identifiers (OIDs) that this sensor type uses are only accessible via the HP Integrated Lights-Out (iLO) interface. If this sensor throws an error that it cannot find "such device types", please create a device in PRTG that points to the address of the HP iLO interface (if available) and add the sensor to this device. We recommend that you use the Agentless Management feature with configured SNMP. You can set this up in the iLO configuration interface under **Administration | Management | SNMP Settings**.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. ⓘ You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. ⓘ This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

SENSOR DISPLAY

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.

SCANNING INTERVAL

- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.
	Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:
	▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** Custom channel types can be set on sensor level only.

More

Knowledge Base: Monitor HP ProLiant via SNMP

- https://kb.paessler.com/en/topic/33133

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Knowledge Base: Why is my SNMP HP ProLiant System Health sensor in error status after updating PRTG?

- https://kb.paessler.com/en/topic/61805

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

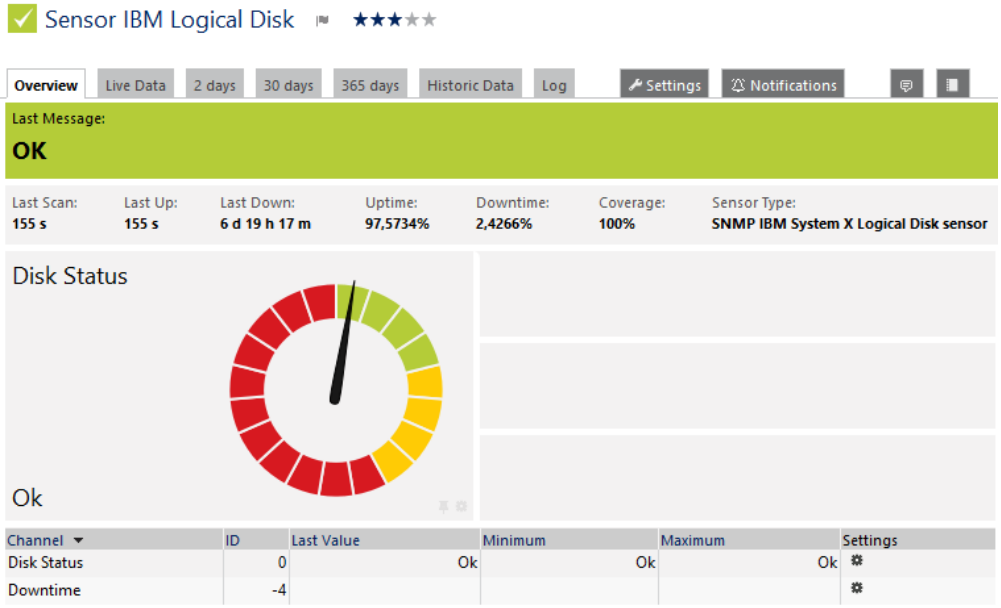
Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.142 SNMP IBM System X Logical Disk Sensor

The SNMP IBM System X Logical Disk sensor monitors a logical disk in an IBM server via Simple Network Management Protocol (SNMP).

- It shows the status of a logical disk in an IBM server.



SNMP IBM System X Logical Disk Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_ibm_systemx_logical_disk.png

Remarks

- Requires 1845 the IBM Systems Director Platform to be installed on the target device.
- Knowledge Base: What are the requirements to monitor IBM System x?
- Knowledge Base: IBM System X sensors could not find any disk/data on this device (PE187/PE188/PE194)
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Requirement: IBM Systems Director Platform Agent

This sensor type needs the IBM Systems Director Platform Agent to be installed on the target IBM device in order to monitor it through SNMP. For more information, please see section **More** below.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the logical disks of the IBM device you want to monitor. PRTG creates one sensor for each disk you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

IBM SYSTEM X LOGICAL DISK SETTINGS

Disk	Select the logical disks you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	Enter one or more **Tags**, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

IBM SYSTEM X LOGICAL DISK SETTINGS

Disk	Shows the ID of the logical disk that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. ⓘ You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.

SCANNING INTERVAL

- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: What are the requirements to monitor IBM System x?

- https://kb.paessler.com/en/topic/59393

Knowledge Base: IBM System X sensors could not find any disk/data on this device (PE187/ PE188/PE194)

- https://kb.paessler.com/en/topic/73914

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

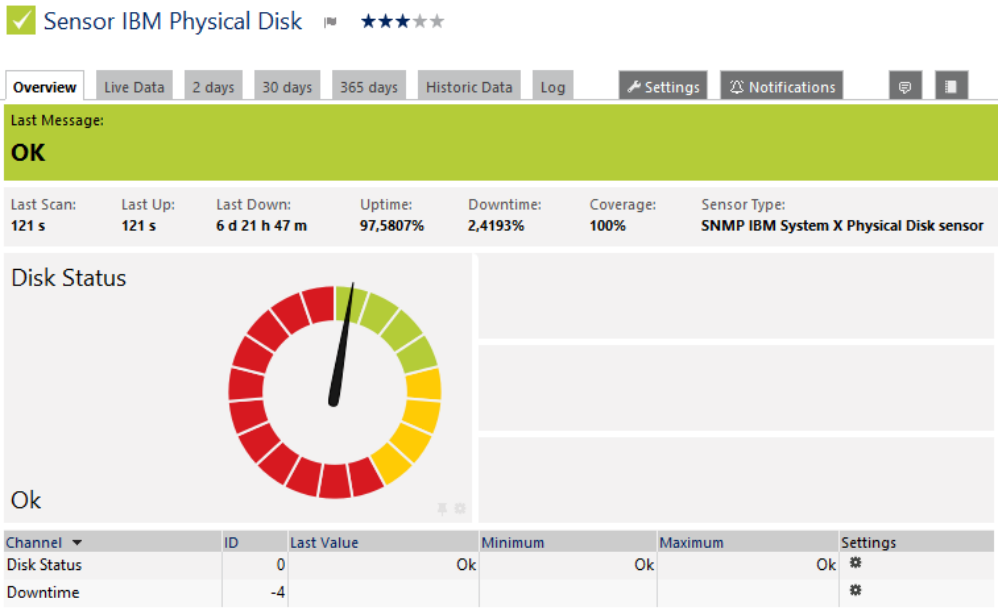
Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.143 SNMP IBM System X Physical Disk Sensor

The SNMP IBM System X Physical Disk sensor monitors a physical disk in an IBM server via Simple Network Management Protocol (SNMP).

- It shows the status of a physical disk.



SNMP IBM System X Physical Disk Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_ibm_systemx_physical_disk.png

Remarks

- Requires 1854 the IBM Systems Director Platform to be installed on the target device.
- Knowledge Base: What are the requirements to monitor IBM System x?
- Knowledge Base: IBM System X sensors could not find any disk/data on this device (PE187/PE188/PE194)
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Requirement: IBM Systems Director Platform Agent

This sensor type needs the IBM Systems Director Platform Agent to be installed on the target IBM device in order to monitor it through SNMP. For more information, please see section **More** below.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the physical disks of the IBM device you want to monitor. PRTG creates one sensor for each disk you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

IBM SYSTEM X PHYSICAL DISK SETTINGS

Disk	Select the physical disks you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	Enter one or more **Tags**, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

IBM SYSTEM X PHYSICAL DISK SETTINGS

Disk	Shows the ID of the physical disk that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. ⓘ You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.

SCANNING INTERVAL

- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: What are the requirements to monitor IBM System x?

- https://kb.paessler.com/en/topic/59393

Knowledge Base: IBM System X sensors could not find any disk/data on this device (PE187/PE188/PE194)

- https://kb.paessler.com/en/topic/73914

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

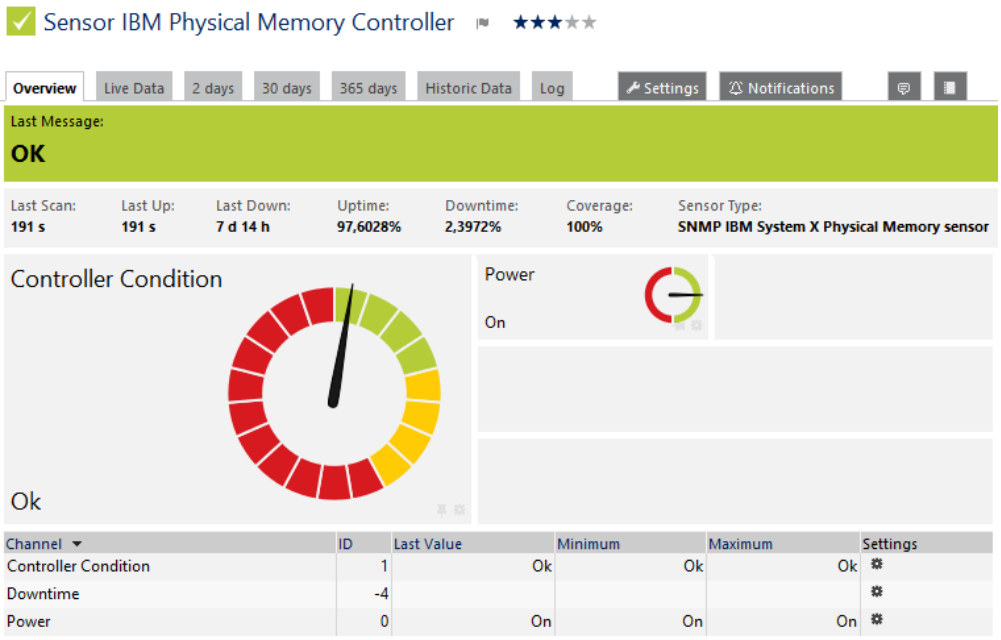
For more general information about settings, please see the **Object Settings** 188 section.

7.8.144 SNMP IBM System X Physical Memory Sensor

The SNMP IBM System X Physical Memory sensor monitors the memory modules in an IBM server via Simple Network Management Protocol (SNMP).

It shows the following:

- Condition of memory controller
- Power status (on or off)



SNMP IBM System X Physical Memory Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_ibm_systemx_physical_memory.png

Remarks

- Requires 1864 the IBM Systems Director Platform to be installed on the target device.
- Knowledge Base: What are the requirements to monitor IBM System x?
- Knowledge Base: IBM System X sensors could not find any disk/data on this device (PE187/PE188/PE194)
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Requirement: IBM Systems Director Platform Agent

This sensor type needs the IBM Systems Director Platform Agent to be installed on the target IBM device in order to monitor it through SNMP. For more information, please see section **More** below.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the memory modules of the IBM server you want to monitor. PRTG creates one sensor for each module you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

IBM SYSTEM X PHYSICAL MEMORY SETTINGS

Module	Select the memory modules you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

IBM SYSTEM X PHYSICAL MEMORY SETTINGS

Name	
Caption	Shows further information about the module. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Serial Number	
Size	

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

SENSOR DISPLAY

	You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

SCANNING INTERVAL

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: What are the requirements to monitor IBM System x?

- https://kb.paessler.com/en/topic/59393

Knowledge Base: IBM System X sensors could not find any disk/data on this device (PE187/ PE188/PE194)

- https://kb.paessler.com/en/topic/73914

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

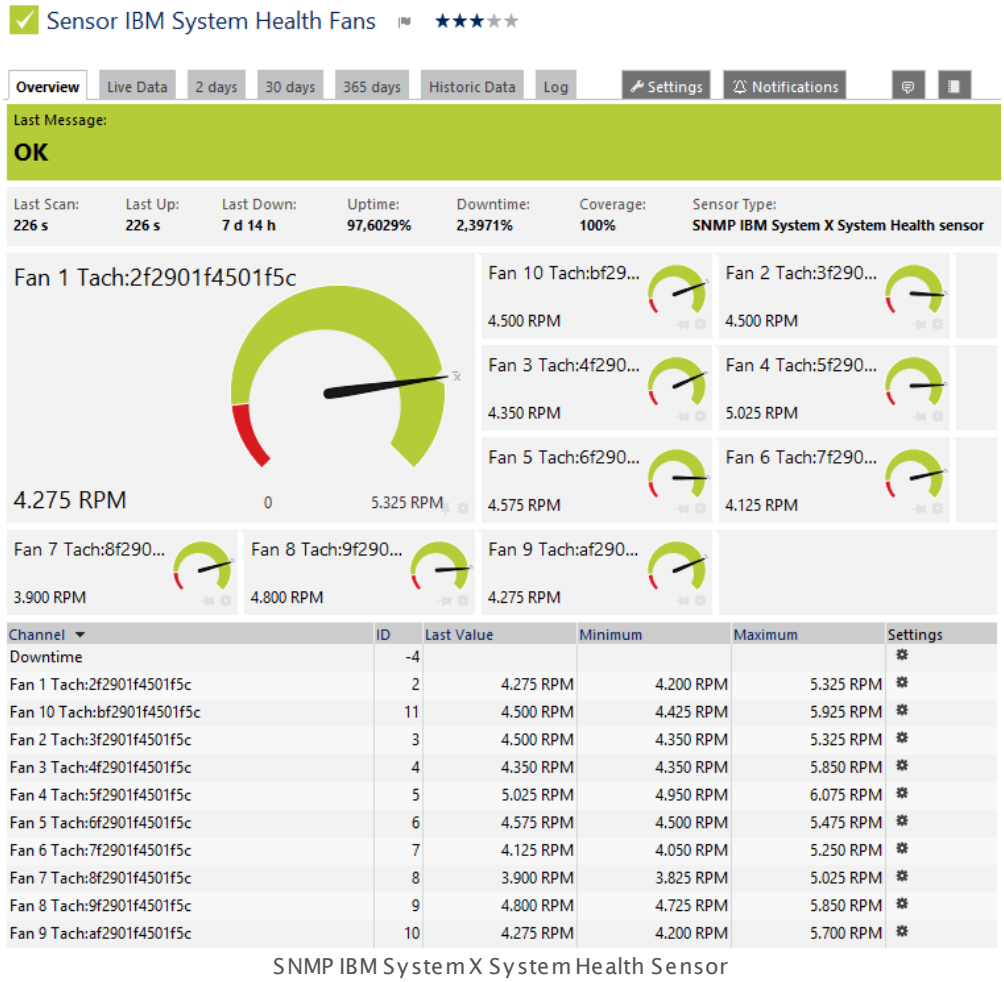
7.8.145 SNMP IBM System X System Health Sensor

The SNMP IBM System X System Health sensor monitors the system health of an IBM device via Simple Network Management Protocol (SNMP).

It can show the following, depending on what measurement you select:

- Revolutions per minute of fans (or the current percentage of the possible maximum)
- Temperature of ambient and CPUs
- Voltage of planars
- Status of power supplies

These channels are created at run-time, depending on the available measurement components. Which channels the sensor actually shows might depend on the monitored device and the sensor setup..



Channel	ID	Last Value	Minimum	Maximum	Settings
Downtime	-4				
Fan 1 Tach:2f2901f4501f5c	2	4.275 RPM	4.200 RPM	5.325 RPM	
Fan 10 Tach:bf2901f4501f5c	11	4.500 RPM	4.425 RPM	5.925 RPM	
Fan 2 Tach:3f2901f4501f5c	3	4.500 RPM	4.350 RPM	5.325 RPM	
Fan 3 Tach:4f2901f4501f5c	4	4.350 RPM	4.350 RPM	5.850 RPM	
Fan 4 Tach:5f2901f4501f5c	5	5.025 RPM	4.950 RPM	6.075 RPM	
Fan 5 Tach:6f2901f4501f5c	6	4.575 RPM	4.500 RPM	5.475 RPM	
Fan 6 Tach:7f2901f4501f5c	7	4.125 RPM	4.050 RPM	5.250 RPM	
Fan 7 Tach:8f2901f4501f5c	8	3.900 RPM	3.825 RPM	5.025 RPM	
Fan 8 Tach:9f2901f4501f5c	9	4.800 RPM	4.725 RPM	5.850 RPM	
Fan 9 Tach:af2901f4501f5c	10	4.275 RPM	4.200 RPM	5.700 RPM	

SNMP IBM System X System Health Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_ibm_systemx_system_health.png

Remarks

- Requires 1873 the IBM Systems Director Platform to be installed on the target device.
- This sensor can also run directly on an Integrated Management Module (IMM) network port and can show the overall health on IMMs.
- If the IBM device returns a string in an unexpected format for the percentage of fan revolutions (for example, "offline"), this sensor will show **-1%** in the corresponding channel. You can define a **Down** status 163 for this via channel limits 2783.
- Knowledge Base: What are the requirements to monitor IBM System x?
- Knowledge Base: IBM System X sensors could not find any disk/data on this device (PE187/PE188/PE194)
- This sensor type has predefined limits for several metrics. You can change these limits individually in the channel settings. For detailed information about channel limits, please refer to the manual section **Sensor Channels Settings** 2782.
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Requirement: IBM Systems Director Platform Agent

This sensor type needs the IBM Systems Director Platform Agent to be installed on the target IBM device in order to monitor it through SNMP. For more information, please see section **More** below.

The SNMP IBM System X System Health sensor can also run directly on an Integrated Management Module (IMM) network port and can show the overall health on IMMs.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the measurements of the IBM device you want to monitor. PRTG creates one sensor for each measurement you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

IBM SYSTEM X SYSTEM HEALTH SPECIFIC

Measurement	Select the measurements you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

IBM SYSTEM X SYSTEM HEALTH SPECIFIC

Source	Shows the source of the measurement that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Measurement	Shows the measurement that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. ⓘ You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. ⓘ This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: What are the requirements to monitor IBM System x?

- https://kb.paessler.com/en/topic/59393

Knowledge Base: IBM System X sensors could not find any disk/data on this device (PE187/ PE188/PE194)

- https://kb.paessler.com/en/topic/73914

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.146 SNMP interSeptor Pro Environment Sensor

The SNMP interSeptor Pro Environment sensor queries data from a Jacarta interSeptor Pro environmental monitoring system via Simple Network Management Protocol (SNMP).

It can shows the following as measured by the Jacarta interSeptor Pro device:

- Temperature
- Humidity

Remarks

- To monitor data of an interSeptor Pro device with this sensor, you have to add the IP address of your PRTG installation to **Access Control** in the interSeptor Pro control panel. Open the interSeptor Pro web interface, select **InterSeptor Pro Menu | System Configuration | Access Control**, and allow access for PRTG's IP address.
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the measuring points of interSeptor Pro device you want to monitor. PRTG creates one sensor for each measuring point you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

INTERSEPTOR ENVIRONMENT SPECIFIC

Measuring Point	Select the measuring points you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

INTERSEPTOR ENVIRONMENT SPECIFIC

Name	Shows information about the measurement which this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Measuring Point	Shows the measuring point which this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

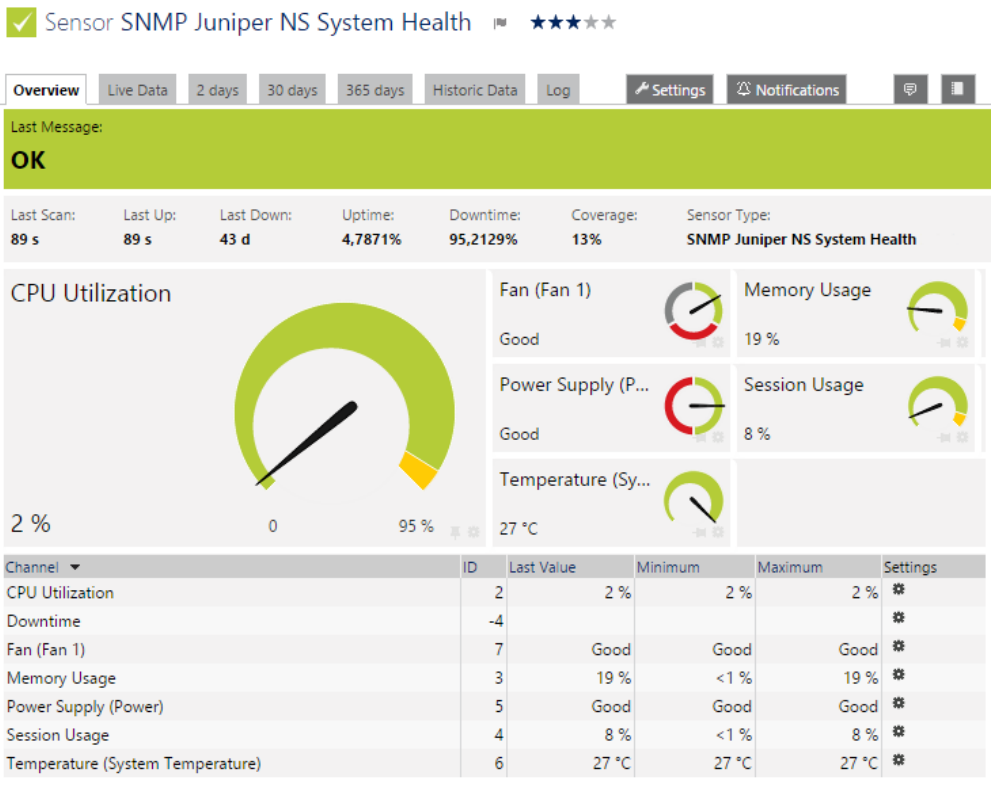
7.8.147 SNMP Juniper NS System Health Sensor

The SNMP Juniper NS System Health sensor monitors the system health of a Juniper NetScreen device using Simple Network Management Protocol (SNMP).

It can show the following:

- CPU utilization
- Fan status
- Power supply status
- System temperature
- Status of memory usage in percent
- Status of session usage in percent

These channels are created at run-time, depending on the available measurement components of your Juniper NetScreen device. Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



SNMP Juniper NS System Health Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_juniper_ns_system_health.png

Remarks

- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.

BASIC SENSOR SETTINGS

Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply. If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply. If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** Custom channel types can be set on sensor level only.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.148 SNMP LenovoEMC Physical Disk Sensor

The SNMP Lenovo Physical Disk sensor monitors a physical disk in a LenovoEMC Network Attached Storage (NAS) via Simple Network Management Protocol (SNMP).

- It shows the overall disk status.

States of the disk can be:

- Normal (sensor status 163 **Up**),
- Unknown (sensor status **Warning**)
- Foreign (sensor status **Warning**)
- Faulted (sensor status **Down**)
- Missing (sensor status **Down**)

Remarks

- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the physical disks in the LenovoEMC NAS. PRTG creates one sensor for each disk you select in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

LENOVOEMC PHYSICAL DISK SETTINGS

Disk	Select the disks you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

LENOVOEMC NAS SETTINGS

Disk	Shows the disk monitored by this sensor. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Name	Shows the name of the disk monitored by this sensor. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Size	Shows the size of the disk monitored by this sensor. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.149 SNMP LenovoEMC System Health Sensor

The SNMP LenovoEMC System Health sensor monitors the system health of a LenovoEMC Network Attached Storage (NAS) via Simple Network Management Protocol (SNMP).

- It shows the overall status of the RAID.

Sensor states 163 can be:

- Normal (sensor status **Up**)
- Unknown (sensor status **Warning**)
- Rebuilding (sensor status **Warning**)
- Degraded (sensor status **Warning**)
- RebuildFS (sensor status **Warning**)
- Faulted (sensor status **Down**)

Furthermore, this sensor can show, for example, states of several fans, voltages, and temperatures. These channels are created at run-time depending on the available measurement components in the LenovoEMC NAS. Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

Remarks

- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. ⓘ You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. ⓘ This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

SENSOR DISPLAY

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.

SCANNING INTERVAL

- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.
	Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:
	▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

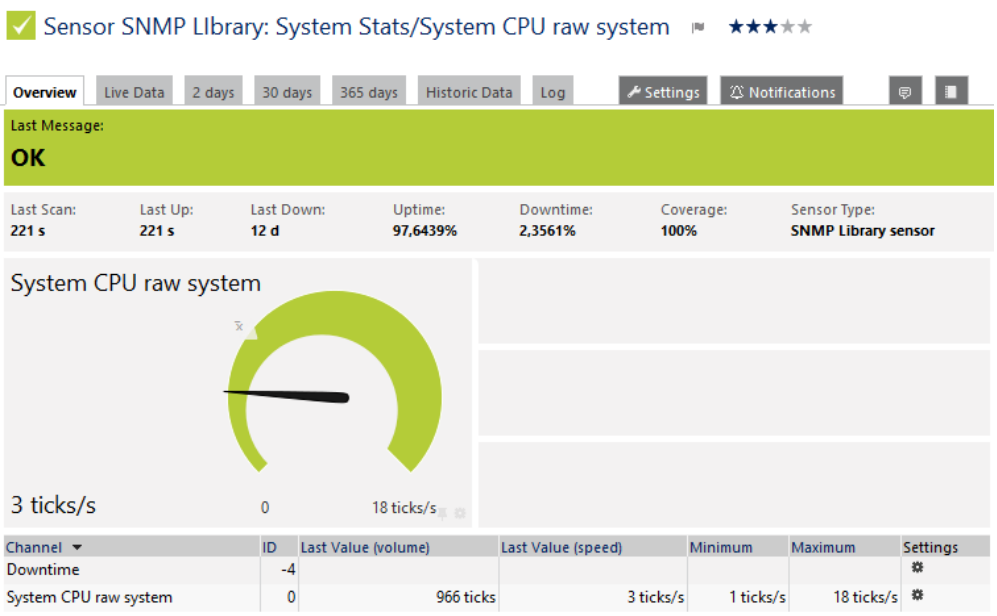
Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.150 SNMP Library Sensor

The SNMP Library sensor monitors a device using Simple Network Management Protocol (SNMP) in combination with a compiled Management Information Base (MIB) library file. This provides custom monitoring beyond the standard SNMP sensors of PRTG. The content of the Management Information Base (MIB) file will determine which data types are available for monitoring. A selection drawn from the OIDs in the MIB is offered when creating the sensor.

To custom monitor SNMP capable devices, download the manufacturer's MIB files for the respective device, convert the Management Information Base (MIB) file to the Paessler oidlib format, and import it into PRTG. To make setting up your monitoring as convenient as possible, PRTG comes with pre-compiled oidlib library files that already contain the Object Identifier (OID) of SNMP counters for the most common devices in a network. See section **More** 1922 for details.



SNMP Library Sensor

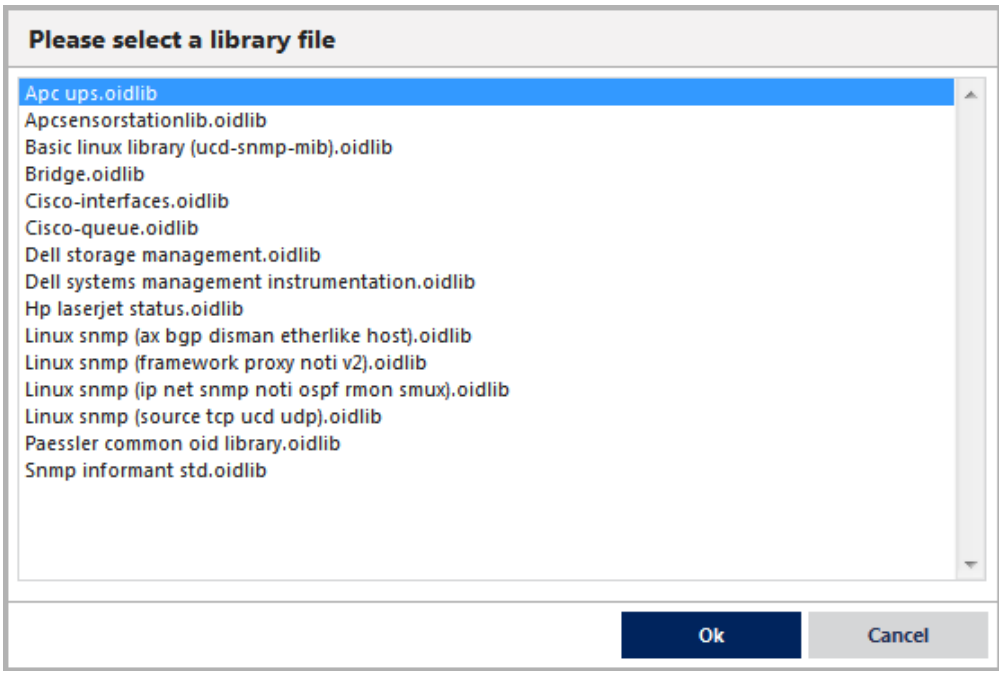
Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_library.png

Remarks

- Knowledge Base: How do SNMP, MIBs and OIDs work?
- Knowledge Base: How can I import my MIB files into PRTG?
- Knowledge Base: Can't find a sensor for my device in PRTG but I believe it supports SNMP. How to proceed?
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Add Sensor

Manually add 288 a new sensor to an SNMP device. From the **Add Sensor** dialog, select **SNMP Library** sensor. PRTG will show a list of oidlib files available on the system. This contains all library files stored at the \snmplibs folder of your PRTG installation directory—both the ones delivered with PRTG and your own files. For details about directory paths, please see section **Data Storage** 3226.



List of SNMP Library Files

The file names on the list indicate the likely purpose. Select a name that appears appropriate for your device (for example, choose an MIB file that you imported before) and confirm via **OK**. Often, the **Paessler common oid library.oidlib** is a good start. If the file does not fit to your device, this will result in the error message the scan for available monitoring items has failed on this device: No such object (SNMP error # 222). If you see this message, click **Cancel** and try adding the sensor with another file. If counters were found for your device, you will see the sensor's settings.

Default OIDLIB Files Overview

The following files are included in PRTG and allow the extension of your SNMP monitoring to many devices. Please be aware that not all devices and/or parameters may be supported by the libraries.

- **APC UPS.oidlib**
  Can be used to monitor uninterruptible power supplies (UPS) from APC American Power Conversion Corp.

- **APCSensorstationlib.oidlib**
  Can be used to monitor alarm status, communication status, humidity, and temperature as shown by an APC sensor station.

- **Basic Linux Library (UCD-SNMP-MIB).oidlib**
  Can be used to monitor basic system parameters on Linux systems, such as memory, disk and swap, CPU, etc.

- **cisco-interfaces.oidlib**
  Can be used to monitor Cisco specific parameters, for example, the number of present network interfaces on a system, several states of an interface (admin, oper, speed, type, errors, discards, etc.), and more.

- **cisco-queue.oidlib**
  Can be used to monitor queues on a Cisco interface, for example, queue depth and its maximum, discarded messages from the queue, the number of the queue within the queue set, etc.

- **Dell Storage Management.oidlib**
  Can be used to monitor Dell storage devices. Possible parameters include disk arrays, battery and power supply, fan and temperature, virtual disk, etc.

- **Dell Systems Management Instrumentation.oidlib**
  Can be used to monitor the hardware of Dell systems. Possible parameters include ACPower and battery, alerts, base board, Bios, BMC, chassis, COO, cooling, event log, firmware, IDE, keyboard, memory, port, network, processor, SCSI, system, temperature, USB, UUID, etc.

- **HP LaserJet Status.oidlib**
  Can be used to monitor toner, paper, and jam status of an HP LaserJet printer.

- **Linux SNMP (AX BGP DisMan EtherLike Host).oidlib**
  Can be used to monitor different aspects of Linux systems.
  This file may detect a very large number of interfaces. It may take a few seconds until the selection table is shown.

- **Linux SNMP (Framework Proxy Noti v2).oidlib**
  Can be used to monitor different aspects of Linux systems.
  This file may detect a very large number of interfaces. It may take a few seconds until the selection table is shown.

- **Linux SNMP (IP Net SNMP Noti OSPF RMON SMUX).oidlib**
  Can be used to monitor different aspects of Linux systems.
  This file may detect a very large number of interfaces. It may take a few seconds until the selection table is shown.

- **Linux SNMP (Source TCP UCD UDP).oidlib**
  Can be used to monitor different aspects of Linux systems.
  This file may detect a very large number of interfaces. It may take a few seconds until the selection table is shown.

- **Paessler Common OID Library.oidlib**
  Can be used to monitor many common hardware devices. It is used for several sensors and is encrypted.

- **SNMP Informant std.oidlib**
  Can be used to monitor logical disks, processor, memory, and network interface on Windows systems.

Import MIB Files

Additionally you can create your own oidlib files by importing your device manufacturers' MIB files with the free tool Paessler **MIB Importer**. Simply convert your mib files and save the resulting oidlib files to the \snmplibs subfolder of your PRTG program directory. For details about directory paths, please see **Data Storage** 3226. For more information and download of **MIB Importer**, please see the link in the **More** 1922 section below.

If your imported oidlib file contains lookups 3183 (you can see this in section **Lookup** in the MIB Importer), you can define your own sensor states for returning values. Add an SNMP Library sensor using this oidlib. PRTG will then create a lookup definition file using the **lookupname** of the chosen library as **id** parameter.
Important: The lookups will be added without state definitions, so the sensor will show a **Warning** status 163 by default! You have to edit the corresponding lookup files to get reliable alarms. Please override the lookup definition with your own custom lookup as described in section **Define Lookups—Customizing Lookups** 3188.

PRTG on demand does not support the import of MIB files. You can use the SNMP Library sensor only with the default oidlib files in PRTG on demand.

SNMP Library Sensor—Add Sensor Settings

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SNMP LIBRARY SPECIFIC

Library	This shows the path to the oidlib file selected before. This setting is shown for your information only and cannot be changed here.
Library-OIDs	Select the aspects of the device you want to monitor. A list specific to your setup is shown. It contains all counters found in the chosen library that match your device. Select one or more items by adding a check mark in front of the respective line. You can also select and deselect all items by using the check box in the table head. For each selection, PRTG will create one sensor when you click the **Continue** button.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SNMP LIBRARY SPECIFIC

Selected Interface	Shows the counter that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Unit String	Enter a string that represents the unit of the returned values. This is for display purposes for the sensor data only. Please enter a string.
Multiplication	Enter the multiplier if you want to multiply the received data by a certain value. Please enter an integer value.
Division	Enter the divisor if you want to divide the received data by a certain value. Please enter an integer value.
If Value Changes	Define what this sensor will do when the sensor value changes. You can choose between: ▪ **Ignore changes (default)**: The sensor takes no action on change. ▪ **Trigger 'change' notification**: The sensor sends an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification 2791 whenever the sensor value changes.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. ⓘ You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel.

SENSOR DISPLAY

	▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. ⓘ This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.

SCANNING INTERVAL

- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: How do SNMP, MIBs and OIDs work?

- https://kb.paessler.com/en/topic/653

Knowledge Base: How can I import my MIB files into PRTG?

- https://kb.paessler.com/en/topic/733

Knowledge Base: Can't find a sensor for my device in PRTG but I believe it supports SNMP. How to proceed?

- https://kb.paessler.com/en/topic/65638

Knowledge Base: How can I monitor EMC Isilon storage systems with PRTG?

- https://kb.paessler.com/en/topic/71413

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

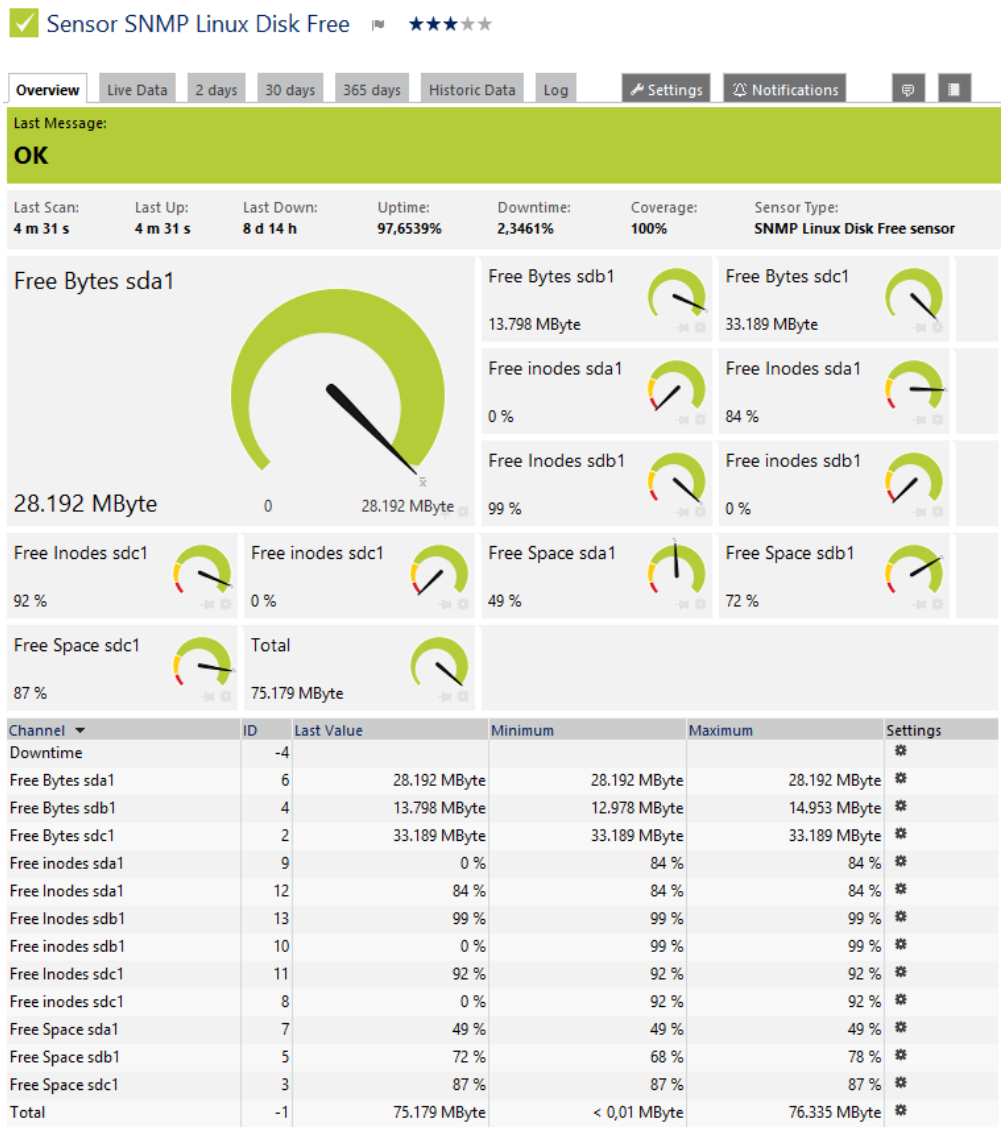
7.8.151 SNMP Linux Disk Free Sensor

The SNMP Linux Disk Free sensor monitors free space on disks of a Linux/Unix system using Simple Network Management Protocol (SNMP).

It shows the following:

- Free total disk space in bytes
- Free space in bytes for every mounted partition
- Free space in percent for every mounted partition
- Free inodes in percent for every mounted partition

The free space returned by this sensor type shows the disk space that is not yet used. Not all of this space may be available for use, as a part of this space can be reserved by the system, for example, for redundancy purposes. For details, please see the article linked in the **More** 1935 section below.



Channel	ID	Last Value	Minimum	Maximum	Settings
Downtime	-4				
Free Bytes sda1	6	28.192 MByte	28.192 MByte	28.192 MByte	
Free Bytes sdb1	4	13.798 MByte	12.978 MByte	14.953 MByte	
Free Bytes sdc1	2	33.189 MByte	33.189 MByte	33.189 MByte	
Free inodes sda1	9	0 %	84 %	84 %	
Free Inodes sda1	12	84 %	84 %	84 %	
Free Inodes sdb1	13	99 %	99 %	99 %	
Free inodes sdb1	10	0 %	99 %	99 %	
Free Inodes sdc1	11	92 %	92 %	92 %	
Free inodes sdc1	8	0 %	92 %	92 %	
Free Space sda1	7	49 %	49 %	49 %	
Free Space sdb1	5	72 %	68 %	78 %	
Free Space sdc1	3	87 %	87 %	87 %	
Total	-1	75.179 MByte	< 0,01 MByte	76.335 MByte	

SNMP Linux Disk Free Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_linux_disk_free.png

Remarks

- Knowledge Base: Why do SSH Disk Free and SNMP Linux Disk Free show different values for my target Linux system?
- Knowledge Base: Checklist: Setting up SNMP on Linux
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SET LIMITS CHECKED AGAINST ALL DISKS

In this section you can set limits that are valid for all channels and all drives. By entering limits, you can define when the sensor will enter a **Warning** or **Down** status, depending on the data provided by all drives that this sensor monitors. If you want to define limits for separate channels individually, please use the limit settings in the sensor **Channel** settings.

All limits that you define here are valid in addition to the limits defined in the particular **Channels** settings! The limits are valid simultaneously, so the first limit that is breached applies.

Percentage Limit Check	Enable or disable a limit check for the free space in percentage channels of all drives. By default, percentage limits are enabled with lower warning and lower error limit. Choose between: ▪ **Only use the limits in the settings of the percentage channels**: Do not define sensor limits which are valid for all percentage channels. The sensor only uses limits which you define in the settings of the particular "free space in percent" channels to determine the status. ▪ **Use the limits of both the sensor and the channel settings**: Define limits for the sensor which are valid for all drives (percentage channels). Additional fields appear below. The sensor enters a **Warning** or **Down** status when free space limits are undercut or overrun.
Upper Error Limit	This field is only visible if you enable percentage limit check above. Specify an upper limit in percent for a **Down** status. If the free disk space of one of your drives overruns this percent value, the sensor switches to **Down**. Please enter an integer value or leave the field empty. The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the **Sensor Channels Settings** 2782. The limits set here and in the channel settings are valid simultaneously!
Upper Warning Limit	This field is only visible if you enable percentage limit check above. Specify an upper limit in percent for a **Warning** status. If the free disk space of one of your drives overruns this percent value, the sensor switches to **Warning**. Please enter an integer value or leave the field empty. The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the **Sensor Channels Settings** 2782. The limits set here and in the channel settings are valid simultaneously!

SET LIMITS CHECKED AGAINST ALL DISKS

Lower Warning Limit	This field is only visible if you enable percentage limit check above. Specify a lower limit in percent for a **Warning** status. If the free disk space of one of your drives undercuts this percent value, the sensor switches to warning. Please enter an integer value or leave the field empty. The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the Sensor Channels Settings 2782. The limits set here and in the channel settings are valid simultaneously!
Lower Error Limit	This field is only visible if you enable percentage limit check above. Specify a lower limit in percent for a **Down** status. If the free disk space of one of your drives undercuts this percent value, the sensor switches to **Down**. Please enter an integer value or leave the field empty. The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the Sensor Channels Settings 2782. The limits set here and in the channel settings are valid simultaneously!
Size Limit Check	Enable or disable a limit check for the free bytes channels of all drives. By default, byte size limits are not enabled for drives. Choose between: • **Only use the limits in the settings of the byte size channels**: Do not define sensor limits which are valid for all byte size channels. The sensor only uses limits which you define in the settings of the particular free space in bytes channels to determine the status. • **Use the limits of both the sensor and the channel settings**: Define limits for the sensor which are valid for all drives (byte size channels). Additional fields appear below. The sensor enters a **Warning** or **Down** status when free space limits are undercut or overrun.
Upper Error Limit	This field is only visible if you enable byte limit check above. Specify an upper limit. Use the same unit as shown by the free bytes channels of this sensor (by default this is MByte). If the free disk space of one of your drives overruns this bytes value, the sensor switches to **Down**. Please enter an integer value or leave the field empty. The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the Sensor Channels Settings 2782. The limits set here and in the channel settings are valid simultaneously!

SET LIMITS CHECKED AGAINST ALL DISKS

Upper Warning Limit	This field is only visible if you enable byte limit check above. Specify an upper limit. Use the same unit as shown by the free bytes channels of this sensor (by default this is MByte). If the free disk space of one of your drives overruns this bytes value, the sensor switches to **Warning**. Please enter an integer value or leave the field empty. The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the **Sensor Channels Settings**. The limits set here and in the channel settings are valid simultaneously!
Lower Warning Limit	This field is only visible if you enable byte limit check above. Specify a lower limit. Use the same unit as shown by the free bytes channels of this sensor (by default this is MByte). If the free disk space of one of your drives undercuts this bytes value, the sensor switches to **Warning**. Please enter an integer value or leave the field empty. The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the **Sensor Channels Settings**. The limits set here and in the channel settings are valid simultaneously!
Lower Error Limit	This field is only visible if you enable byte limit check above. Specify a lower limit. Use the same unit as shown by the free bytes channels of this sensor (by default this is MByte). If the free disk space of one of your drives undercuts this bytes value, the sensor switches to **Down**. Please enter an integer value or leave the field empty. The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the **Sensor Channels Settings**. The limits set here and in the channel settings are valid simultaneously!
Alarm on Missing/ Removed Disk	If a monitored disk is removed or not found, values are set to zero. Select the alarming approach in this case. Choose between: ▪ **Deactivate alarm (default)**: Select this option if you do not want an alarm for a removed disk. ▪ **Activate alarm**: Select this option if you want to be alerted if a monitored disk is removed.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: Why do SSH Disk Free and SNMP Linux Disk Free show different values for my target Linux system?

- https://kb.paessler.com/en/topic/43183

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Knowledge Base: Checklist: Setting up SNMP on Linux

- https://kb.paessler.com/en/topic/5353

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

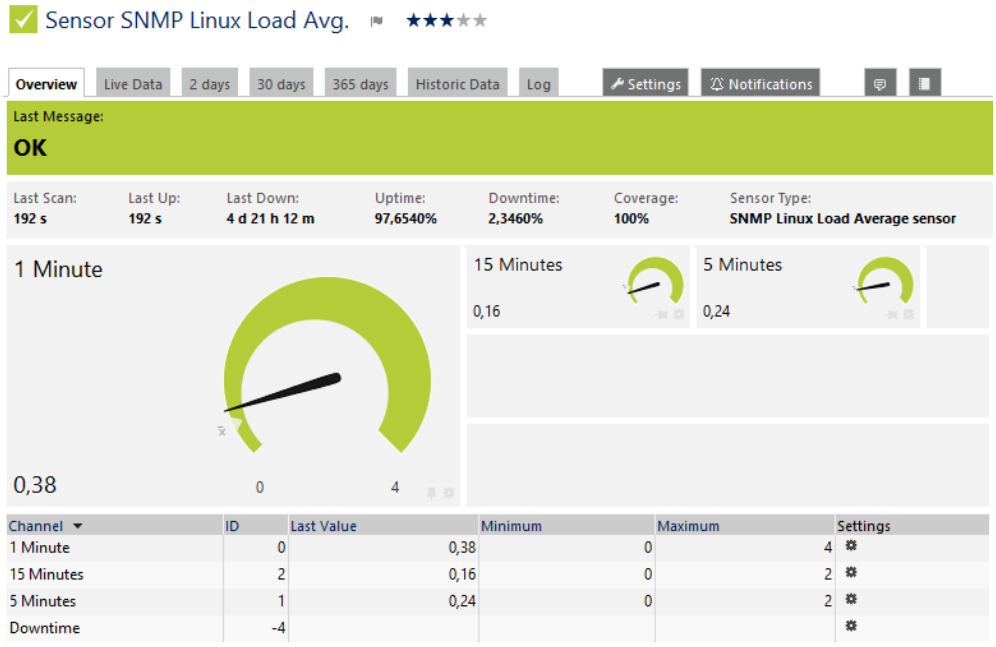
For more general information about settings, please see the **Object Settings** 188 section.

7.8.152 SNMP Linux Load Average Sensor

The SNMP Load Average sensor monitors the system load average of a Linux/Unix system using Simple Network Management Protocol (SNMP).

It shows the following:

- Average system load within a 1-minute interval
- Average system load within a 5-minute interval
- Average system load within a 15-minute interval



SNMP Linux Load Average Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_linux_load_average.png

Remarks

- Knowledge Base: Checklist: Setting up SNMP on Linux
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

SENSOR DISPLAY

Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Knowledge Base: Checklist: Setting up SNMP on Linux

- https://kb.paessler.com/en/topic/5353

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

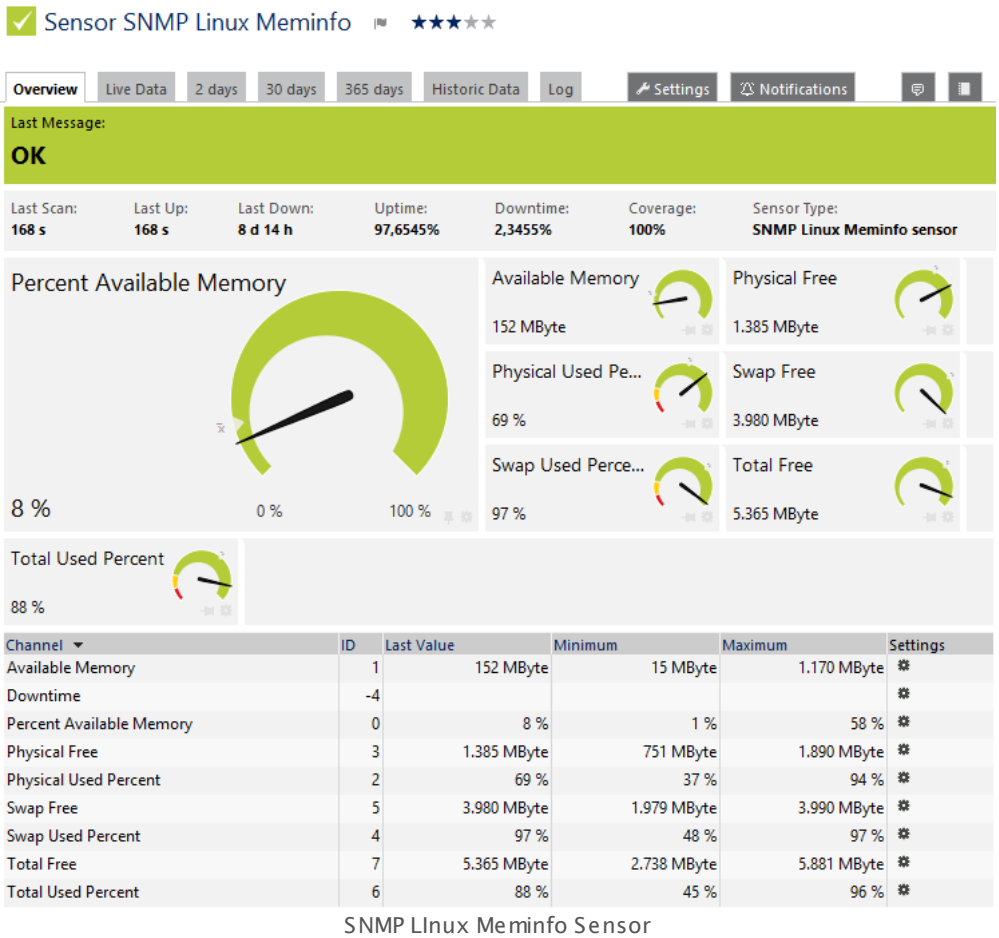
For more general information about settings, please see the **Object Settings** 188 section.

7.8.153 SNMP Linux Meminfo Sensor

The SNMP Linux Meminfo sensor monitors the memory usage of a Linux/Unix system using Simple Network Management Protocol (SNMP).

It shows the following :

- Available memory in absolute and percentage values
- Used physical memory (free memory plus buffer plus cache) in percent
- Free physical memory (free memory plus buffer plus cache) in bytes
- Used swap memory in percent
- Free swap memory in bytes
- Used memory on the whole system (physical memory plus swap) in percent
- Free memory on the whole system (physical memory plus swap) in bytes



SNMP LInux Meminfo Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_linux_meminfo.png

Remarks

- Knowledge Base: Checklist: Setting up SNMP on Linux
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Knowledge Base: Checklist: Setting up SNMP on Linux

- https://kb.paessler.com/en/topic/5353

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

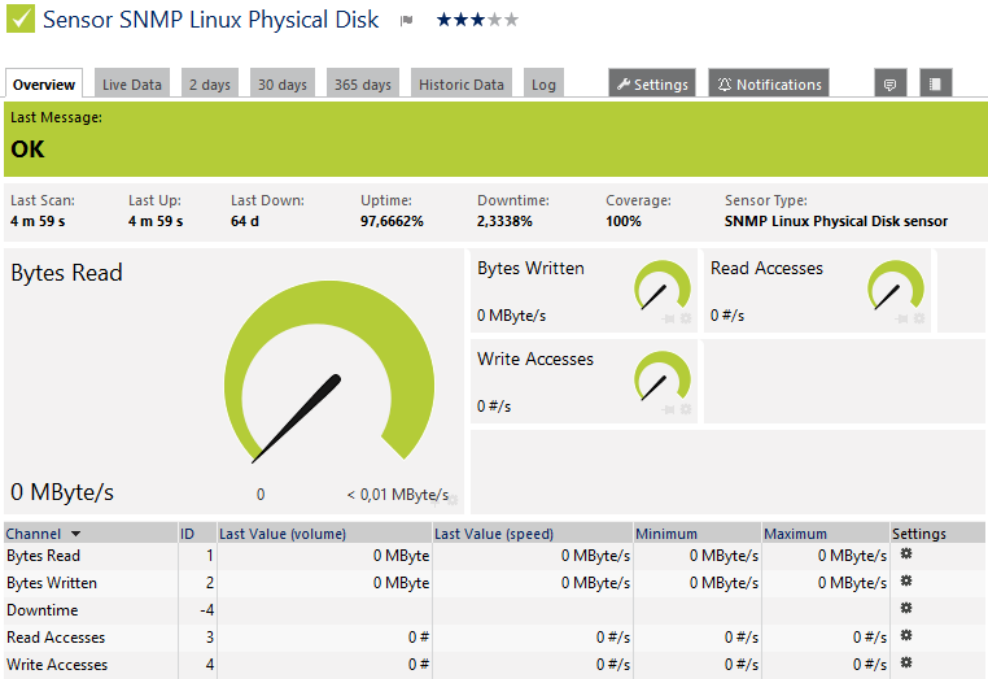
For more general information about settings, please see the **Object Settings** 188 section.

7.8.154 SNMP Linux Physical Disk Sensor

The SNMP Linux Physical Disk sensor monitors input/output (I/O) on disks of a Linux/Unix system using Simple Network Management Protocol (SNMP).

It shows the following:

- Read bytes per second
- Written bytes per second
- Number of read accesses per second
- Number of write accesses per second



SNMP Linux Physical Disk Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_linux_physical_disk.png

Remarks

- Knowledge Base: Checklist: Setting up SNMP on Linux
- For a general introduction to the technology behind SNMP, please see the manual section Monitoring via SNMP 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the disks of the Linux/Unix system you want to monitor. PRTG creates one sensor for each disk you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

PHYSICAL DISK SETTINGS

Disk	Select the disks you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	Enter one or more **Tags**, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

PHYSICAL DISK SETTINGS

Disk Bitmask	Shows further information about the disk that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. ⓘ You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.

SCANNING INTERVAL

- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. ⓘ To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Knowledge Base: Checklist: Setting up SNMP on Linux

- https://kb.paessler.com/en/topic/5353

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

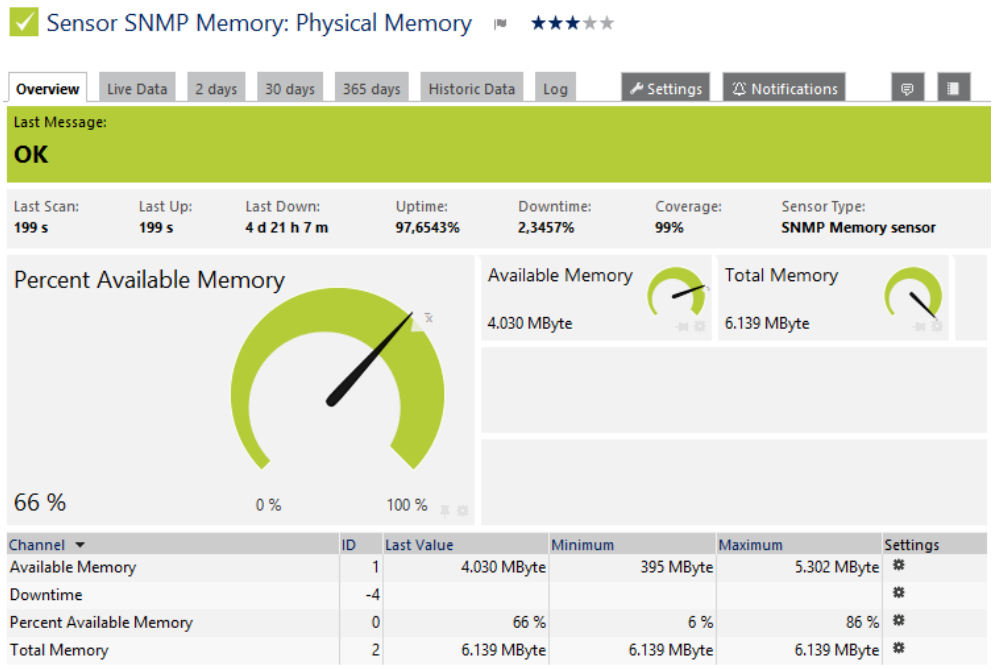
7.8.155 SNMP Memory Sensor

The SNMP Memory sensor monitors the memory usage of a system via Simple Network Management Protocol (SNMP).

It can show the following:

- Available memory in bytes
- Available memory in percent
- Total memory

This sensor uses more generic Object Identifier (OID) values compared to the **SNMP Linux Meminfo Sensor** 1944.



SNMP Memory Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_memory.png

Remarks

- It might not work to query data from a probe device via SNMP (querying localhost, 127.0.0.1, or ::1). Add this device to PRTG 275 with the IP address that it has in your network and create the SNMP sensor on this device instead.
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the memory types you want to monitor. PRTG creates one sensor for each memory type you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

MEMORY SETTINGS

Memory	Select one or more memory types you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	Enter one or more **Tags**, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

MEMORY SETTINGS

Memory	Shows the type of the memory that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. ⓘ You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel.

SENSOR DISPLAY

	▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. ⓘ This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.

SCANNING INTERVAL

- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.156 SNMP NetApp Disk Free Sensor

The SNMP NetApp Disk Free sensor monitors free space on disks of a NetApp storage system via Simple Network Management Protocol (SNMP).

It can show the following:

- Free disk space in bytes and percent
- Deduplication saved space in bytes and percent
- Deduplication shared space in bytes and percent
- Disk free status
- Free files in percent
- Free INodes in percent

SNMP NetApp Disk Free Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_netapp_disk_free.png

Remarks

- Knowledge Base: How can I monitor capacity and used disk space on a NetApp?
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the disk on the NetApp you want to monitor. PRTG creates one sensor for each disk you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

NETAPP DISK FREE SETTINGS

File System	Select the disks you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

NETAPP DISK FREE SETTINGS

File System	Shows the name of the disk that this sensor is monitoring. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Virtual Disk	Shows the name of the virtual disk that this sensor is monitoring (if applicable). Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: How can I monitor capacity and used disk space on a NetApp?

- https://kb.paessler.com/en/topic/61231

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

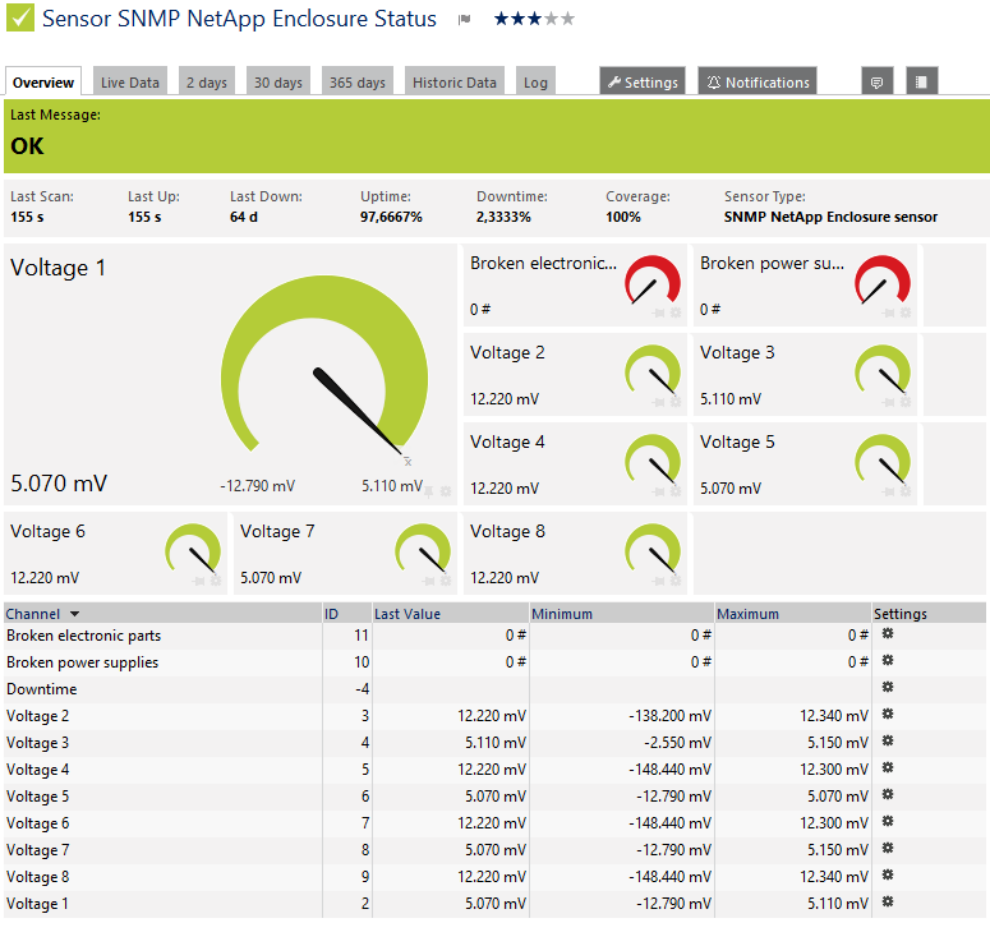
For more general information about settings, please see the **Object Settings** 188 section.

7.8.157 SNMP NetApp Enclosure Sensor

The SNMP NetApp Enclosure sensor monitors the power supply and cooling of an enclosure that is part of a NetApp storage system via Simple Network Management Protocol (SNMP).

It can show the following, depending on the measurements you choose:

- Temperatures
- Rotations per minute (RPM) of fans and the number of failed fans
- Voltages in mV, the number of broken electronic parts, and the number of broken power supplies
- Currents in mA



Channel	ID	Last Value	Minimum	Maximum	Settings
Broken electronic parts	11	0 #	0 #	0 #	
Broken power supplies	10	0 #	0 #	0 #	
Downtime	-4				
Voltage 2	3	12.220 mV	-138.200 mV	12.340 mV	
Voltage 3	4	5.110 mV	-2.550 mV	5.150 mV	
Voltage 4	5	12.220 mV	-148.440 mV	12.300 mV	
Voltage 5	6	5.070 mV	-12.790 mV	5.070 mV	
Voltage 6	7	12.220 mV	-148.440 mV	12.300 mV	
Voltage 7	8	5.070 mV	-12.790 mV	5.150 mV	
Voltage 8	9	12.220 mV	-148.440 mV	12.340 mV	
Voltage 1	2	5.070 mV	-12.790 mV	5.110 mV	

SNMP NetApp Enclosure Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_netapp_enclosure.png

Remarks

- This sensor type has predefined limits for several metrics. You can change these limits individually in the channel settings. For detailed information about channel limits, please refer to the manual section **Sensor Channels Settings** 2782.
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the power supply and cooling measurements of an enclosure on a NetApp you want to monitor. PRTG creates one sensor for each enclosure/measurement combination you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

NETAPP ENCLOSURE SETTINGS

Enclosure	Select the enclosures with the measurement you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

NETAPP ENCLOSURE SETTINGS

Enclosure	Shows the identifier of the enclosure that this sensor is monitoring. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Measurement	Shows the monitored measurement. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

NETAPP SPECIFIC

N/A Measurements

Define the sensor behavior if the requested NetApp value is not available ("N/A" values). Choose between:

- **Interpret as error (default)**: Choose this option to set the sensor to a **Down** status if a measurement is not available. We recommend that you use this setting to not miss any hardware errors.
- **Interpret as valid**: Choose this option to handle unavailable measurements as valid sensor results to keep the sensor in **Up** status. This might be useful, for example, if a hardware sensor on the NetApp is disabled for some reason but actually there is no hardware error. If the NetApp returns an "N/A" measurement, the sensor interprets this as "0".
  We recommend that you use the lookup file **prtg.standardlookups.netapp.notavailable.ovl** for channels with unavailable measurements if you choose this option. This replaces "0" with the message "Not Available". Open the **Sensor Channels Settings** 2782 of the affected channel(s) and choose this file in section **Value Lookup**. For details, please see section **Define Lookups** 3183.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

ⓘ You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.
- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  ⓘ This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

SENSOR DISPLAY

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.

SCANNING INTERVAL

- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.
	Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:
	▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

(i) To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

(i) Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** Custom channel types can be set on sensor level only.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

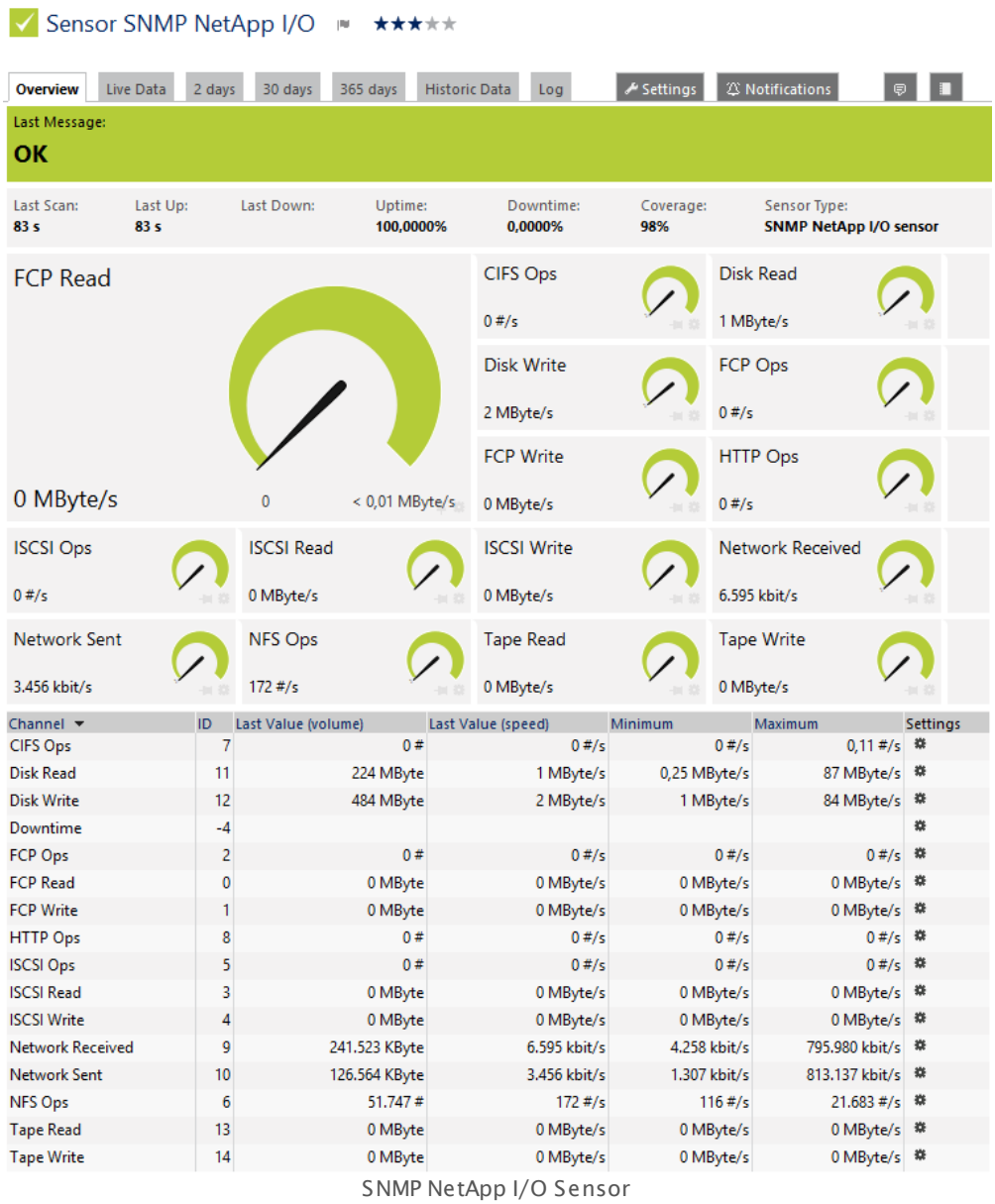
For more general information about settings, please see the **Object Settings** 188 section.

7.8.158 SNMP NetApp I/O Sensor

The SNMP NetApp I/O sensor monitors input/output operations (IOPS) on a NetApp storage system via Simple Network Management Protocol (SNMP).

It can show the following:

- FCP read speed
- CIFS operations per second
- Disk read speed
- Disk write speed
- FCP operations per second
- FCP read speed
- FCP write speed
- HTTP operations per second
- ISCSI operations per second
- ISCSI read speed
- ISCSI write speed
- Network received bytes
- Network sent bytes
- NFS operations per second
- Tape read speed
- Tape write speed



Channel	ID	Last Value (volume)	Last Value (speed)	Minimum	Maximum	Settings
CIFS Ops	7	0 #	0 #/s	0 #/s	0,11 #/s	
Disk Read	11	224 MByte	1 MByte/s	0,25 MByte/s	87 MByte/s	
Disk Write	12	484 MByte	2 MByte/s	1 MByte/s	84 MByte/s	
Downtime	-4					
FCP Ops	2	0 #	0 #/s	0 #/s	0 #/s	
FCP Read	0	0 MByte	0 MByte/s	0 MByte/s	0 MByte/s	
FCP Write	1	0 MByte	0 MByte/s	0 MByte/s	0 MByte/s	
HTTP Ops	8	0 #	0 #/s	0 #/s	0 #/s	
ISCSI Ops	5	0 #	0 #/s	0 #/s	0 #/s	
ISCSI Read	3	0 MByte	0 MByte/s	0 MByte/s	0 MByte/s	
ISCSI Write	4	0 MByte	0 MByte/s	0 MByte/s	0 MByte/s	
Network Received	9	241.523 KByte	6.595 kbit/s	4.258 kbit/s	795.980 kbit/s	
Network Sent	10	126.564 KByte	3.456 kbit/s	1.307 kbit/s	813.137 kbit/s	
NFS Ops	6	51.747 #	172 #/s	116 #/s	21.683 #/s	
Tape Read	13	0 MByte	0 MByte/s	0 MByte/s	0 MByte/s	
Tape Write	14	0 MByte	0 MByte/s	0 MByte/s	0 MByte/s	

SNMP NetApp I/O Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_netapp_io.png

Remarks

- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

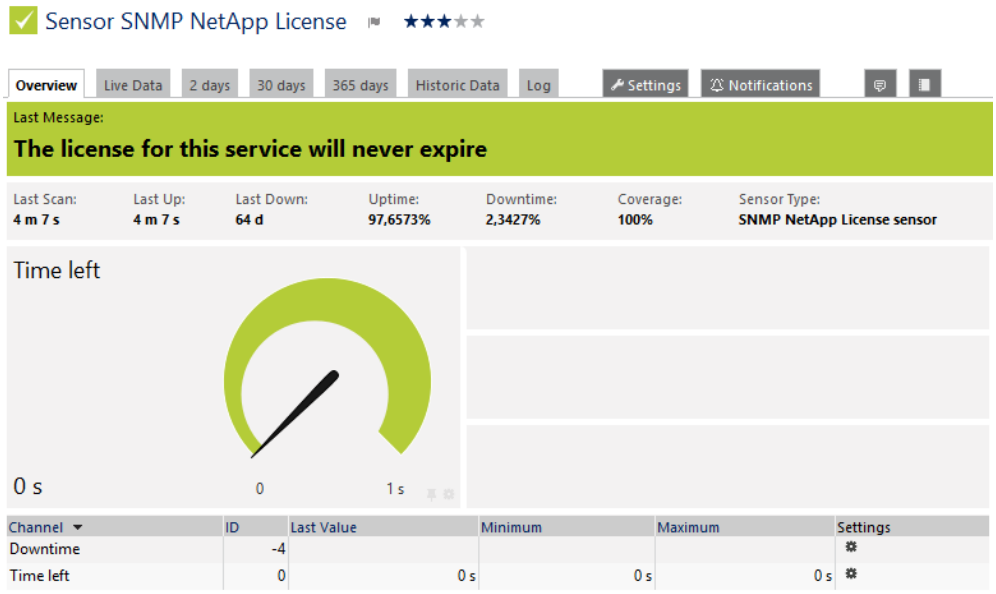
Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.159 SNMP NetApp License Sensor

The SNMP NetApp License sensor monitors the licenses for the services of a NetApp storage system via Simple Network Management Protocol (SNMP).

- It shows how much time is left until the license for a service expires. This can help you detect when a NetApp license is going to expire.



SNMP NetApp License Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_netapp_license.png

Remarks

- For a general introduction to the technology behind SNMP, please see the manual section Monitoring via SNMP 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the NetApp license you want to monitor. PRTG creates one sensor for each license you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

NETAPP LICENSE SETTINGS

License for Service	Select the licenses you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

NETAPP LICENSE SETTINGS

License for Service	Shows the name of the service whose license this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply. If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply. If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

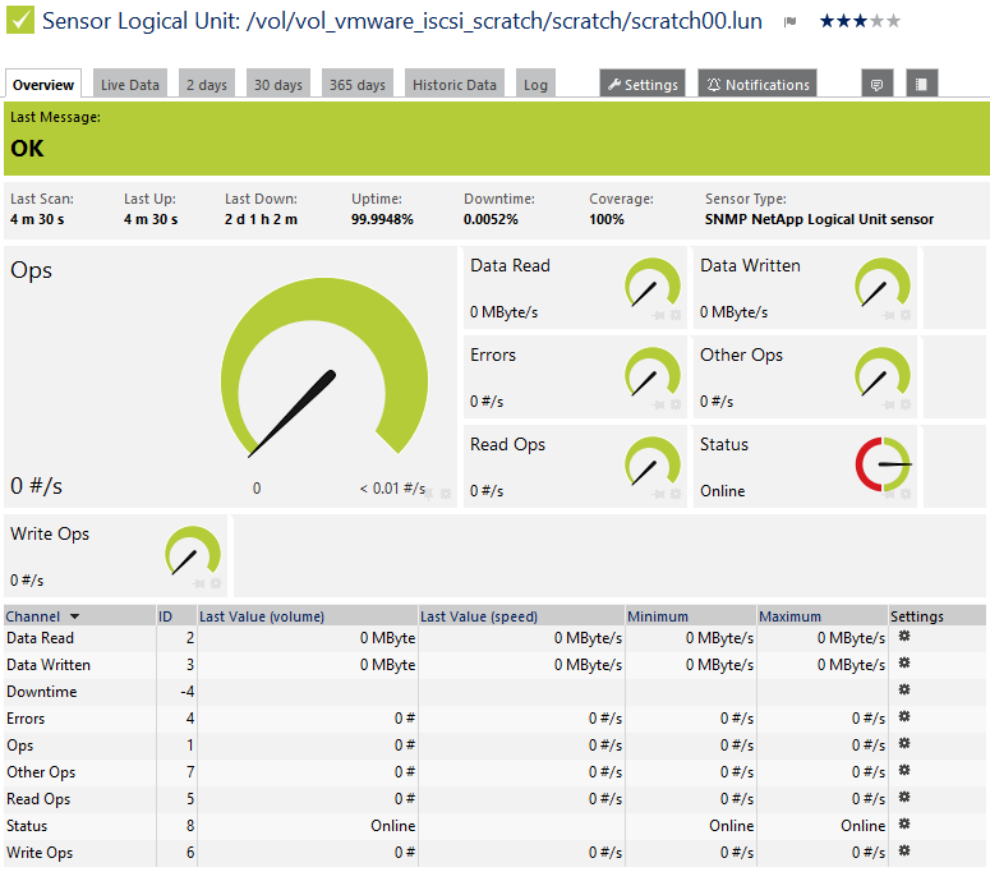
For more general information about settings, please see the **Object Settings** 188 section.

7.8.160 SNMP NetApp Logical Unit Sensor

The SNMP NetApp Logical Unit sensor monitors the input/output operations (IOPS) on a logical unit of a NetApp storage system via Simple Network Management Protocol (SNMP).

It can show the following:

- Total number of operations per second
- Data read speed
- Data write speed
- Number of errors per second
- Number of read operations per second
- Number of write operations per second
- Number of other operations per second
- Status of the logical unit (online or offline)



SNMP NetApp Logical Unit Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_netapp_logical_unit.png

Remarks

- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the logical units on the NetApp you want to monitor. PRTG creates one sensor for each unit you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

NETAPP DISK FREE SETTINGS

Logical Unit	Select the logical units you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

NETAPP LOGICAL UNIT SETTINGS

Logical Unit	Shows the name of the logical unit that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. ⓘ You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor.

SENSOR DISPLAY

- **Show channels independently (default)**: Show an own graph for each channel.
- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

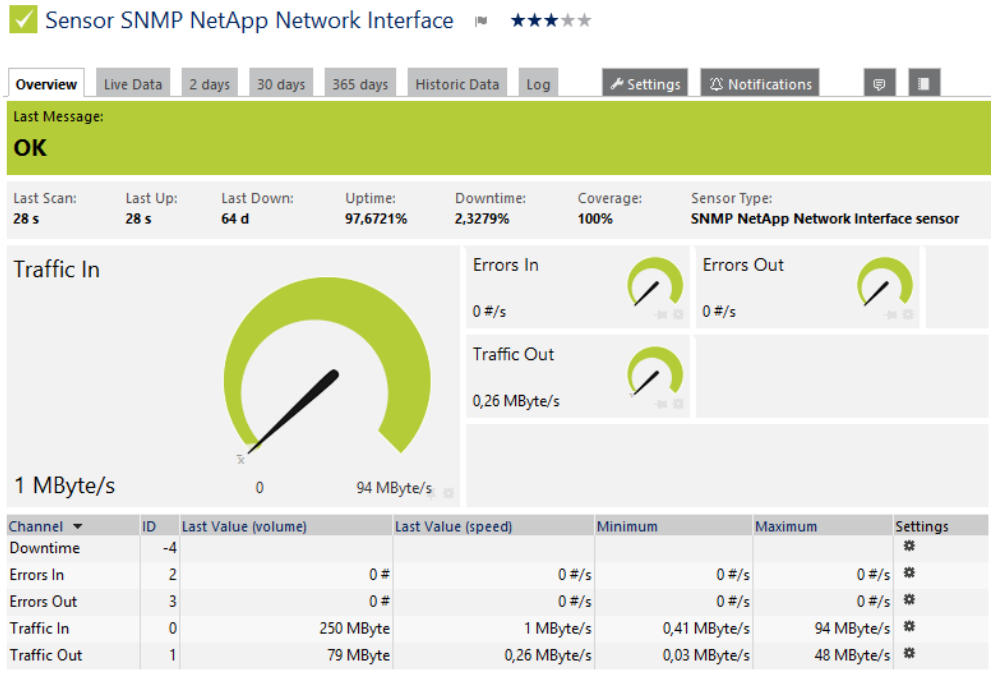
For more general information about settings, please see the **Object Settings** 188 section.

7.8.161 SNMP NetApp Network Interface Sensor

The SNMP NetApp Network Interface sensor monitors a network card of a NetApp storage system via Simple Network Management Protocol (SNMP).

It can show the following:

- Traffic in
- Traffic out
- Number of errors per second (in and out).



SNMP NetApp Network Interface Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_netapp_network_interface.png

Remarks

- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the network interfaces on the NetApp you want to monitor. PRTG creates one sensor for each interface you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

NETAPP NETWORK INTERFACE SETTINGS

Network Interface	Select the interfaces you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.

BASIC SENSOR SETTINGS

Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

NETAPP NETWORK INTERFACE SETTINGS

Network Interface	Shows the name of the interface that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. ⓘ Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

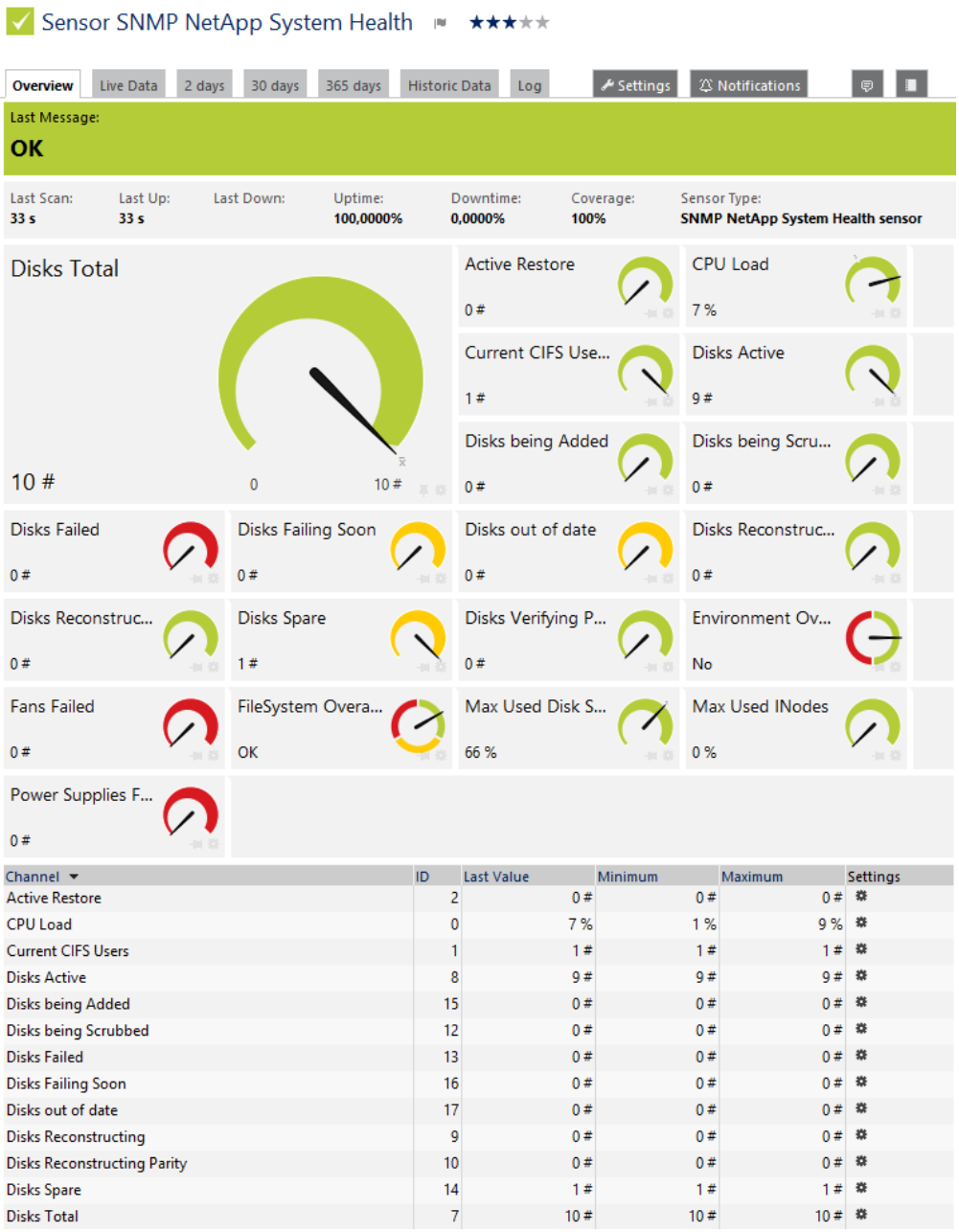
7.8.162 SNMP NetApp System Health Sensor

The SNMP NetApp System Health sensor monitors the status of a NetApp storage system via Simple Network Management Protocol (SNMP).

It can show the following:

- CPU load in percent
- Number of active restores
- Number of current CIFS users
- Number of active disks
- Number of disks being added
- Number of disks being scrubbed
- Number of failed disks
- Number of soon failing disks
- Number of disks being out of date
- Number of reconstructing (parity) disks
- Number of spare disks
- Total number of disks
- Number of verifying (parity) disks
- Number of failed fans
- Number of failed power supplies
- Maximum used disk space in percent
- Maximum used INodes in percent
- If the environment is over temperature

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



SNMP NetApp System Health Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_netapp_system_health.png

Remarks

- For a general introduction to the technology behind SNMP, please see the manual section Monitoring via SNMP 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

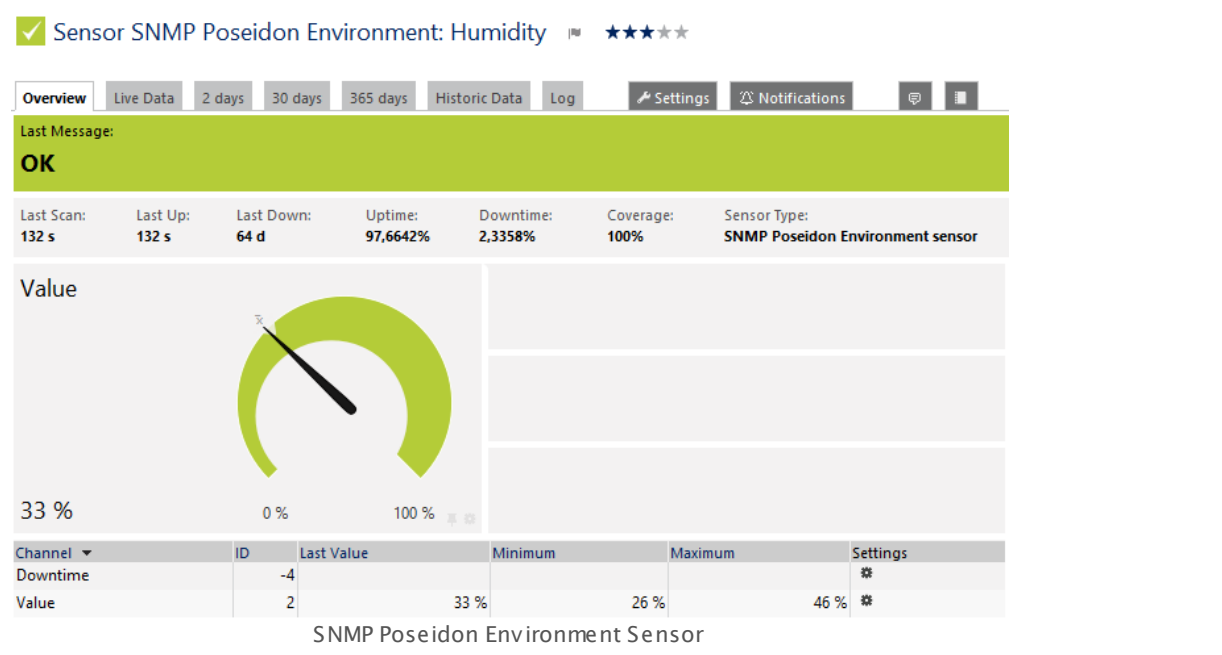
7.8.163 SNMP Poseidon Environment Sensor

The SNMP Poseidon Environment sensor monitors performance counters for environmental measurements on Poseidon hardware via Simple Network Management Protocol (SNMP).

It can show, depending on available measurement components on the hardware device and what measurement you choose:

- Humidity
- Temperature

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



SNMP Poseidon Environment Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_poseidon_environment.png

Remarks

- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

In order to monitor performance counters for environmental measurements on Poseidon hardware, PRTG will create one sensor for each measuring point you choose. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

POSEIDON ENVIRONMENT SPECIFIC

Measuring Point	Select the measurements you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.

BASIC SENSOR SETTINGS

Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

POSEIDON ENVIRONMENT SPECIFIC

Name	
Unit	Shows further information about the measurement. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Measuring Point	

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

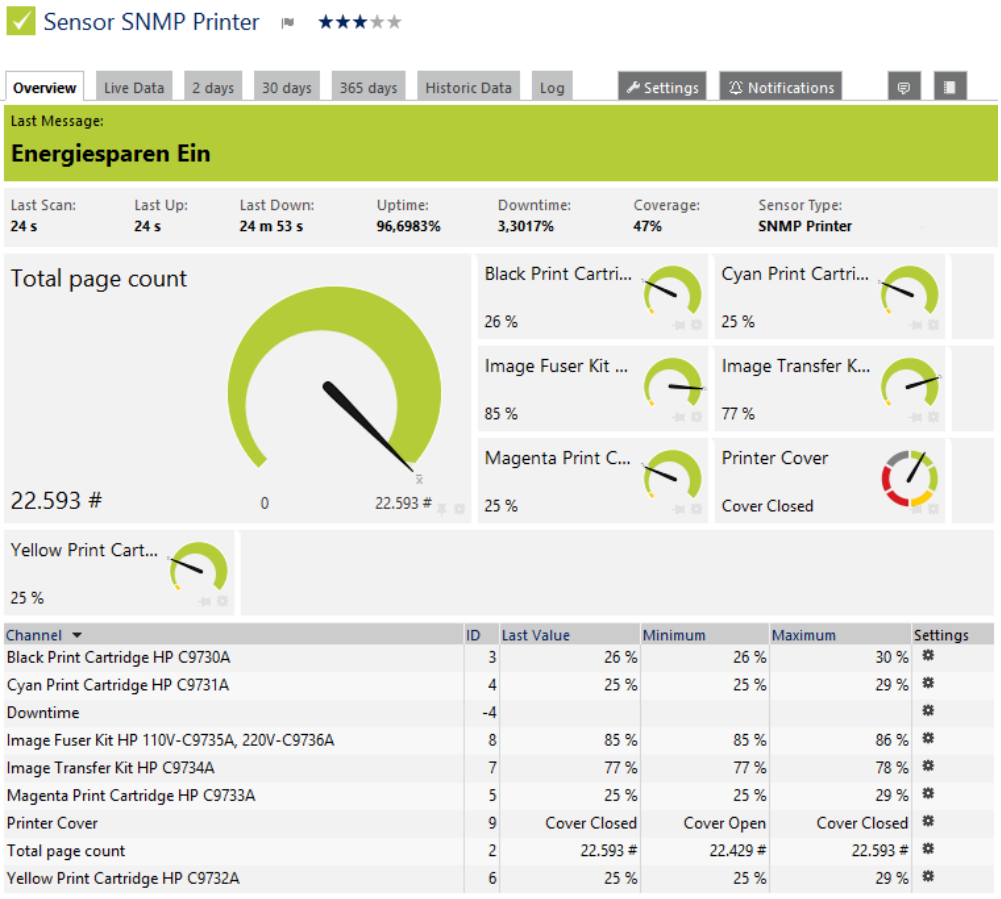
For more general information about settings, please see the **Object Settings** 188 section.

7.8.164 SNMP Printer Sensor

The SNMP Printer sensor is a generic sensor that monitors various types of printers via Simple Network Management Protocol (SNMP).

It can show the following:

- Total number of printed pages
- Fill level of cartridges and toners
- Status of the printer cover
- Additionally, the sensor shows the printer status as sensor message.



SNMP Printer Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_printer.png

Remarks

- This sensor type supports the following printers, among others: HP OfficeJet printers, HP LaserJet printers, RICOH SP 5200, SP 3410, SP C242DN, MP C3003, MP C2503

- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

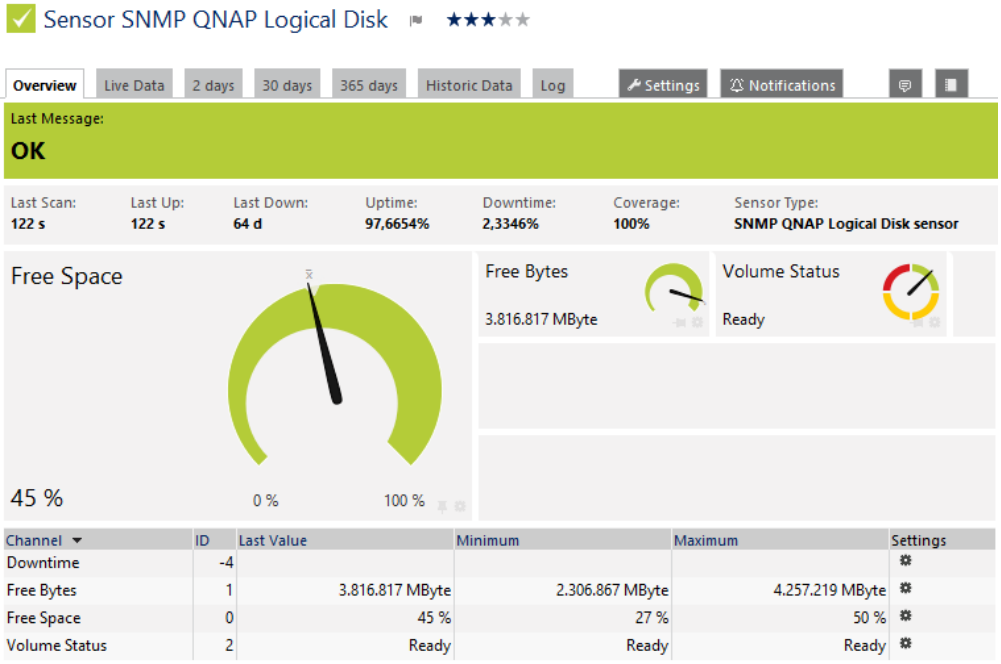
For more general information about settings, please see the **Object Settings** 188 section.

7.8.165 SNMP QNAP Logical Disk Sensor

The SNMP QNAP Logical Disk sensor monitors a logical disk in a QNAP Network Attached Storage (NAS) via Simple Network Management Protocol (SNMP).

It can show the following:

- Free disk space in percent
- Free disk space in bytes
- Status of the volume



SNMP QNAP Logical Disk Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_qnap_logical_disk.png

Remarks

- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the logical disks in the QNAP NAS you want to monitor. PRTG creates one sensor for each disk you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

QNAP NAS SETTINGS

Disk	Select the logical disks you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	Enter one or more **Tags**, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

QNAP NAS SETTINGS

Disk	
Description	Shows further information about the disk that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
File System	

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. ⓘ You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.

SCANNING INTERVAL

- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

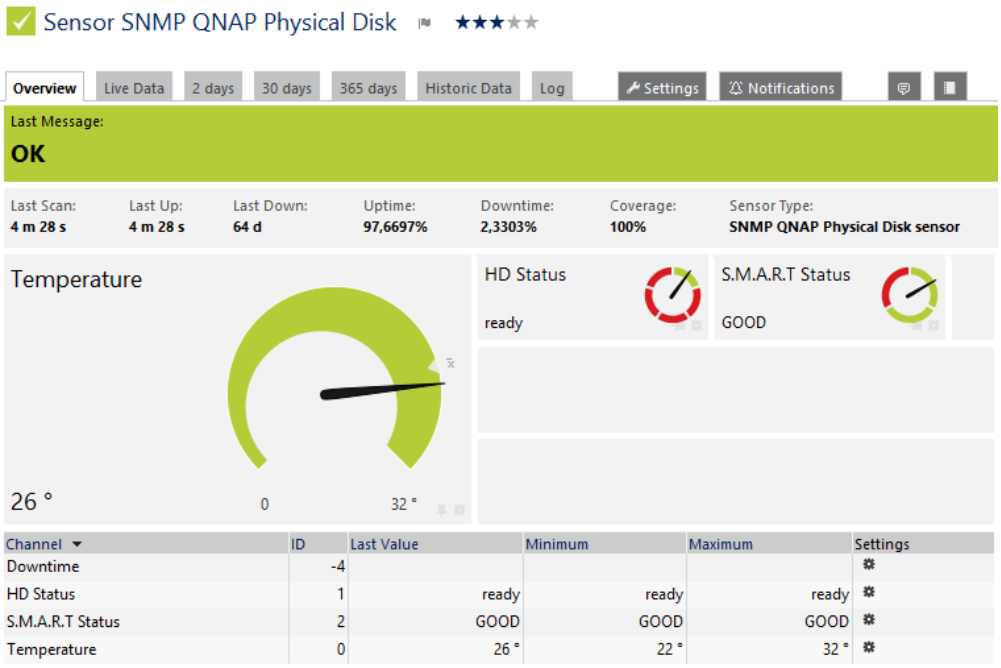
For more general information about settings, please see the **Object Settings** 188 section.

7.8.166 SNMP QNAP Physical Disk Sensor

The SNMP QNAP Physical Disk sensor monitors a physical disk in a QNAP Network Attached Storage (NAS) via Simple Network Management Protocol (SNMP).

It can show the following:

- Temperature
- Disk status
- Self-Monitoring, Analysis and Reporting Technology (S.M.A.R.T.) status of the disk.



SNMP QNAP Physical Disk Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_qnap_physical_disk.png

Remarks

- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the physical disks in the QNAP NAS you want to monitor. PRTG creates one sensor for each disk you choose in the **Add Sensor** dialog. You can also define the unit of the temperature measurement. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

QNAP NAS SETTINGS

Disk	Select the physical disks you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.
Unit	Select the unit of the temperature measurement. Choose between **Celsius** and **Fahrenheit**.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.

BASIC SENSOR SETTINGS

Parent Tags	Shows **Tags** [124] that this sensor inherits [124] from its parent device, group, and probe [118]. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** [124], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited [124] from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

QNAP NAS SETTINGS

Disk	
Description	
Model	Shows further information about the disk. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Capacity	
Unit	

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

SENSOR DISPLAY

Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

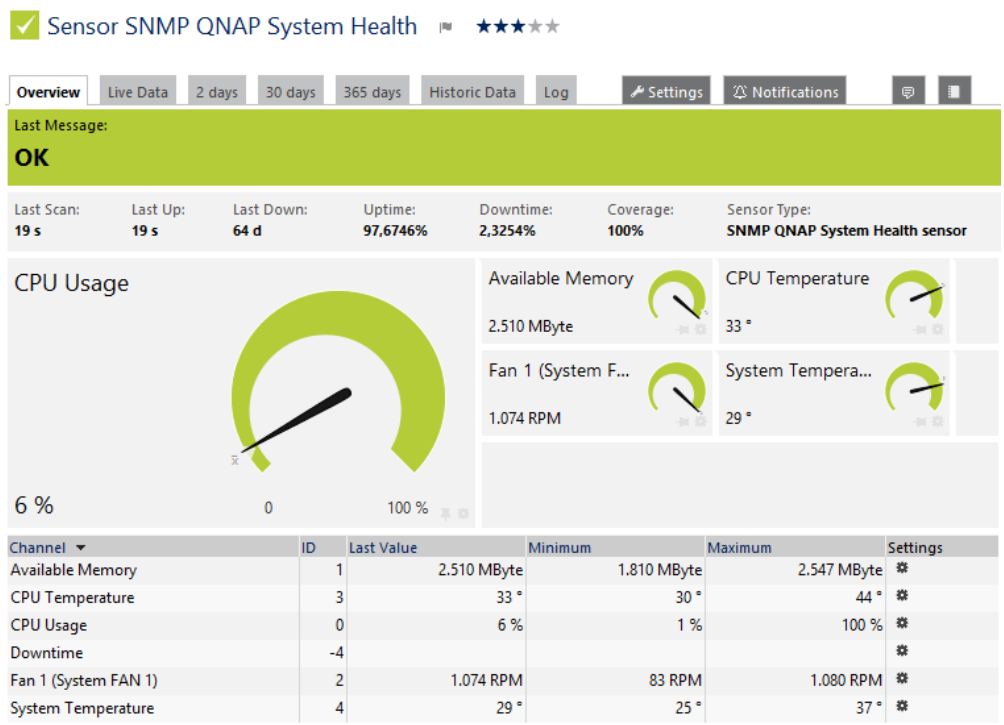
7.8.167 SNMP QNAP System Health Sensor

The SNMP QNAP System Health sensor monitors the system health of a QNAP Network Attached Storage (NAS) via Simple Network Management Protocol (SNMP).

It can show the following, depending on the available measurement components:

- CPU usage in percent
- Available memory in bytes
- Temperature of CPU
- Temperature of system
- Revolutions of fans per minute (RPM)

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



SNMP QNAP System Health Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_qnap_system_health.png

Remarks

- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

To monitor the system health of a QNAP NAS, specify the unit of the temperature measurement.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

QNAP NAS SETTINGS

Unit	Select the unit of the temperature measurement. Choose between **Celsius** and **Fahrenheit**.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

BASIC SENSOR SETTINGS

	You can add additional tags to the sensor if you like. Other tags are automatically inherited[124] from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

QNAP NAS SETTINGS

Unit	Shows the unit of temperatures as monitored with this sensor. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. ⓘ You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. ⓘ This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings**[2782] settings).

SENSOR DISPLAY

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.

SCANNING INTERVAL

- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

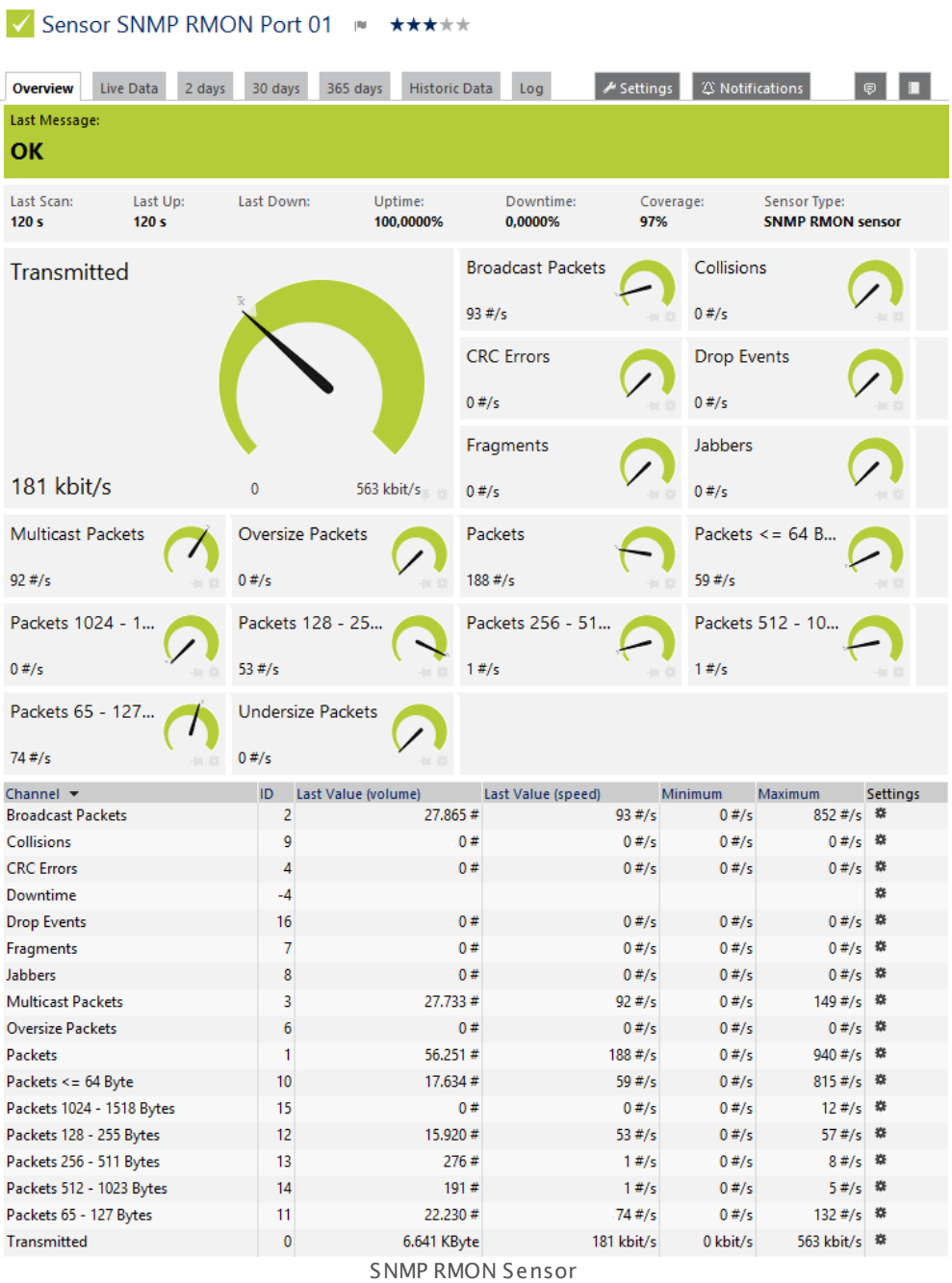
7.8.168 SNMP RMON Sensor

The SNMP RMON sensor monitors traffic on a device using the Remote Monitoring (RMON) standard via Simple Network Management Protocol (SNMP). You can create it on an SNMP compatible device that provides traffic data via RMON. Depending on the data returned by your device, traffic data for each port can be displayed in different channels, allowing detailed analysis. If available, the sensor queries 64-bit counters.

For each port, the sensor can show, for example:

- Transmitted kbit/s
- Packets (#/s)
- Broadcast Packets (#/s)
- Multicast Packets (#/s)
- CRC Errors (#/s)
- Undersize Packets (#/s)
- Oversize Packets (#/s)
- Fragments (#/s)
- Jabbers (#/s)
- Collisions (#/s)
- Packets <= 64 Byte (#/s)
- Packets 65 - 127 Bytes (#/s)
- Packets 128 - 255 Bytes (#/s)
- Packets 256 - 511 Bytes (#/s)
- Packets 512 - 1023 Bytes (#/s)
- Packets 1024 - 1518 Bytes (#/s)
- Drop Events (#/s)

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Channel	ID	Last Value (volume)	Last Value (speed)	Minimum	Maximum	Settings
Broadcast Packets	2	27.865 #	93 #/s	0 #/s	852 #/s	
Collisions	9	0 #	0 #/s	0 #/s	0 #/s	
CRC Errors	4	0 #	0 #/s	0 #/s	0 #/s	
Downtime	-4					
Drop Events	16	0 #	0 #/s	0 #/s	0 #/s	
Fragments	7	0 #	0 #/s	0 #/s	0 #/s	
Jabbers	8	0 #	0 #/s	0 #/s	0 #/s	
Multicast Packets	3	27.733 #	92 #/s	0 #/s	149 #/s	
Oversize Packets	6	0 #	0 #/s	0 #/s	0 #/s	
Packets	1	56.251 #	188 #/s	0 #/s	940 #/s	
Packets <= 64 Byte	10	17.634 #	59 #/s	0 #/s	815 #/s	
Packets 1024 - 1518 Bytes	15	0 #	0 #/s	0 #/s	12 #/s	
Packets 128 - 255 Bytes	12	15.920 #	53 #/s	0 #/s	57 #/s	
Packets 256 - 511 Bytes	13	276 #	1 #/s	0 #/s	8 #/s	
Packets 512 - 1023 Bytes	14	191 #	1 #/s	0 #/s	5 #/s	
Packets 65 - 127 Bytes	11	22.230 #	74 #/s	0 #/s	132 #/s	
Transmitted	0	6.641 KByte	181 kbit/s	0 kbit/s	563 kbit/s	

SNMP RMON Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_rmon.png

Remarks

- You can define the displayed sensor name with port name templates in the **SNMP Compatibility Options** 373 of the parent device.
- It might not work to query data from a probe device via SNMP (querying localhost, 127.0.0.1, or ::1). Add this device to PRTG 275 with the IP address that it has in your network and create the SNMP sensor on this device instead.

- Knowledge Base: What value does the "Transmitted" channel of an RMON sensor show?
- Knowledge Base: How do PRTG's automatic port name and number updates work for SNMP traffic sensors?
- Knowledge Base: Where is the volume line in graphs?
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the ports you want to monitor. PRTG creates one sensor for each port you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

RMON SPECIFIC

Ports	Select the ports you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

RMON SPECIFIC

Port	Shows the number of the interface port in your physical device that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Channel Mask	Describes which channels are available and might be useful for technical support. This setting is shown for your information only and cannot be changed here.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.

SENSOR DISPLAY

	You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how to show different channels for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. You cannot use this option in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782). Manual scaling is not possible if you choose this option. ▪ **Show in and out traffic as positive and negative area chart**: Show channels for incoming and outgoing traffic as positive and negative area chart. This will visualize your traffic in a clear way. You cannot use this option in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782). Manual scaling is not possible if you choose this option. You cannot show a positive/negative chart for a channel if you choose to display its data in percent of maximum (available in the **Sensor Channels Settings** 2782).
Stack Unit	This setting is only available if you choose **Stack channels on top of each other** above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply. If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply. If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: What value does the "Transmitted" channel of an RMON sensor show?

- https://kb.paessler.com/en/topic/59821

Knowledge Base: How do PRTG's automatic port name and number updates work for SNMP traffic sensors?

- https://kb.paessler.com/en/topic/25893

Knowledge Base: Where is the volume line in graphs?

- https://kb.paessler.com/en/topic/61272

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

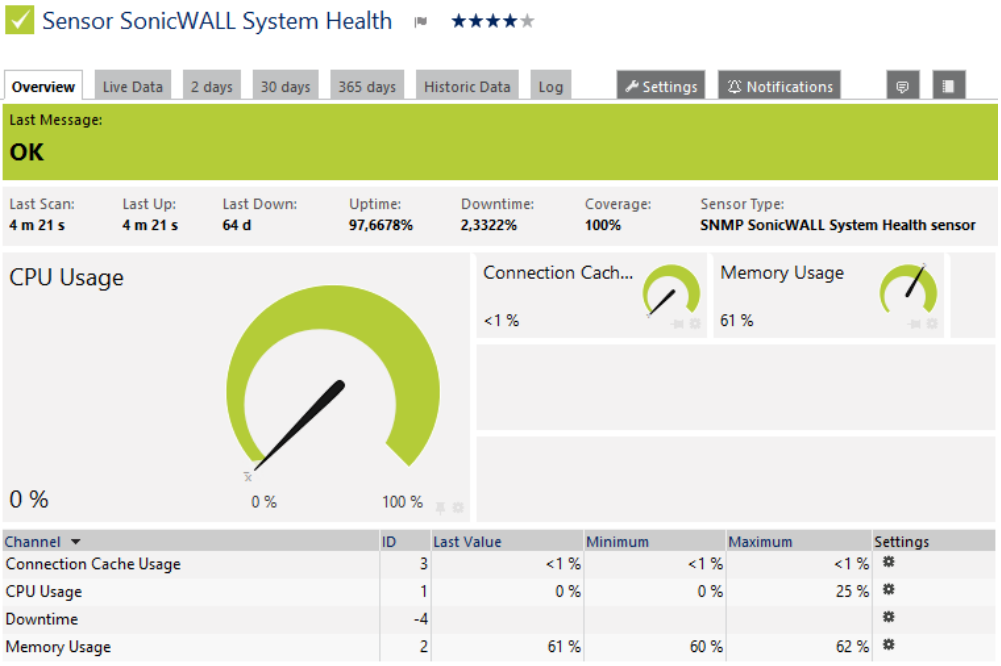
For more general information about settings, please see the **Object Settings** 188 section.

7.8.169 SNMP SonicWALL System Health Sensor

The SNMP SonicWALL System Health sensor monitors health values of a Dell SonicWALL Network Security Appliance (NSA) via Simple Network Management Protocol (SNMP).

It shows the following:

- CPU usage in percent
- Memory usage in percent
- Connection cache usage in percent



SNMP SonicWALL System Health Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_sonicwall_system_health.png

Remarks

- Knowledge Base: Why does PRTG write error messages into my SonicWALL log?
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

SENSOR DISPLAY

Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Knowledge Base: Why does PRTG write error messages into my SonicWALL log?

- https://kb.paessler.com/en/topic/61961

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

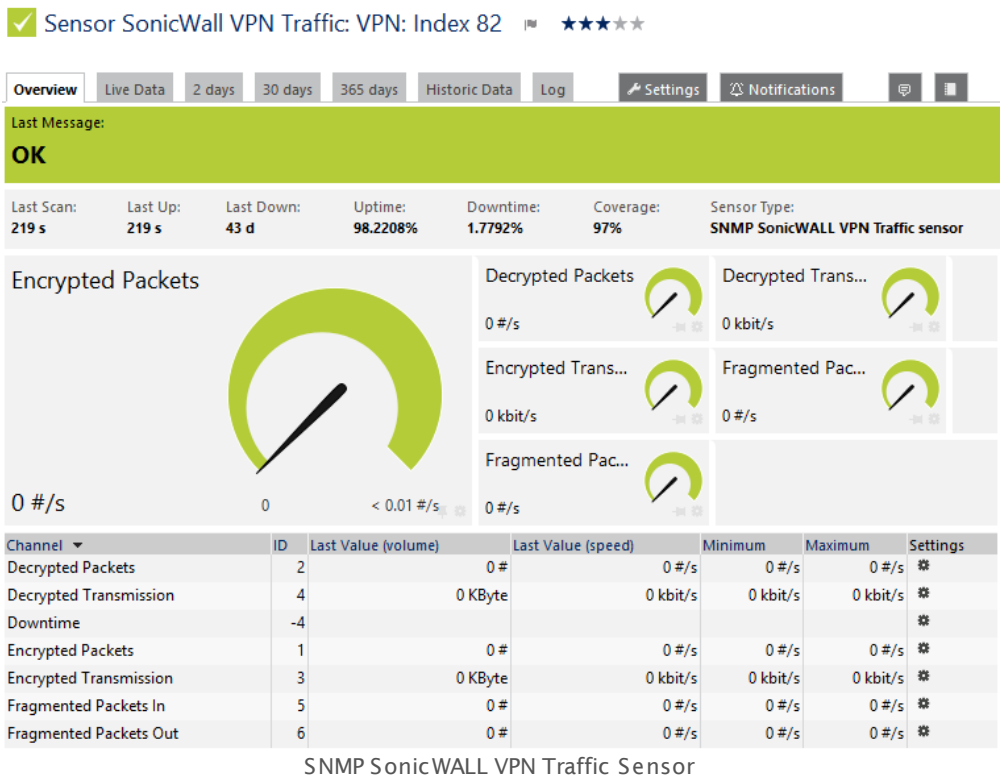
For more general information about settings, please see the **Object Settings** 188 section.

7.8.170 SNMP SonicWALL VPN Traffic Sensor

The SNMP SonicWALL VPN Traffic sensor monitors the traffic of an Internet Protocol Security (IPsec) Virtual Private Network (VPN) on a Dell SonicWALL Network Security Appliance (NSA) via Simple Network Management Protocol (SNMP).

It can show the following:

- Number of encrypted and decrypted packets per second
- Bytes of encrypted and decrypted transmissions per second
- Number of ingoing and outgoing fragmented packets per second



SNMP SonicWALL VPN Traffic Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_sonicwall_vpn_traffic.png

Remarks

- Knowledge Base: Why does PRTG write error messages into my SonicWALL log?
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the connections of the SonicWALL VPN you want to monitor. PRTG will create one sensor for each connection you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SONICWALL VPN SPECIFIC

Connections	Select the connections you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.
Identification Method	Define how you want to identify the connection that you want to monitor. PRTG always uses the first connection found that matches all criteria. Choose between: ▪ **By index**: Every connection has a unique index. This is the safest method to identify your connection. Though, if the connection is lost and reconnected, a new index will be assigned. ▪ **By remote IP**: If the target of the VPN always has the same IP, you can use this IP to identify the connection. ▪ **By security policy name**: If you use a different security policy for every VPN, you can use its name to identify the connection. ▪ **By remote IP and security policy name**: You can also combine both identification methods. ▪ **By remote IP, security policy name, and IP ranges:** If you use separate connections for specific IP ranges, identify the connection by remote IP, security policy name, and IP ranges. ▪ **By IP ranges**: Use IP ranges only to identify the connection.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SONICWALL VPN SPECIFIC

Security Policy Remote IP Source IPs Destination IPs Index	Shows information about the monitored connection. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SONICWALL VPN SPECIFIC

Identification Method

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply. If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply. If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Knowledge Base: Why does PRTG write error messages into my SonicWALL log?

- https://kb.paessler.com/en/topic/61961

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

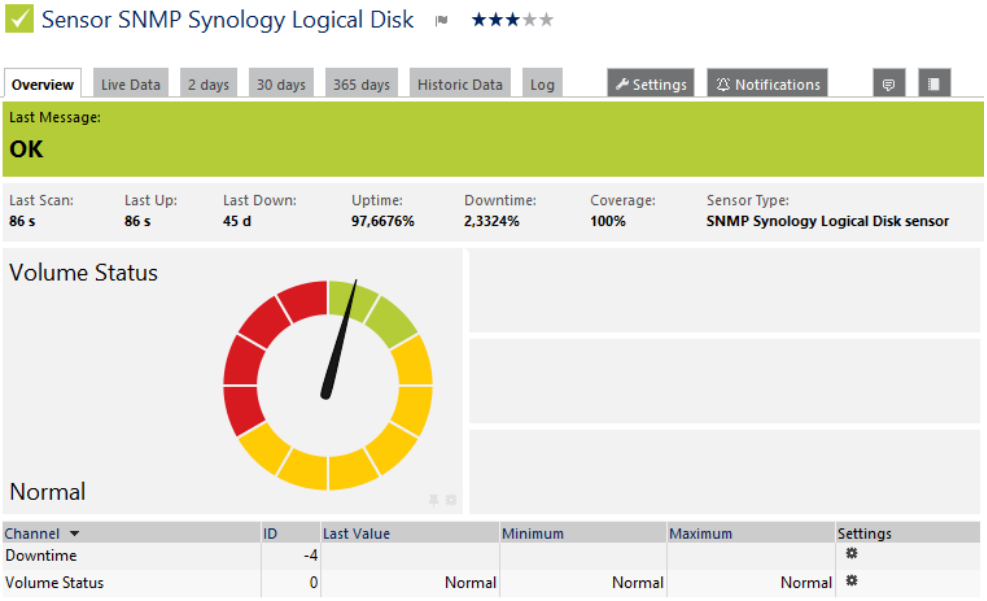
Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.171 SNMP Synology Logical Disk Sensor

The SNMP Synology Logical Disk sensor monitors a logical disk in a Synology Network Attached Storage (NAS) via Simple Network Management Protocol (SNMP).

- It can show the status of a volume.



SNMP Synology Logical Disk Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_synology_logical_disk.png

Remarks

- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the logical disks in the Synology NAS. PRTG creates one sensor for each disk you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SYNOLOGY NAS SETTINGS

Disk	Select the logical disks you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SYNOLOGY NAS SETTINGS

Disk	
Name	Shows further information about the disk that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply. If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply. If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

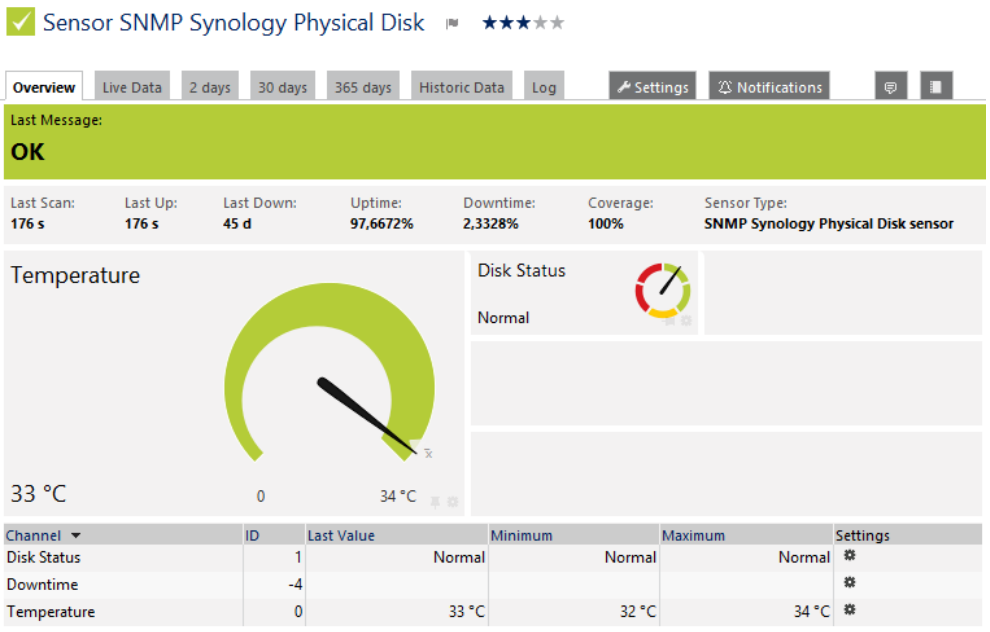
For more general information about settings, please see the **Object Settings** 188 section.

7.8.172 SNMP Synology Physical Disk Sensor

The SNMP Physical Disk sensor monitors a physical disk in a Synology Network Attached Storage (NAS) via Simple Network Management Protocol (SNMP).

It can show the following:

- Temperature
- Disk status



SNMP Synology Physical Disk Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_synology_physical_disk.png

Remarks

- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the physical disks in the Synology NAS you want to monitor. PRTG creates one sensor for each disk you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SYNOLOGY NAS SETTINGS

Disk	Select the physical disks you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.

BASIC SENSOR SETTINGS

Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SYNOLOGY NAS SETTINGS

Disk	
Name	Shows further information about the disk that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Model	
Type	

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

SENSOR DISPLAY

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.

SCANNING INTERVAL

- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.
	Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:
	▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

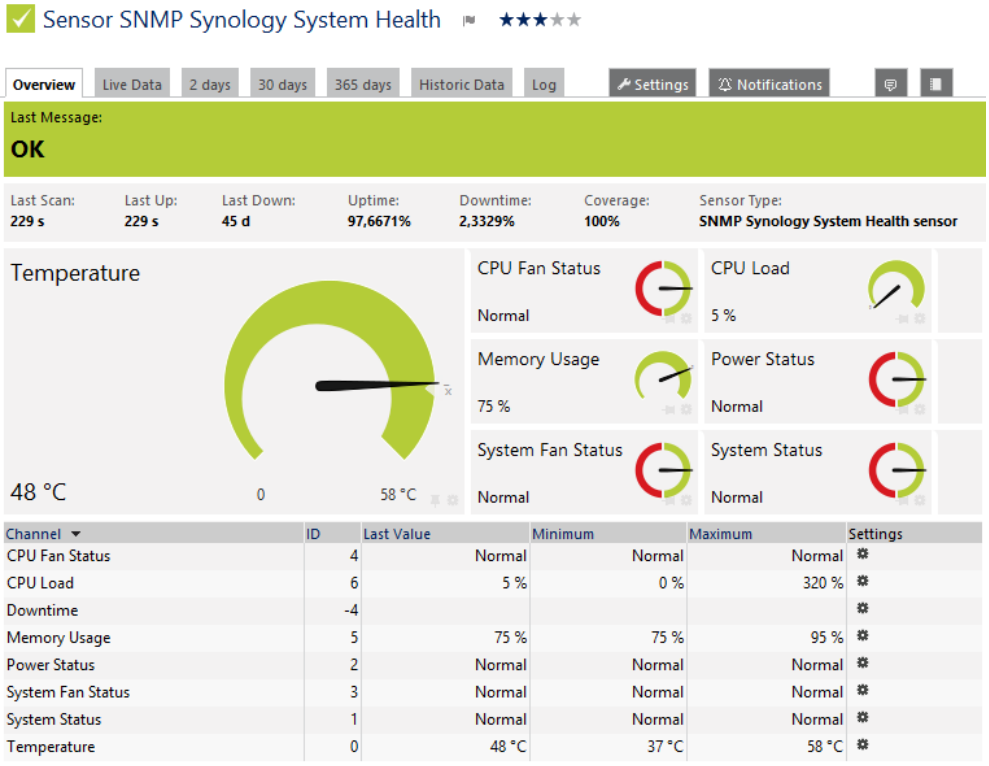
7.8.173 SNMP Synology System Health Sensor

The SNMP Synology System Health sensor monitors the system health of a Synology Network Attached Storage (NAS) via Simple Network Management Protocol (SNMP).

It can show the following, depending on the available measurement components:

- Temperature (if available on the target device)
- System status
- Power status
- Fan status
- Memory usage in percent
- CPU load in percent

Which channels the sensor actually shows might depend on the monitored device and the sensor setup. For more information about the shown memory and CPU load values, please see section More 2122.



Channel	ID	Last Value	Minimum	Maximum	Settings
CPU Fan Status	4	Normal	Normal	Normal	
CPU Load	6	5 %	0 %	320 %	
Downtime	-4				
Memory Usage	5	75 %	75 %	95 %	
Power Status	2	Normal	Normal	Normal	
System Fan Status	3	Normal	Normal	Normal	
System Status	1	Normal	Normal	Normal	
Temperature	0	48 °C	37 °C	58 °C	

SNMP Synology System Health Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_synology_system_health.png

Remarks

- Knowledge Base: Why does my Synology System Health sensor show incorrect CPU and memory values?
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.

BASIC SENSOR SETTINGS

Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply. If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply. If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: Why does my Synology System Health sensor show incorrect CPU and memory values?

- https://kb.paessler.com/en/topic/63283

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

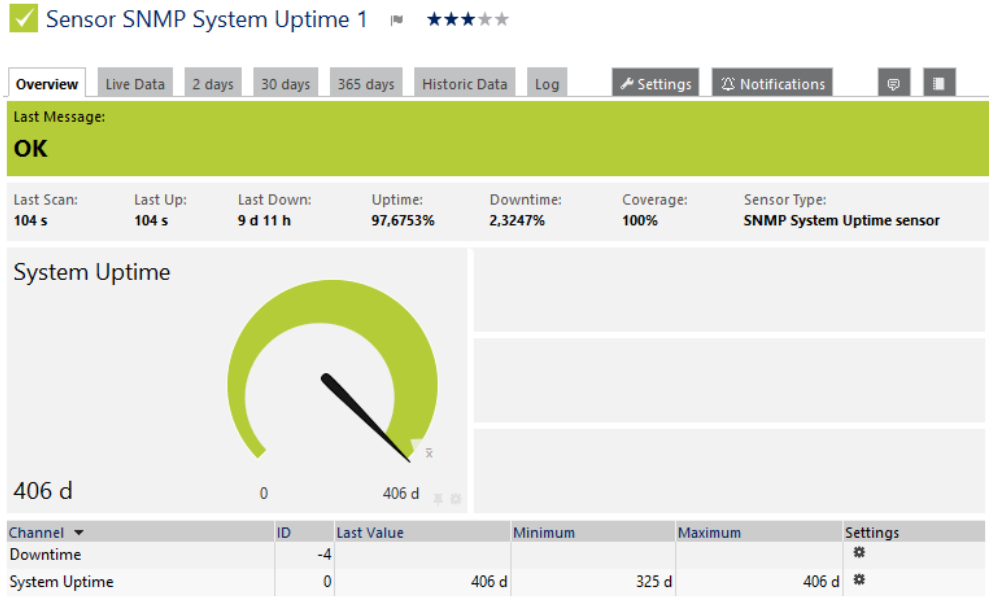
Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.174 SNMP System Uptime Sensor

The SNMP System Uptime sensor monitors the time a device is running via Simple Network Management Protocol (SNMP).

- It reads the system uptime value of the monitored device and shows it.



SNMP System Uptime Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_system_uptime.png

Remarks

- It might not work to query data from a probe device via SNMP (querying localhost, 127.0.0.1, or ::1). Add this device to PRTG 275 with the IP address that it has in your network and create the SNMP sensor on this device instead.
- Knowledge Base: Why does the SNMP System Uptime sensor report wrong values?
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel.

SENSOR DISPLAY

	▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. ⓘ This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.

SCANNING INTERVAL

- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: Why does the SNMP System Uptime sensor report wrong values?

- https://kb.paessler.com/en/topic/61249

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.175 SNMP Traffic Sensor

The SNMP Traffic sensor monitors traffic on a device using Simple Network Management Protocol (SNMP). You can create it on a device that provides traffic data, one traffic sensor for each individual port.

It can show the following:

- Traffic in
- Traffic out
- Traffic total

You can also add additional channels:

- Errors in and out
- Discards in and out
- Unicast packets in and out
- Non unicast packets in and out
- Multicast packets in and out
- Broadcast packets in and out
- Unknown protocols

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

Channel	ID	Last Value (volume)	Last Value (speed)	Minimum	Maximum	Settings
Discards in	12	0 #	0 #/s	0 #/s	0 #/s	
Discards out	13	0 #	0 #/s	0 #/s	0 #/s	
Downtime	-4					
Errors in	10	0 #	0 #/s	0 #/s	1 #/s	
Errors out	11	0 #	0 #/s	0 #/s	0 #/s	
Non-Unicast in	4	0 #	0 #/s	0 #/s	0 #/s	
Non-Unicast out	5	240 #	242 #/s	197 #/s	1.086.175.668 #/s	
Traffic In	0	0 KByte	0 kbit/s	0 kbit/s	901 kbit/s	
Traffic Out	1	27 KByte	221 kbit/s	154 kbit/s	7.023 kbit/s	
Traffic Total	-1	27 KByte	221 kbit/s	0 kbit/s	8.697.330 kbit/s	
Unicast in	2	0 #	0 #/s	0 #/s	0 #/s	
Unicast out	3	2 #	2 #/s	2 #/s	2 #/s	
Unknown protocols in	14	0 #	0 #/s	0 #/s	0 #/s	

SNMP Traffic Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_traffic.png

Remarks

- You can define the displayed sensor name with port name templates in the **SNMP Compatibility Options** 373 of the parent device.
- We recommend that you choose SNMP v2c (most common) or SNMP v3 in the **Credentials for SNMP Devices** 368 of the parent device (if supported by the device that you monitor). SNMP v1 does not support 64-bit counters, which may result in invalid data. For details, please see the Knowledge Base: Querying 64-bit Counters with SNMP Traffic Sensors
- It might not work to query data from a probe device via SNMP (querying localhost, 127.0.0.1, or ::1). Add this device to PRTG 275 with the IP address that it has in your network and create the SNMP sensor on this device instead.

- Knowledge Base: How do PRTG's automatic port name and number updates work for SNMP traffic sensors?
- Knowledge Base: Where is the volume line in graphs?
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the ports on SNMP devices with multiple interfaces you want to monitor. PRTG creates one sensor for each port you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

TRAFFIC SPECIFIC

Interface Number	You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items. You can see the connection status of an interface in the respective table column. You can group-select and deselect interfaces by using the buttons **Select all connected interfaces**, **Select all disconnected interfaces**, and **Deselect all interfaces**.
Description "IN" Channel	For the standard channel "Traffic In", enter the channel name here. The sensor shows it in graphs and tables. You can change this description and the description of all other channels in the sensor channel settings 2782 later.
Description "OUT" Channel	For the standard channel "Traffic Out", enter the channel name here. The sensor shows it in graphs and tables. You can change this description and the description of all other channels in the sensor channel settings 2782 later.
Description "TOTAL" Channel	For the standard channel "Traffic Total" enter the channel name here. The sensor shows it in graphs and tables. You can change this description and the description of all other channels in the sensor channel settings 2782 later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

TRAFFIC SPECIFIC

Interface Number	Shows the number and name of the interface in your physical device that this sensor monitors. This value is shown for reference purposes only. We strongly recommend that you only change it if Paessler support explicitly asks you to do so. Wrong usage can result in incorrect monitoring data!
Additional Channels	By default, the channels "Traffic In", "Traffic Out", and "Traffic Total" are created for each SNMP Traffic sensor. Choose additional channels for all selected interfaces. Click on the respective channel name(s) to mark them and monitor their data. You can choose from the following additional channels: ▪ **Errors In & Out**: The number of in-/outbound packets that could not be delivered because of errors. ▪ **Discards In & Out**: The number of discarded in-/outbound packets even though no errors had been detected. ▪ **Unicast Packets In & Out**: The number of unicast packets that were delivered. ▪ **Non Unicast Packets In & Out (32-bit only)**: The number of non-unicast packets that were delivered. ▪ **Multicast Packets In & Out (64-bit only)**: The number of delivered packets which were addressed to a multicast address. ▪ **Broadcast Packets In & Out (64-bit only)**: The number of delivered packets which were addressed to a broadcast address ▪ **Unknown Protocols**: The number of received packets which were discarded because of an unknown or unsupported protocol. Channels that are once created cannot be deleted later. You can disable them only.
Connection Status Handling	Define how PRTG will react when an interface is operational. A interface which is not operational is, for example, an ethernet port on a switch with no cable plugged in. This setting is valid for all interfaces selected above. You can choose between: ▪ **Show alarm for all "disconnected" states**: The sensor for the interface will always turn into a red error status for a disconnected interface. This applies if the ifOperStatus of the interface is not "up". ▪ **Show alarm when disconnected, but ignore when deactivated**: The sensor will go into an error status for a disconnected interface only if it is not deliberately deactivated in the configuration. This applies if the ifOperStatus of the interface is not "up" **and** the ifAdminStatus is "up". So the sensor will keep the **Up** status when the interface has been deactivated. ▪ **Ignore all "disconnected" states**: The sensor will not show an alarm and its status remains green. Monitoring will be discontinued without notice.
Alias Availability	Shows if an alias is available for automatic port name updates 373. This value is shown for reference purposes only. We strongly

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how to show different channels for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. You cannot use this option in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782). Manual scaling is not possible if you choose this option. ▪ **Show in and out traffic as positive and negative area chart**: Show channels for incoming and outgoing traffic as positive and negative area chart. This will visualize your traffic in a clear way. You cannot use this option in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782). Manual scaling is not possible if you choose this option. You cannot show a positive/negative chart for a channel if you choose to display its data in percent of maximum (available in the **Sensor Channels Settings** 2782).
Stack Unit	This setting is only available if you choose **Stack channels on top of each other** above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply. If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply. If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: How do PRTG's automatic port name and number updates work for SNMP traffic sensors?

- https://kb.paessler.com/en/topic/25893

Knowledge Base: Where is the volume line in graphs?

- https://kb.paessler.com/en/topic/61272

Knowledge Base: Querying 64-bit Counters with SNMP Traffic Sensors

- https://kb.paessler.com/en/topic/67503

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

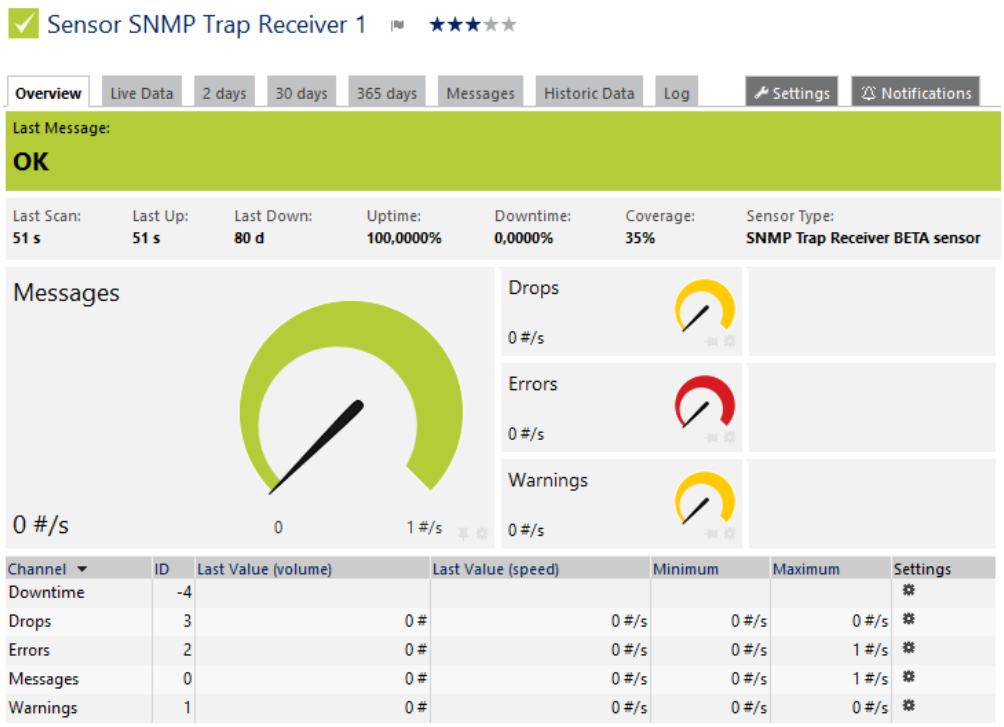
For more general information about settings, please see the **Object Settings** 188 section.

7.8.176 SNMP Trap Receiver Sensor

The SNMP Trap Receiver sensor receives and analyzes Simple Network Management Protocol (SNMP) traps.

It shows the following:

- Overall number of received traps per second
- Trap messages categorized as "warning" per second
- Trap messages categorized as "error" per second
- Number of dropped packets per second
- The actual trap messages



SNMP Trap Receiver Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_trap_receiver.png

Remarks

- With the available filter options, you can define individually which types of messages the sensor will consider for monitoring, and which messages it will categorize as warning or error messages. Depending on the filters, received messages are counted in the respective channels.
- Add the sensor to the probe device to receive all messages of the system running the probe.

- Add the sensor to a specific device to receive all messages from this device directly. This makes this sensor type faster than just using source filters.
- You can use specific placeholders in email notification templates 2921 to see the messages when you receive an email notification. See the Knowledge Base: What placeholders can I use with PRTG?
- Sensor states 163 of this sensor type persist for one scanning interval only. If there is no warning or error message in the following scanning interval, the sensor will show an **up** status again. For a workaround, see this Knowledge Base article: How can I configure sensors using speed limits to keep the status for more than one interval?
- If you do not add the sensor to a probe device but to another device in PRTG, be careful with the configuration: Ensure that the IP address or DNS name of the parent device matches the proper sender. For example, if you want to receive messages from a Storage Area Network (SAN), you might have to add a device to PRTG using the IP address of a specific array member that sends the messages. Providing a DNS name that points to the IP address of a whole group might not work for SANs.
- This sensor type cannot be used in cluster mode. You can set it up on a local probe or remote probe only, not on a cluster probe.
- For a general introduction to the receiver's configuration, please see manual section **Monitoring Syslogs and SNMP Traps** 3125.
- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.
- In PRTG on premises you can copy the Management Information Base (MIB) file for your traps into the **\MIB** subfolder of your PRTG installation 3226 to translate the OIDs for the traps into readable messages.
- This sensor type does not support SNMP v3 traps! Please use SNMP v1 or v2c instead.
- Knowledge Base: How do I test an SNMP Trap Receiver Sensor?
- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

- You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.
- PRTG on demand does not support the import of MIB files. The SNMP Trap Receiver sensor will only consider the MIBs that PRTG includes by default.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SNMP TRAP SPECIFIC

Listen on Port	Enter the number of the port on which the sensor waits for SNMP traps. The default port is **162**. Please enter an integer value. We recommend that you use the default value.
Purge Messages After	Define how long PRTG stores received trap messages for analysis. Choose a period of time from the dropdown list.

FILTER

Include Filter	Define if you want to filter traps. If you leave this field empty or use the keyword "any", the sensor will process all data. This is the default setting. To include specific types of traps only, define filters using a special syntax. For more information, see section **Filter Rules** 2152.
Exclude Filter	Define which types of traps the sensor will discard and not process. To exclude specific types of traps, define filters using a special syntax. For more information, see section **Filter Rules** 2152.
Warning Filter	Define which types of traps count for the **Warnings** channel. To categorize received traps as warning messages, define filters using a special syntax. For more information, see section **Filter Rules** 2152. Messages are collected until a scanning interval ends. As long as the scanning interval is running, no status change will happen. By default, the sensor will turn into a **Warning** status after a scanning interval has finished and there was at least one warning message (and no error message) during this interval. The status will remain **Warning** at least until the succeeding scanning interval has finished. If the sensor did not receive any warning or error message in this scanning interval, its status will turn **Up** again after the interval.
Error Filter	Define which types of traps count for the **Errors** channel. To categorize received traps as error messages, define filters using a special syntax. For more information, see section **Filter Rules** 2152. Messages are collected until a scanning interval ends. As long as the scanning interval is running, no status change will happen. By default, the sensor will turn into a **Down** status after a scanning interval has finished and there was at least one error message during this interval. The status will remain **Down** at least until the succeeding scanning interval has finished. If the sensor did not receive any warning or error message in this scanning interval, its status will turn **Up** again after the interval.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

SENSOR DISPLAY

Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

DEBUGGING

Log Data to Disk	Define if the probe will write a log file of the received data to the data folder (see **Data Storage** 3226) to the disk for debugging purposes. Choose between: ▪ **Off (recommended)**: Do not write additional log files. Recommended for normal use cases. ▪ **On**: Write log files for all data received. ⚠ Use with caution! When enabled, huge data files can be created. Please use for a short time and for debugging purposes only.

Filter Rules for Traps

Filter rules are used for the include, exclude, warning, and error definition fields of the Trap Receiver sensor. They are based on the following format:

```
field[filter]
```

You can use various filters suitable to your needs. Include and exclude filters define which traps to monitored. Warning and error filters define how to categorize received traps. Provide these filters in the sensor settings as formulas. Formulas are fields which you can combine with boolean operators (AND, OR, NOT) and brackets.

Field	Parameter	Examples
source[ip]	Enter an IP address where the UDPs come from; IP masks and ranges 3182 are also possible.	source[10.0.23.50], source[10.0.23.10-50], source[10.0.23.10/255]
agent[ip]	Enter an IP address which specifies the object that creates the SNMP trap. Only v1 is supported.	agent[10.0.0.1]
enterprise[oid]	Enter an OID which specifies the object that originates the trap. Only v1 is supported.	enterprise[1.3.6.1.4.1.2.6.182.1.2.3 1.1.0]
bindings[text]	Enter a substring to match all OIDs and values in the bindings.	bindings[ERROR], bindings[1.3.6.1.4.1.2.6.182.1.2.3 1.1.0]
bindings[oid,value]	Enter an OID and a substring to match a value in the given OID. Separate OID and value with a comma.	bindings[1.3.6.1.4.1.2.6.182.1.2.3 1.1.0,error]
gentrap[number]	Enter a number which specifies the generic trap type. Ranges are also possible.	gentrap[3], gentrap[2-6]

spectrap [number]	Enter a number which defines the specific trap code. Ranges are also possible.	spectrap[4], spectrap[0-3]
version [number]	Enter a number (**1** or **2**) which specifies the SNMP version.	version[1], version[2]
community [text]	Enter a community string for exact, case sensitive match.	community[public], community[private]

Messages Tab: Review and Analyze Traps

PRTG stores received traps as common files in the data folder (see section **Data Storage** 3226). To review and analyze all received messages, you can access the most recent data directly in a table list 207 in the PRTG web interface. You can access this list via the **Overview** tab of the sensors.

Received traps are only shown after an (automatic) page refresh following to a sensor scan in the table on the **Overview** tab (default for auto refresh 2909 is 30 seconds).

For more details and further filter options, click the **Messages** tab of the SNMP Trap Receiver sensor. You will see all received messages in a table list 207. On the top, you have display filter options to drill down into the data for specific events of your interest. The filters are the same as available in the sensor settings, but you can define them without using formulas. Provide the desired parameters and PRTG loads the filtered list automatically.

You can automatically add a filter by clicking the content of a column.

Advanced Filter Settings

You can open advanced filter settings with by clicking the gear icon in the **Filter** row. The **Advanced Filter** will appear in a popup window. In the text field, you can define a filter using the syntax as given in section **Filter Rules for Traps** 2152. If you have provided filter parameters on the **Messages** tab, the advanced filter will already include them as a corresponding formula with the correct syntax. You can adjust this filter to your needs. You can also copy the automatically created and manually adjusted formula for usage in the filter fields of the sensor settings.

More

Video Tutorial: How to Set Up an SNMP Trap Receiver Sensor in PRTG

- https://www.paessler.com/support/videos/prtg-advanced/snmp-trap-receiver

Knowledge Base: How can I configure sensors using speed limits to keep the status for more than one interval?

- https://kb.paessler.com/en/topic/73212

Knowledge Base: How do I test an SNMP Trap Receiver Sensor?

- https://kb.paessler.com/en/topic/10193

Knowledge Base: What placeholders can I use with PRTG?

- https://kb.paessler.com/en/topic/373

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

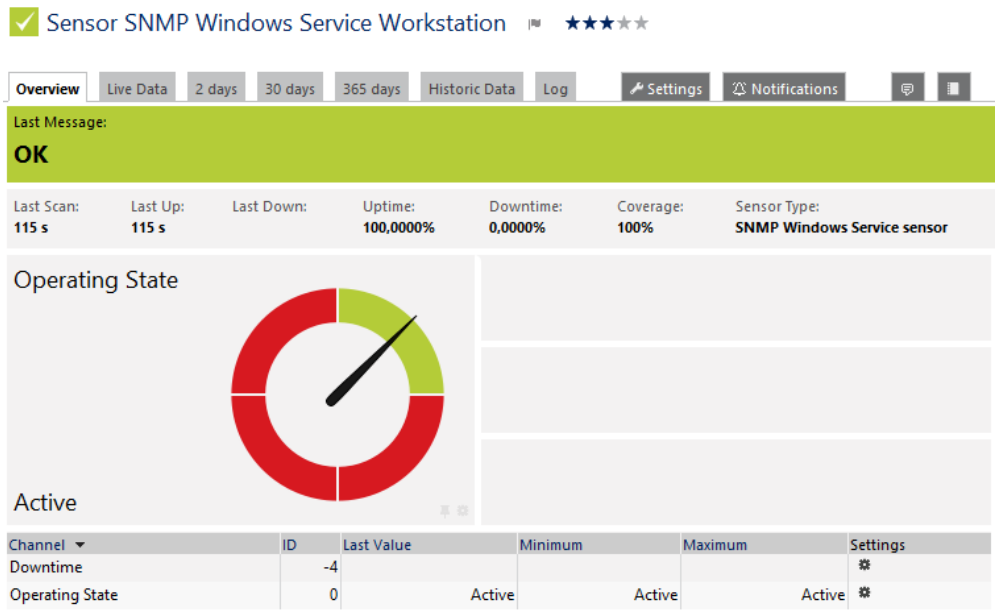
7.8.177 SNMP Windows Service Sensor

The SNMP Windows Service sensor monitors a Windows service via Simple Network Management Protocol (SNMP).

- It shows the operating status of the monitored service.

Operating states can be:

- Active (sensor status 163 **Up**)
- Continue-Pending
- Pause-Pending
- Paused (all with sensor status **Down**)



SNMP Windows Service

Click here to enlarge: http://media.paessler.com/prtg-screenshots/snmp_windows_service.png

Remarks

- This sensor type cannot distinguish the status "not installed" from "not running".
- It might not work to query data from a probe device via SNMP (querying localhost, 127.0.0.1, or ::1). Add this device to PRTG 275 with the IP address that it has in your network and create the SNMP sensor on this device instead.
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.

- For a general introduction to the technology behind SNMP, please see the manual section **Monitoring via SNMP** 3087.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the Windows services you want to monitor. PRTG creates one sensor for each service you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SNMP WINDOWS SERVICE MONITOR

Service	Select the services you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	Enter one or more **Tags**, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SNMP WINDOWS SERVICE MONITOR

Service	Shows the Windows service that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. ⓘ You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel.

SENSOR DISPLAY

	▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. ⓘ This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.

SCANNING INTERVAL

- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

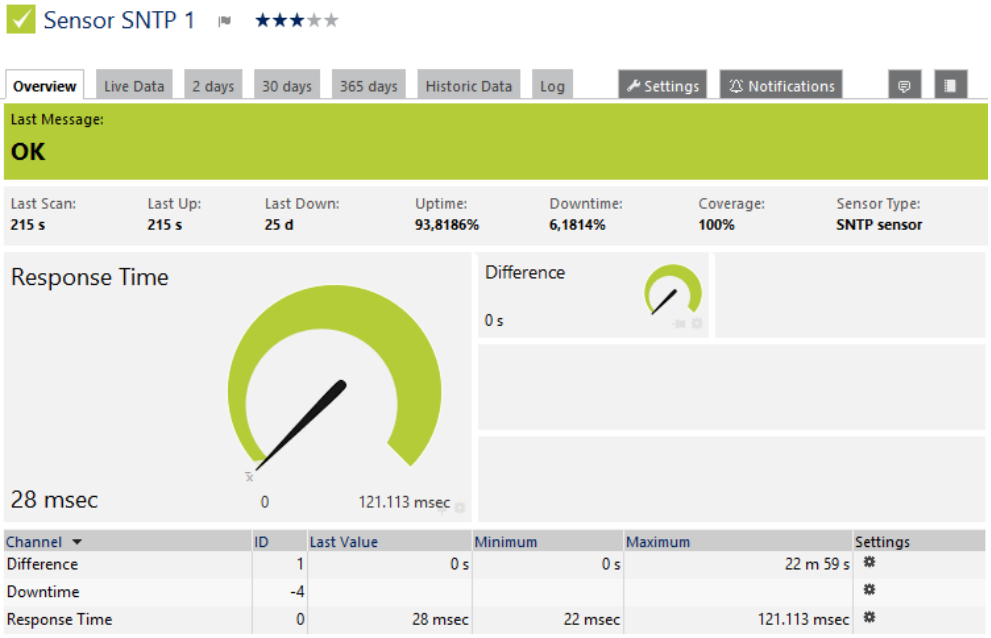
7.8.178 SNTP Sensor

The SNTP Sensor monitors a Simple Network Time Protocol (SNTP) server.

It shows the following:

- Response time of the server
- Time difference in comparison to the local system time

The sensor tries to get a valid timestamp from the server up to three times per scan until it reports an error.



SNTP Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/sntp.png

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SPECIFC

Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

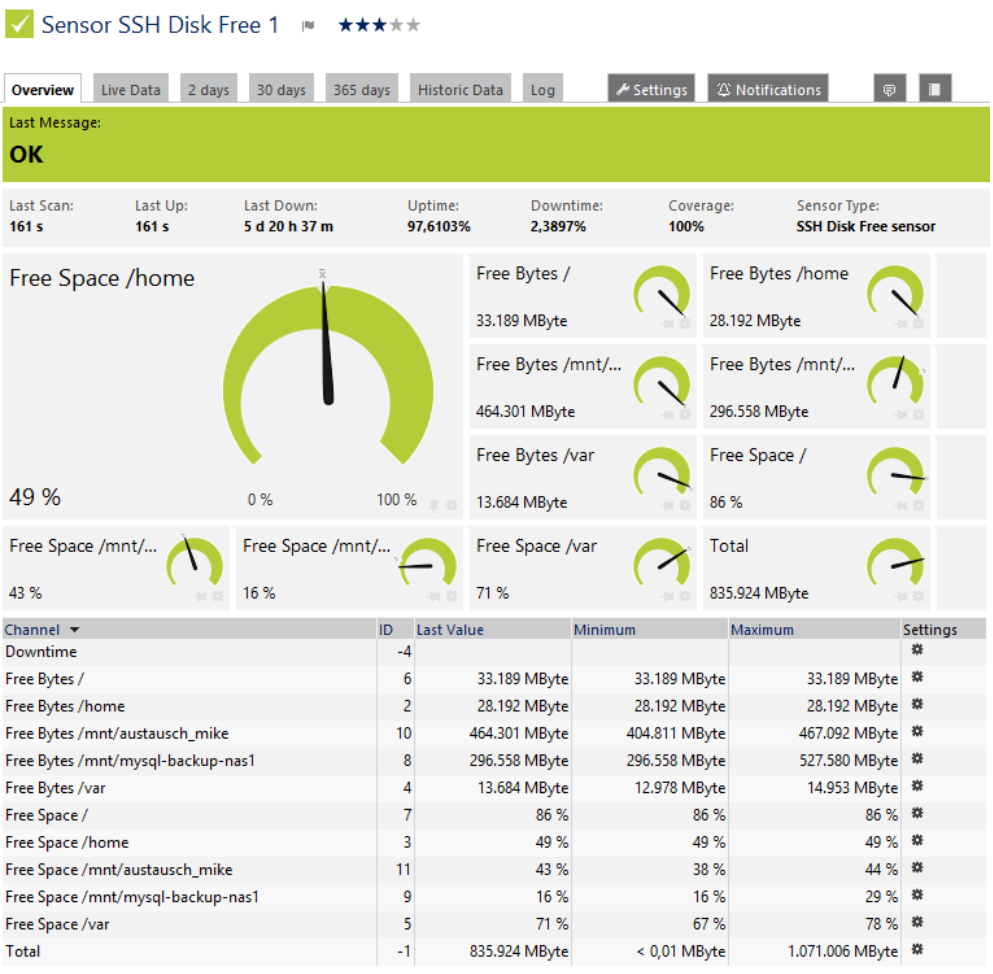
7.8.179 SSH Disk Free Sensor

The SSH Disk Free sensor monitors free space on disks of a Linux/Unix system using Secure Shell (SSH).

It shows the following:

- Free disk space in bytes for every mounted partition
- Free disk space in percent for every mounted partition
- Total disk space

The free space returned by this sensor type shows the available disk space of the volume, minus a reserve defined for this volume (for example, for redundancy purposes). So, this sensor shows the disk space that is actually available for use. The size of the reserved disk space can be defined with tune2fs. For details, please see the **More** 2182 section below.



SSH Disk Free Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/ssh_disk_free.png

Remarks

- For this sensor type you must define credentials for Linux/Solaris/Mac OS (SSH/WBEM) systems on the device you want to use the sensor on.
- This sensor type cannot support all Linux/Unix and Mac OS distributions.
- For a general introduction to SSH monitoring, please see manual section **Monitoring via SSH** 3095.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the disk(s) you want to monitor. PRTG will create two sensor channels (free space in percent and bytes) for each partition you choose in the **Add Sensor** dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SSH DISK FREE

Disk	Select the partitions that you want to monitor. You see a list with the names of all items that are available to monitor. Select the desired items by adding check marks in front of the respective lines. PRTG creates two channels for each selection. You can also select and deselect all items by using the check box in the table head. You can select up to 100 disks. If you select more disks, you will not be able to create the sensor. Add the sensor multiple times to monitor more than 100 disks with several sensors.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SSH SPECIFIC

Connection Timeout (Sec.)	Define a timeout in seconds for the connection. This is the time the sensor will wait to establish a connection to the host. Keep this value as low as possible. The maximum value is **900** seconds (15 minutes). Please enter an integer value.
Shell Timeout (Sec.)	Define a timeout in seconds for the shell response. This is the time in seconds the sensor will wait for the shell to return a response after it has sent its specific command (for example, cat /proc/loadavg). The maximum value is **300** seconds (5 minutes). Please enter an integer value.
SSH Port	Define which port this sensor uses for the SSH connection. Choose between: ▪ **Inherit port number from parent device (default)**: Use the port number as defined in the **Credentials for Linux/Solaris/Mac OS (SSH/WBEM) Systems** 365 section of the device this sensor is created on.

SSH SPECIFIC

- **Enter custom port number**: Define a custom port number below and do not use the port number from the parent device settings.

Use Port Number

This field is only visible if you choose **Enter custom port number** above. Enter the port number (between 1 and 65535) that this sensor will use for the SSH connection. Please enter an integer value.

SSH Engine

Select the method you want to use to access data with this SSH sensor [3095]. We strongly recommend that you use the default engine! For some time you still can use the legacy mode to ensure compatibility with your target systems. Choose between:

- **Inherit from parent device (default)**: Use the SSH engine that you have defined in the parent device settings or higher in the object hierarchy [118]. If you did not change it, this is the recommended default engine.
- **Default**: This is the default monitoring method for SSH sensors. It provides best performance and security. It is set by default in objects that are higher in the hierarchy so usually you can keep the **Inherit from parent device (default)** option.
- **Compatibility Mode (deprecated)**: Try this legacy method only if the default mode does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions and is deprecated. We will remove this legacy option soon, so please try to get your SSH sensors running with the default SSH engine.

The option you select here overrides the selection of the SSH engine in a higher object (which is a parent device, group, probe, or root).

Result Handling

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result**: Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section **Data Storage** [3226].

SSH SPECIFIC

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt") in case of error**: Store the last result of the sensor only if it throws an error.

SET LIMITS CHECKED AGAINST ALL DISKS

In this section you can set limits that are valid for all channels and all drives. By entering limits, you can define when the sensor will enter a **Warning** or **Down** status, depending on the data provided by all drives that this sensor monitors. If you want to define limits for separate channels individually, please use the limit settings in the sensor **Channel** settings.

All limits that you define here are valid in addition to the limits defined in the particular **Channels** settings! The limits are valid simultaneously, so the first limit that is breached applies.

Percentage Limit Check	Enable or disable a limit check for the free space in percentage channels of all drives. By default, percentage limits are enabled with lower warning and lower error limit. Choose between: ▪ **Only use the limits in the settings of the percentage channels**: Do not define sensor limits which are valid for all percentage channels. The sensor only uses limits which you define in the settings of the particular "free space in percent" channels to determine the status. ▪ **Use the limits of both the sensor and the channel settings**: Define limits for the sensor which are valid for all drives (percentage channels). Additional fields appear below. The sensor enters a **Warning** or **Down** status when free space limits are undercut or overrun.
Upper Error Limit	This field is only visible if you enable percentage limit check above. Specify an upper limit in percent for a **Down** status. If the free disk space of one of your drives overruns this percent value, the sensor switches to **Down**. Please enter an integer value or leave the field empty. The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the **Sensor Channels Settings** 2782. The limits set here and in the channel settings are valid simultaneously!

SET LIMITS CHECKED AGAINST ALL DISKS

Upper Warning Limit	This field is only visible if you enable percentage limit check above. Specify an upper limit in percent for a **Warning** status. If the free disk space of one of your drives overruns this percent value, the sensor switches to **Warning**. Please enter an integer value or leave the field empty. The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the **Sensor Channels Settings** 2782. The limits set here and in the channel settings are valid simultaneously!
Lower Warning Limit	This field is only visible if you enable percentage limit check above. Specify a lower limit in percent for a **Warning** status. If the free disk space of one of your drives undercuts this percent value, the sensor switches to warning. Please enter an integer value or leave the field empty. The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the **Sensor Channels Settings** 2782. The limits set here and in the channel settings are valid simultaneously!
Lower Error Limit	This field is only visible if you enable percentage limit check above. Specify a lower limit in percent for a **Down** status. If the free disk space of one of your drives undercuts this percent value, the sensor switches to **Down**. Please enter an integer value or leave the field empty. The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the **Sensor Channels Settings** 2782. The limits set here and in the channel settings are valid simultaneously!
Size Limit Check	Enable or disable a limit check for the free bytes channels of all drives. By default, byte size limits are not enabled for drives. Choose between: • **Only use the limits in the settings of the byte size channels**: Do not define sensor limits which are valid for all byte size channels. The sensor only uses limits which you define in the settings of the particular free space in bytes channels to determine the status. • **Use the limits of both the sensor and the channel settings**: Define limits for the sensor which are valid for all drives (byte size channels). Additional fields appear below. The sensor enters a **Warning** or **Down** status when free space limits are undercut or overrun.

SET LIMITS CHECKED AGAINST ALL DISKS

Upper Error Limit	This field is only visible if you enable byte limit check above. Specify an upper limit. Use the same unit as shown by the free bytes channels of this sensor (by default this is MByte). If the free disk space of one of your drives overruns this bytes value, the sensor switches to **Down**. Please enter an integer value or leave the field empty. The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the **Sensor Channels Settings** 2782. The limits set here and in the channel settings are valid simultaneously!
Upper Warning Limit	This field is only visible if you enable byte limit check above. Specify an upper limit. Use the same unit as shown by the free bytes channels of this sensor (by default this is MByte). If the free disk space of one of your drives overruns this bytes value, the sensor switches to **Warning**. Please enter an integer value or leave the field empty. The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the **Sensor Channels Settings** 2782. The limits set here and in the channel settings are valid simultaneously!
Lower Warning Limit	This field is only visible if you enable byte limit check above. Specify a lower limit. Use the same unit as shown by the free bytes channels of this sensor (by default this is MByte). If the free disk space of one of your drives undercuts this bytes value, the sensor switches to **Warning**. Please enter an integer value or leave the field empty. The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the **Sensor Channels Settings** 2782. The limits set here and in the channel settings are valid simultaneously!
Lower Error Limit	This field is only visible if you enable byte limit check above. Specify a lower limit. Use the same unit as shown by the free bytes channels of this sensor (by default this is MByte). If the free disk space of one of your drives undercuts this bytes value, the sensor switches to **Down**. Please enter an integer value or leave the field empty. The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the **Sensor Channels Settings** 2782. The limits set here and in the channel settings are valid simultaneously!
Alarm on Missing/ Removed Disk	If a monitored disk is removed or not found, values are set to zero. Select the alarming approach in this case. Choose between:

SET LIMITS CHECKED AGAINST ALL DISKS

- **Deactivate alarm (default)**: Select this option if you do not want an alarm for a removed disk.
- **Activate alarm**: Select this option if you want to be alerted if a monitored disk is removed.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply. If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply. If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: How and Where Does PRTG Store its Data?

- https://kb.paessler.com/en/topic/463

Knowledge Base: Why do SSH Disk Free and SNMP Linux Disk Free show different values for my target Linux system?

- https://kb.paessler.com/en/topic/43183

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

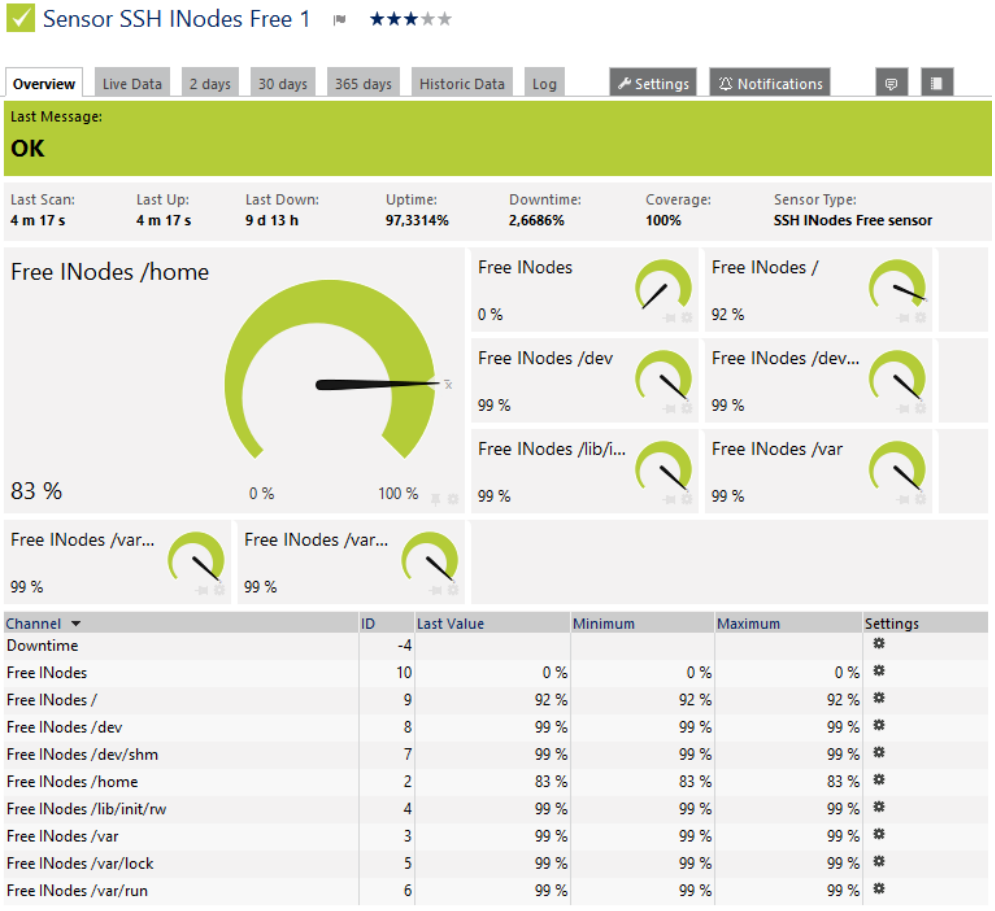
For more general information about settings, please see the **Object Settings** 188 section.

7.8.180 SSH INodes Free Sensor

The SSH INodes Free sensor monitors the free index nodes on disks of Linux/Unix and Mac OS systems via Secure Shell (SSH).

- It shows free index nodes in percent, for each mount in an own sensor channel.

UNIX file systems only allow a limited number of index nodes. If the limit is exceeded, no more data can be stored, although there might still be free space available. This sensor can help you to notice early on if one of your drives is running out of INodes.



SSH INodes Free Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/ssh_inodes_free.png

Remarks

- For this sensor type you must define credentials for Linux/Solaris/Mac OS (SSH/WBEM) systems on the device you want to use the sensor on.
- This sensor type cannot support all Linux/Unix and Mac OS distributions.
- For a general introduction to SSH monitoring, please see manual section **Monitoring via SSH** 3095.

- This sensor type does not support ESX(i) hosts.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SSH SPECIFIC

Connection Timeout (Sec.)	Define a timeout in seconds for the connection. This is the time the sensor will wait to establish a connection to the host. Keep this value as low as possible. The maximum value is **900** seconds (15 minutes). Please enter an integer value.
Shell Timeout (Sec.)	Define a timeout in seconds for the shell response. This is the time in seconds the sensor will wait for the shell to return a response after it has sent its specific command (for example, cat /proc/loadavg). The maximum value is **300** seconds (5 minutes). Please enter an integer value.
SSH Port	Define which port this sensor uses for the SSH connection. Choose between: ▪ **Inherit port number from parent device (default)**: Use the port number as defined in the **Credentials for Linux/Solaris/Mac OS (SSH/WBEM) Systems** 365 section of the device this sensor is created on. ▪ **Enter custom port number**: Define a custom port number below and do not use the port number from the parent device settings.
Use Port Number	This field is only visible if you choose **Enter custom port number** above. Enter the port number (between 1 and 65535) that this sensor will use for the SSH connection. Please enter an integer value.
SSH Engine	Select the method you want to use to access data with this SSH sensor 3095. We strongly recommend that you use the default engine! For some time you still can use the legacy mode to ensure compatibility with your target systems. Choose between: ▪ **Inherit from parent device (default)**: Use the SSH engine that you have defined in the parent device settings or higher in the object hierarchy 118. If you did not change it, this is the recommended default engine. ▪ **Default**: This is the default monitoring method for SSH sensors. It provides best performance and security. It is set by default in objects that are higher in the hierarchy so usually you can keep the **Inherit from parent device (default)** option. ▪ **Compatibility Mode (deprecated)**: Try this legacy method only if the default mode does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions and is deprecated. We will remove this legacy option soon, so please try to get your SSH sensors running with the default SSH engine.

SSH SPECIFIC

The option you select here overrides the selection of the SSH engine in a higher object (which is a parent device, group, probe, or root).

Result Handling

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result**: Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section Data Storage 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt") in case of error**: Store the last result of the sensor only if it throws an error.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.

SCANNING INTERVAL

- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. ⓘ To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: How and Where Does PRTG Store its Data?

- https://kb.paessler.com/en/topic/463

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

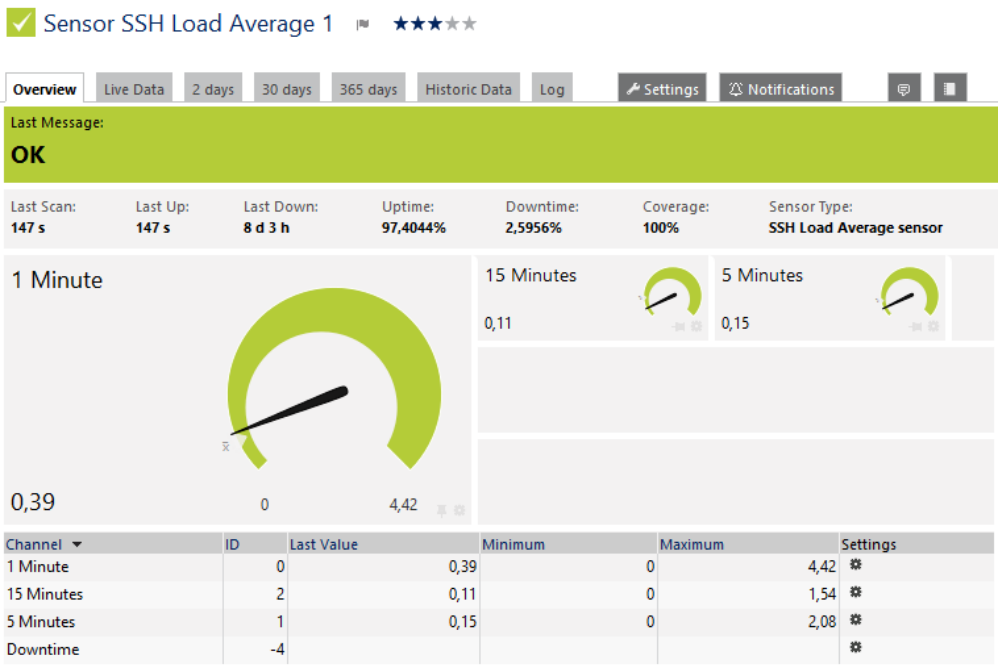
For more general information about settings, please see the **Object Settings** 188 section.

7.8.181 SSH Load Average Sensor

The SSH Load Average sensor monitors the load average of a Linux/Unix system using Secure Shell (SSH).

It shows the following:

- Average system load within a 1-minute interval
- Average system load within a 5-minute interval
- Average system load within a 15-minute interval



SSH Load Average Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/ssh_load_average.png

Remarks

- For this sensor type you must define credentials for Linux/Solaris/Mac OS (SSH/WBEM) systems on the device you want to use the sensor on.
- This sensor type cannot support all Linux/Unix and Mac OS distributions.
- For a general introduction to SSH monitoring, please see manual section **Monitoring via SSH** 3095.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SSH SPECIFIC

Connection Timeout (Sec.)	Define a timeout in seconds for the connection. This is the time the sensor will wait to establish a connection to the host. Keep this value as low as possible. The maximum value is **900** seconds (15 minutes). Please enter an integer value.
Shell Timeout (Sec.)	Define a timeout in seconds for the shell response. This is the time in seconds the sensor will wait for the shell to return a response after it has sent its specific command (for example, cat /proc/loadavg). The maximum value is **300** seconds (5 minutes). Please enter an integer value.
SSH Port	Define which port this sensor uses for the SSH connection. Choose between: ▪ **Inherit port number from parent device (default)**: Use the port number as defined in the **Credentials for Linux/Solaris/Mac OS (SSH/WBEM) Systems** 365 section of the device this sensor is created on. ▪ **Enter custom port number**: Define a custom port number below and do not use the port number from the parent device settings.
Use Port Number	This field is only visible if you choose **Enter custom port number** above. Enter the port number (between 1 and 65535) that this sensor will use for the SSH connection. Please enter an integer value.
SSH Engine	Select the method you want to use to access data with this SSH sensor 3095. We strongly recommend that you use the default engine! For some time you still can use the legacy mode to ensure compatibility with your target systems. Choose between: ▪ **Inherit from parent device (default)**: Use the SSH engine that you have defined in the parent device settings or higher in the object hierarchy 118. If you did not change it, this is the recommended default engine. ▪ **Default**: This is the default monitoring method for SSH sensors. It provides best performance and security. It is set by default in objects that are higher in the hierarchy so usually you can keep the **Inherit from parent device (default)** option. ▪ **Compatibility Mode (deprecated)**: Try this legacy method only if the default mode does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions and is deprecated. We will remove this legacy option soon, so please try to get your SSH sensors running with the default SSH engine.

SSH SPECIFIC

The option you select here overrides the selection of the SSH engine in a higher object (which is a parent device, group, probe, or root).

Result Handling

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result**: Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section Data Storage 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt") in case of error**: Store the last result of the sensor only if it throws an error.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.

SCANNING INTERVAL

- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: How and Where Does PRTG Store its Data?

- https://kb.paessler.com/en/topic/463

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

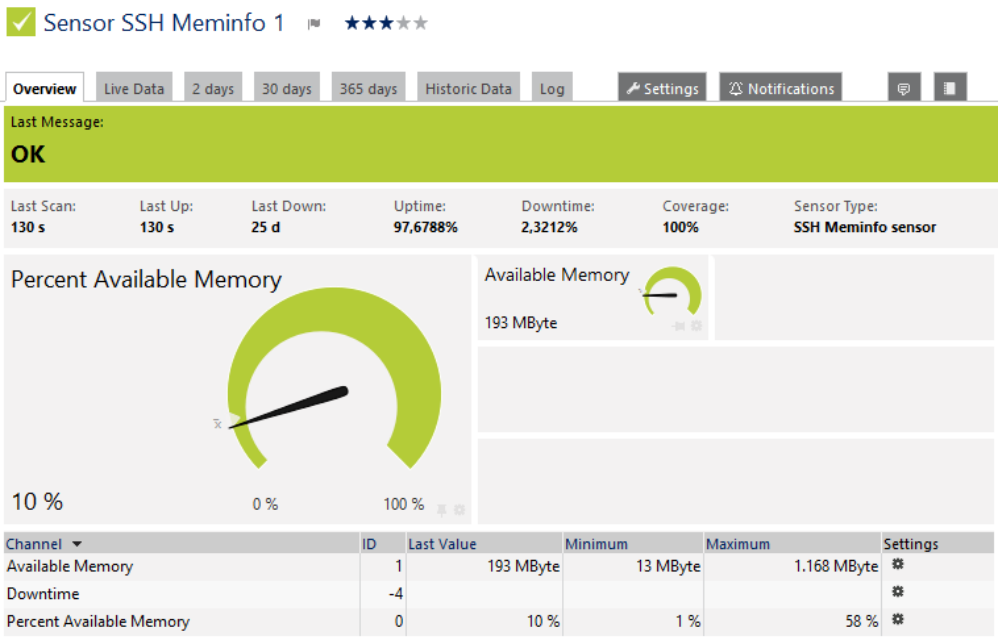
For more general information about settings, please see the **Object Settings** 188 section.

7.8.182 SSH Meminfo Sensor

The SSH Meminfo sensor monitors the memory usage of a Linux/Unix system using Secure Shell (SSH).

It shows the following:

- Available memory in bytes
- Available memory in percent



SSH Meminfo Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/ssh_meminfo.png

Remarks

- For this sensor type you must define credentials for Linux/Solaris/Mac OS (SSH/WBEM) systems on the device you want to use the sensor on.
- This sensor type cannot support all Linux/Unix and Mac OS distributions.
- For a general introduction to SSH monitoring, please see manual section **Monitoring via SSH** 3095.
- This sensor type is not compatible with Mac OS systems.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SSH SPECIFIC

Connection Timeout (Sec.)	Define a timeout in seconds for the connection. This is the time the sensor will wait to establish a connection to the host. Keep this value as low as possible. The maximum value is **900** seconds (15 minutes). Please enter an integer value.
Shell Timeout (Sec.)	Define a timeout in seconds for the shell response. This is the time in seconds the sensor will wait for the shell to return a response after it has sent its specific command (for example, cat /proc/loadavg). The maximum value is **300** seconds (5 minutes). Please enter an integer value.
SSH Port	Define which port this sensor uses for the SSH connection. Choose between: ▪ **Inherit port number from parent device (default)**: Use the port number as defined in the **Credentials for Linux/Solaris/Mac OS (SSH/WBEM) Systems** 365 section of the device this sensor is created on. ▪ **Enter custom port number**: Define a custom port number below and do not use the port number from the parent device settings.
Use Port Number	This field is only visible if you choose **Enter custom port number** above. Enter the port number (between 1 and 65535) that this sensor will use for the SSH connection. Please enter an integer value.
SSH Engine	Select the method you want to use to access data with this SSH sensor 3095. We strongly recommend that you use the default engine! For some time you still can use the legacy mode to ensure compatibility with your target systems. Choose between: ▪ **Inherit from parent device (default)**: Use the SSH engine that you have defined in the parent device settings or higher in the object hierarchy 118. If you did not change it, this is the recommended default engine. ▪ **Default**: This is the default monitoring method for SSH sensors. It provides best performance and security. It is set by default in objects that are higher in the hierarchy so usually you can keep the **Inherit from parent device (default)** option. ▪ **Compatibility Mode (deprecated)**: Try this legacy method only if the default mode does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions and is deprecated. We will remove this legacy option soon, so please try to get your SSH sensors running with the default SSH engine.

SSH SPECIFIC

The option you select here overrides the selection of the SSH engine in a higher object (which is a parent device, group, probe, or root).

Result Handling

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result**: Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section Data Storage 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt") in case of error**: Store the last result of the sensor only if it throws an error.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.

SCANNING INTERVAL

- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: How and Where Does PRTG Store its Data?

- https://kb.paessler.com/en/topic/463

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

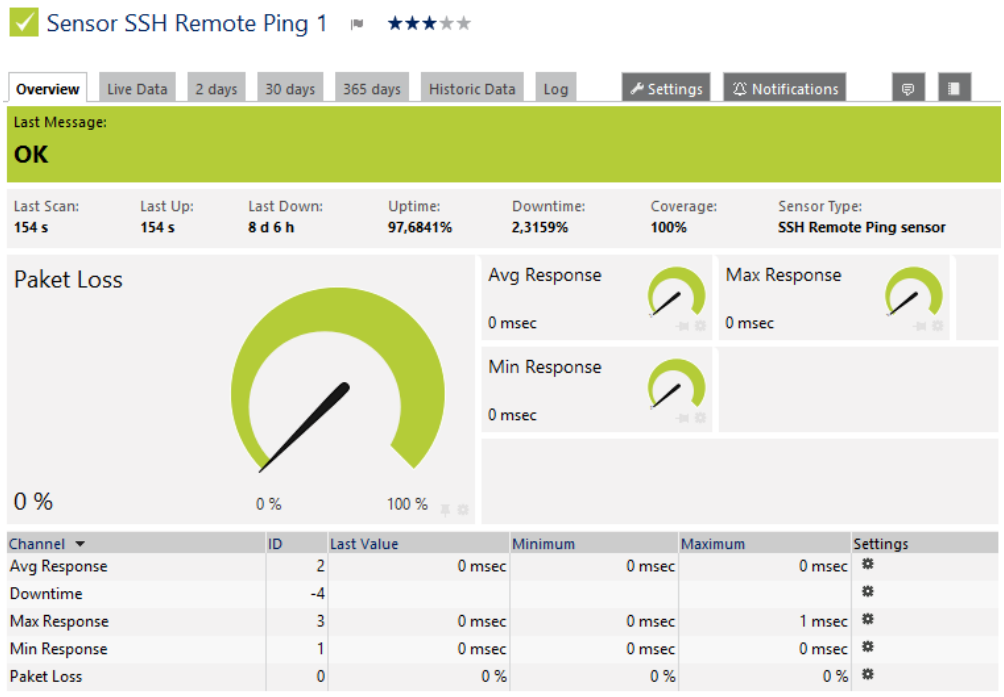
For more general information about settings, please see the **Object Settings** 188 section.

7.8.183 SSH Remote Ping Sensor

The SSH Remote Ping sensor remotely monitors the connectivity between a system running Linux/OS X and another device, using Internet Control Message Protocol (ICMP) echo requests (Ping) and Secure Shell (SSH).

It can show the following:

- Packet loss in percent
- Minimum, maximum, and average response times measured from the remote device you connect to



SSH Remote Ping Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/ssh_remote_ping.png

Remarks

- For this sensor type you must define credentials for Linux/Solaris/Mac OS (SSH/WBEM) systems on the device you want to use the sensor on.
- This sensor type cannot support all Linux/Unix and Mac OS distributions.
- For a general introduction to SSH monitoring, please see manual section **Monitoring via SSH** 3095.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SSH REMOTE PING CONFIGURATION

Target	Enter the DNS name or IP address of the target device the Ping is sent to. The sensor will remotely connect to the parent device it is created on via SSH, then perform a ping request from this remote device to the target device or server. Please enter a string.
Packet Size (Bytes)	Enter the packet size in bytes for the Ping. You can choose any value between 1 and 10000. Please enter an integer value. We recommend that you use the default value.
Packet Count	Enter the number of packets that is sent with each scanning interval.
Custom Parameter	Optionally enter additional parameters that will be added at the end of the ping command. Please do not use parameters that change the output format of the result to make sure it can still be parsed. You cannot enter another command here. Please enter a string or leave the field empty.

SSH SPECIFIC

Connection Timeout (Sec.)	Define a timeout in seconds for the connection. This is the time the sensor will wait to establish a connection to the host. Keep this value as low as possible. The maximum value is **900** seconds (15 minutes). Please enter an integer value.
Shell Timeout (Sec.)	Define a timeout in seconds for the shell response. This is the time in seconds the sensor will wait for the shell to return a response after it has sent its specific command (for example, cat /proc/loadavg). The maximum value is **300** seconds (5 minutes). Please enter an integer value.
SSH Port	Define which port this sensor uses for the SSH connection. Choose between: ▪ **Inherit port number from parent device (default)**: Use the port number as defined in the **Credentials for Linux/Solaris/Mac OS (SSH/WBEM) Systems** section of the device this sensor is created on. ▪ **Enter custom port number**: Define a custom port number below and do not use the port number from the parent device settings.

SSH SPECIFIC

Use Port Number	This field is only visible if you choose **Enter custom port number** above. Enter the port number (between 1 and 65535) that this sensor will use for the SSH connection. Please enter an integer value.
SSH Engine	Select the method you want to use to access data with this SSH sensor [3095]. We strongly recommend that you use the default engine! For some time you still can use the legacy mode to ensure compatibility with your target systems. Choose between: ▪ **Inherit from parent device (default)**: Use the SSH engine that you have defined in the parent device settings or higher in the object hierarchy [118]. If you did not change it, this is the recommended default engine. ▪ **Default**: This is the default monitoring method for SSH sensors. It provides best performance and security. It is set by default in objects that are higher in the hierarchy so usually you can keep the **Inherit from parent device (default)** option. ▪ **Compatibility Mode (deprecated)**: Try this legacy method only if the default mode does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions and is deprecated. We will remove this legacy option soon, so please try to get your SSH sensors running with the default SSH engine. The option you select here overrides the selection of the SSH engine in a higher object (which is a parent device, group, probe, or root).
Result Handling	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section **Data Storage** [3226]. You cannot access stored logs of sensors that run on the local probe of PRTG on demand. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt") in case of error**: Store the last result of the sensor only if it throws an error.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: How and Where Does PRTG Store its Data?

- https://kb.paessler.com/en/topic/463

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.184 SSH SAN Enclosure Sensor

The SSH SAN Enclosure sensor monitors a Storage Area Network (SAN) enclosure via Secure Shell (SSH). The SAN has to provide a command-line interface (CLI) for this purpose.

It can show the following:

- Overall status of the enclosure
- Health status of the power supplies
- Health status of the controllers

Remarks

- This sensor type does not support every SAN, even if it provides a CLI. The sensor only works with specific devices, for example, with the HP P2000.
- It may happen that the controller of your target device breaks down. The experience shows that this issue strongly depends on the hardware model you monitor. Please increase the scanning interval to discharge the controller and try again.
- Sometimes the devices you monitor with this SSH SAN sensor return status values that are not officially documented so that the shown sensor status in PRTG differs from the "real" device status. For more information regarding this issue, please see the Knowledge Base: Knowledge Base: Why does my SSH SAN sensor show a wrong status?
- After a firmware update of the target device, this sensor might show incorrect channel values. Please add this sensor type anew in this case.
- For this sensor type, you must define corresponding credentials in section **Credentials for Linux/Solaris/Mac OS (SSH/WBEM) System** in the settings of the device 360 you want to use the sensor on.
- For a general introduction to SSH monitoring, please see the **Monitoring via SSH** 3095 section.
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the SAN enclosures you want to monitor. PRTG creates one sensor for each enclosure you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SSH SAN ENCLOSURE SETTINGS

Enclosure	Select the enclosures you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SSH SAN ENCLOSURE SETTINGS

Enclosure	Shows the identifier of the enclosure that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Durable ID	Shows the durable identifier of the enclosure that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Name	Shows the name of the enclosure that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
WWN	Shows the WWN (World Wide Name) of the enclosure that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SSH SPECIFIC

Connection Timeout (Sec.)	Define a timeout in seconds for the connection. This is the time the sensor will wait to establish a connection to the host. Keep this value as low as possible. The maximum value is **900** seconds (15 minutes). Please enter an integer value.
Shell Timeout (Sec.)	Define a timeout in seconds for the shell response. This is the time in seconds the sensor will wait for the shell to return a response after it has sent its specific command (for example, cat /proc/loadavg). The maximum value is **300** seconds (5 minutes). Please enter an integer value.
SSH Port	Define which port this sensor uses for the SSH connection. Choose between: ▪ **Inherit port number from parent device (default)**: Use the port number as defined in the **Credentials for Linux/Solaris/Mac OS (SSH/WBEM) Systems** 365 section of the device this sensor is created on. ▪ **Enter custom port number**: Define a custom port number below and do not use the port number from the parent device settings.

SSH SPECIFIC

Use Port Number	This field is only visible if you choose **Enter custom port number** above. Enter the port number (between 1 and 65535) that this sensor will use for the SSH connection. Please enter an integer value.
SSH Engine	Select the method you want to use to access data with this SSH sensor 3095. We strongly recommend that you use the default engine! For some time you still can use the legacy mode to ensure compatibility with your target systems. Choose between: ▪ **Inherit from parent device (default)**: Use the SSH engine that you have defined in the parent device settings or higher in the object hierarchy 118. If you did not change it, this is the recommended default engine. ▪ **Default**: This is the default monitoring method for SSH sensors. It provides best performance and security. It is set by default in objects that are higher in the hierarchy so usually you can keep the **Inherit from parent device (default)** option. ▪ **Compatibility Mode (deprecated)**: Try this legacy method only if the default mode does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions and is deprecated. We will remove this legacy option soon, so please try to get your SSH sensors running with the default SSH engine. The option you select here overrides the selection of the SSH engine in a higher object (which is a parent device, group, probe, or root).
Result Handling	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section **Data Storage** 3226. You cannot access stored logs of sensors that run on the local probe of PRTG on demand. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt") in case of error**: Store the last result of the sensor only if it throws an error.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: Why does my SSH SAN sensor show a wrong status?

- https://kb.paessler.com/en/topic/60145

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

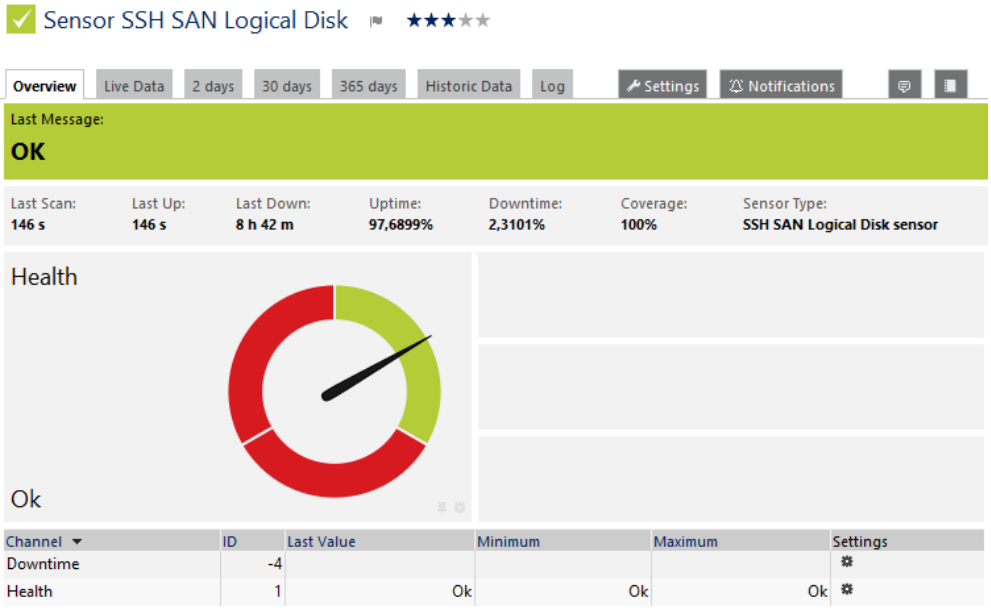
7.8.185 SSH SAN Logical Disk Sensor

The SSH SAN Logical Disk sensor monitors a logical disk on a Storage Area Network (SAN) via Secure Shell (SSH). The SAN has to provide a command-line interface (CLI) for this purpose.

It can show the following:

- Health status of the disk
- Number of I/O operations per second
- Transferred data per second

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



SSH SAN Logical Disk Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/ssh_san_logical_disk.png

Remarks

- This sensor type does not support every SAN, even if it provides a CLI. The sensor only works with specific devices, for example, with the HP P2000.
- It may happen that the controller of your target device breaks down. The experience shows that this issue strongly depends on the hardware model you monitor. Please increase the scanning interval to discharge the controller and try again.
- Sometimes the devices you monitor with this SSH SAN sensor return status values that are not officially documented so that the shown sensor status in PRTG differs from the "real" device status. For more information regarding this issue, please see the Knowledge Base: Knowledge Base: Why does my SSH SAN sensor show a wrong status?

- After a firmware update of the target device, this sensor might show incorrect channel values. Please add this sensor type anew in this case.
- For this sensor type, you must define corresponding credentials in section **Credentials for Linux/Solaris/Mac OS (SSH/WBEM) System** in the settings of the device 360 you want to use the sensor on.
- For a general introduction to SSH monitoring, please see the **Monitoring via SSH** 3095 section.
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.

Add Sensor

The **Add Sensor** dialog appears when you manually 286 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the volumes on the SAN device you want to monitor. PRTG creates one sensor for each volume you choose. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SSH SAN LOGICAL DISK SETTINGS

Volume	Select the volumes you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SSH SPECIFIC

Connection Timeout (Sec.)	Define a timeout in seconds for the connection. This is the time the sensor will wait to establish a connection to the host. Keep this value as low as possible. The maximum value is **900** seconds (15 minutes). Please enter an integer value.
Shell Timeout (Sec.)	Define a timeout in seconds for the shell response. This is the time in seconds the sensor will wait for the shell to return a response after it has sent its specific command (for example, cat /proc/loadavg). The maximum value is **300** seconds (5 minutes). Please enter an integer value.
SSH Port	Define which port this sensor uses for the SSH connection. Choose between: ▪ **Inherit port number from parent device (default)**: Use the port number as defined in the **Credentials for Linux/Solaris/Mac OS (SSH/WBEM) Systems** 365 section of the device this sensor is created on.

SSH SPECIFIC

	▪ **Enter custom port number**: Define a custom port number below and do not use the port number from the parent device settings.
Use Port Number	This field is only visible if you choose **Enter custom port number** above. Enter the port number (between 1 and 65535) that this sensor will use for the SSH connection. Please enter an integer value.
SSH Engine	Select the method you want to use to access data with this SSH sensor [3095]. We strongly recommend that you use the default engine! For some time you still can use the legacy mode to ensure compatibility with your target systems. Choose between: ▪ **Inherit from parent device (default)**: Use the SSH engine that you have defined in the parent device settings or higher in the object hierarchy [118]. If you did not change it, this is the recommended default engine. ▪ **Default**: This is the default monitoring method for SSH sensors. It provides best performance and security. It is set by default in objects that are higher in the hierarchy so usually you can keep the **Inherit from parent device (default)** option. ▪ **Compatibility Mode (deprecated)**: Try this legacy method only if the default mode does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions and is deprecated. We will remove this legacy option soon, so please try to get your SSH sensors running with the default SSH engine. The option you select here overrides the selection of the SSH engine in a higher object (which is a parent device, group, probe, or root).
Result Handling	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section **Data Storage** [3226].

SSH SPECIFIC

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt") in case of error**: Store the last result of the sensor only if it throws an error.

SSH SAN LOGICAL DISK SETTINGS

Volume	Shows the volume that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Size	Shows the size of the volume that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Command Mode	Define the command set to use on the monitored device to get monitoring data. Choose between: ▪ **Basic (recommended)**: We recommend that you use the basic command set for best sensor performance. This setting is appropriate for most scenarios. ▪ **Advanced**: This command set enables you to monitor additional data on the target device like IOs and bandwidth. Because this setting results in higher usage of system resources and so might cause sensor instabilities, we strongly recommend that you choose this option only if this data is crucial for your monitored volume.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

SENSOR DISPLAY

Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. ⓘ To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: Why does my SSH SAN sensor show a wrong status?

- https://kb.paessler.com/en/topic/60145

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

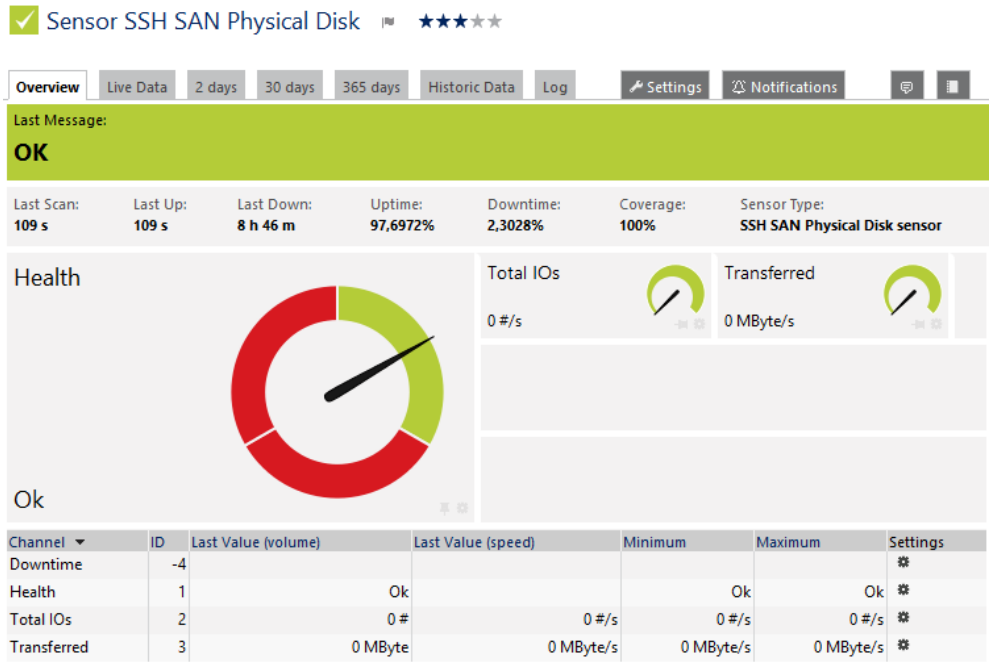
7.8.186 SSH SAN Physical Disk Sensor

The SSH SAN Physical Disk sensor monitors a physical disk on a Storage Area Network (SAN) via Secure Shell (SSH). The SAN has to provide a command-line interface (CLI) for this purpose.

It can show the following:

- Health status of the disk
- Number of I/O operations per second
- Transferred data per second

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



SSH SAN Physical Disk Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/ssh_san_physical_disk.png

Remarks

- This sensor type does not support every SAN, even if it provides a CLI. The sensor only works with specific devices, for example, with the HP P2000.
- It may happen that the controller of your target device breaks down. The experience shows that this issue strongly depends on the hardware model you monitor. Please increase the scanning interval to discharge the controller and try again.

- Sometimes the devices you monitor with this SSH SAN sensor return status values that are not officially documented so that the shown sensor status in PRTG differs from the "real" device status. For more information regarding this issue, please see the Knowledge Base: Knowledge Base: Why does my SSH SAN sensor show a wrong status?
- After a firmware update of the target device, this sensor might show incorrect channel values. Please add this sensor type anew in this case.
- For this sensor type, you must define corresponding credentials in section **Credentials for Linux/Solaris/Mac OS (SSH/WBEM) System** in the settings of the device 360 you want to use the sensor on.
- For a general introduction to SSH monitoring, please see the **Monitoring via SSH** 3095 section.
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the disks on the SAN device you want to monitor. PRTG creates one sensor for each disk you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SSH SAN PHYSICAL DISK SETTINGS

Disk	Select the disks you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SSH SPECIFIC

Connection Timeout (Sec.)	Define a timeout in seconds for the connection. This is the time the sensor will wait to establish a connection to the host. Keep this value as low as possible. The maximum value is **900** seconds (15 minutes). Please enter an integer value.
Shell Timeout (Sec.)	Define a timeout in seconds for the shell response. This is the time in seconds the sensor will wait for the shell to return a response after it has sent its specific command (for example, cat /proc/loadavg). The maximum value is **300** seconds (5 minutes). Please enter an integer value.
SSH Port	Define which port this sensor uses for the SSH connection. Choose between: ▪ **Inherit port number from parent device (default)**: Use the port number as defined in the **Credentials for Linux/Solaris/Mac OS (SSH/WBEM) Systems** 365 section of the device this sensor is created on.

SSH SPECIFIC

- **Enter custom port number**: Define a custom port number below and do not use the port number from the parent device settings.

Use Port Number

This field is only visible if you choose **Enter custom port number** above. Enter the port number (between 1 and 65535) that this sensor will use for the SSH connection. Please enter an integer value.

SSH Engine

Select the method you want to use to access data with this SSH sensor [3095]. We strongly recommend that you use the default engine! For some time you still can use the legacy mode to ensure compatibility with your target systems. Choose between:

- **Inherit from parent device (default)**: Use the SSH engine that you have defined in the parent device settings or higher in the object hierarchy [118]. If you did not change it, this is the recommended default engine.
- **Default**: This is the default monitoring method for SSH sensors. It provides best performance and security. It is set by default in objects that are higher in the hierarchy so usually you can keep the **Inherit from parent device (default)** option.
- **Compatibility Mode (deprecated)**: Try this legacy method only if the default mode does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions and is deprecated. We will remove this legacy option soon, so please try to get your SSH sensors running with the default SSH engine.

The option you select here overrides the selection of the SSH engine in a higher object (which is a parent device, group, probe, or root).

Result Handling

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result**: Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section **Data Storage** [3226].

SSH SPECIFIC

- You cannot access stored logs of sensors that run on the local probe of PRTG on demand.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt") in case of error**: Store the last result of the sensor only if it throws an error.

SSH SAN PHYSICAL DISK SETTINGS

Disk	Shows the disk that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Disk Name	Shows the label of disk that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Size	Shows the size of the disk that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Command Mode	Define the command set to use on the monitored device to get monitoring data. Choose between: ▪ **Basic (recommended)**: We recommend that you use the basic command set for best sensor performance. This setting is appropriate for most scenarios. ▪ **Advanced**: This command set enables you to monitor additional data on the target device like IOs and bandwidth. Because this setting results in higher usage of system resources and so might cause sensor instabilities, we strongly recommend that you choose this option only if this data is crucial for your monitored volume.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: Why does my SSH SAN sensor show a wrong status?

- https://kb.paessler.com/en/topic/60145

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

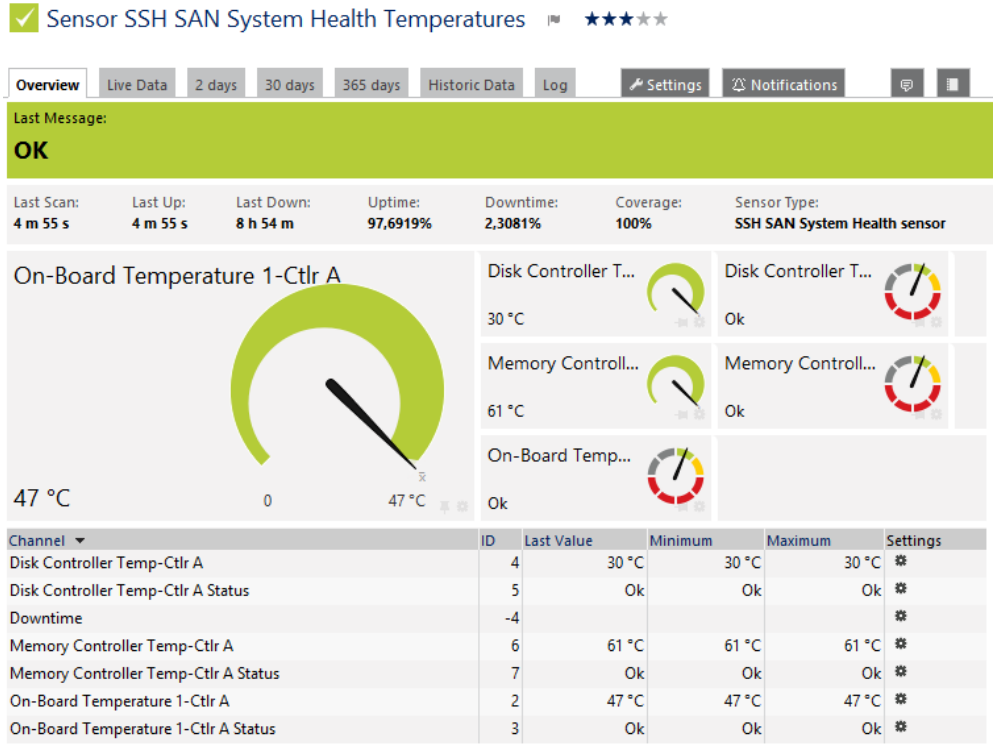
7.8.187 SSH SAN System Health Sensor

The SSH SAN System Health sensor monitors the system health of a Storage Area Network (SAN) via Secure Shell (SSH). The SAN has to provide a command-line interface (CLI) for this purpose.

It can show several metrics of an SAN, depending on the available measurement components on the SAN:

- Overall unit status
- Temperature and temperature states
- Voltage and voltage states
- Capacitor charge and status

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



SSH SAN System Health Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/ssh_san_system_health.png

Remarks

- This sensor type does not support every SAN, even if it provides a CLI. The sensor only works with specific devices, for example, with the HP P2000.

- It may happen that the controller of your target device breaks down. The experience shows that this issue strongly depends on the hardware model you monitor. Please increase the scanning interval to discharge the controller and try again.
- Sometimes the devices you monitor with this SSH SAN sensor return status values that are not officially documented so that the shown sensor status in PRTG differs from the "real" device status. For more information regarding this issue, please see the Knowledge Base: Knowledge Base: Why does my SSH SAN sensor show a wrong status?
- After a firmware update of the target device, this sensor might show incorrect channel values. Please add this sensor type anew in this case.
- For this sensor type, you must define corresponding credentials in section **Credentials for Linux/Solaris/Mac OS (SSH/WBEM) System** in the settings of the device 360 you want to use the sensor on.
- For a general introduction to SSH monitoring, please see the **Monitoring via SSH** 3095 section.
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the metrics you want to monitor. PRTG creates one sensor for each metric you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SSH SAN SPECIFIC

Metric	Select the metrics you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SSH SAN SPECIFIC

Metric	Shows the metric this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SSH SPECIFIC

Connection Timeout (Sec.)	Define a timeout in seconds for the connection. This is the time the sensor will wait to establish a connection to the host. Keep this value as low as possible. The maximum value is **900** seconds (15 minutes). Please enter an integer value.
Shell Timeout (Sec.)	Define a timeout in seconds for the shell response. This is the time in seconds the sensor will wait for the shell to return a response after it has sent its specific command (for example, cat /proc/loadavg). The maximum value is **300** seconds (5 minutes). Please enter an integer value.
SSH Port	Define which port this sensor uses for the SSH connection. Choose between: ▪ **Inherit port number from parent device (default)**: Use the port number as defined in the **Credentials for Linux/Solaris/Mac OS (SSH/WBEM) Systems** 365 section of the device this sensor is created on. ▪ **Enter custom port number**: Define a custom port number below and do not use the port number from the parent device settings.
Use Port Number	This field is only visible if you choose **Enter custom port number** above. Enter the port number (between 1 and 65535) that this sensor will use for the SSH connection. Please enter an integer value.
SSH Engine	Select the method you want to use to access data with this SSH sensor 3095. We strongly recommend that you use the default engine! For some time you still can use the legacy mode to ensure compatibility with your target systems. Choose between: ▪ **Inherit from parent device (default)**: Use the SSH engine that you have defined in the parent device settings or higher in the object hierarchy 118. If you did not change it, this is the recommended default engine. ▪ **Default**: This is the default monitoring method for SSH sensors. It provides best performance and security. It is set by default in objects that are higher in the hierarchy so usually you can keep the **Inherit from parent device (default)** option. ▪ **Compatibility Mode (deprecated)**: Try this legacy method only if the default mode does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions and is deprecated. We will remove this legacy option soon, so please try to get your SSH sensors running with the default SSH engine.

SSH SPECIFIC

The option you select here overrides the selection of the SSH engine in a higher object (which is a parent device, group, probe, or root).

Result Handling

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result**: Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section Data Storage 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt") in case of error**: Store the last result of the sensor only if it throws an error.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.

SCANNING INTERVAL

- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: Why does my SSH SAN sensor show a wrong status?

- https://kb.paessler.com/en/topic/60145

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

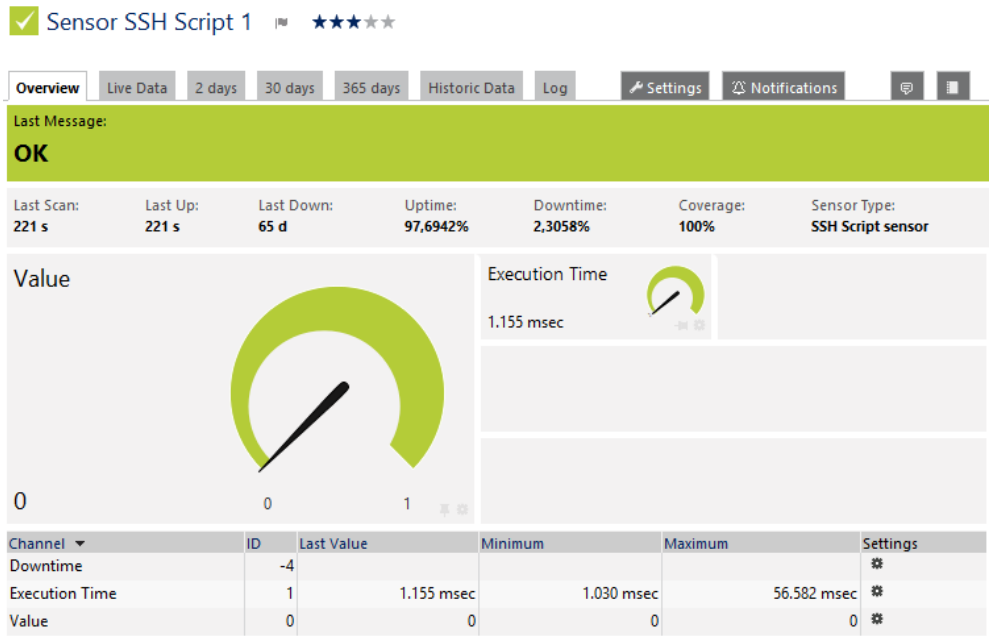
For more general information about settings, please see the **Object Settings** 188 section.

7.8.188 SSH Script Sensor

The SSH Script sensor connects to a Linux/Unix system via Secure Shell (SSH) and executes a script file located on the target system. This option is provided as part of the PRTG Application Programming Interface (API). For details about the return value format, please see the Application Programming Interface (API) Definition 3174.

It shows the following:

- Execution time
- One value returned by the executable file or script (in one channel only).



SSH Script Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/ssh_script.png

Remarks

- For details about the return value format, please see the Application Programming Interface (API) Definition 3174.
- For security reasons, you must store your script file on the target system. The file must be located in the directory **/var/prtg/scripts**. Ensure the script has executable rights. If the script is not available or was deleted from the script folder, you will get the error message "Script not found (237)".
- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.
- For this sensor type you must define credentials for Linux/Solaris/Mac OS (SSH/WBEM) systems on the device you want to use the sensor on.
- This sensor type cannot support all Linux/Unix and Mac OS distributions.

- For a general introduction to SSH monitoring, please see manual section **Monitoring via SSH** 3095.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SENSOR SETTINGS

Script	Select a script file from the list. The dropdown menu will list all script files available in the /var/prtg/scripts directory on the target Linux/Unix system. For a script file to appear in this list, store the target file into this directory. Ensure the script has executable rights. To show the expected sensor value and status 163, your file must use the correct format for the returned values. In this case it is exitcode:value:message to standard output stdout. The exit code determines the sensor status. For detailed information on the expected return format and on how to build custom sensors, please see the PRTG API documentation (**Application Programming Interface (API) Definition** 3174). There you will find detailed information on the **Custom Sensors** tab. For an example script, please see **More** 2277 section below.
Value Type	Define the type of the values that your script returns. Choose between: ▪ **Integer**: The return values are from the type integer. If the script returns a float, PRTG will show the value **0**. ▪ **Float:** The return values are from the type float, with a dot (.) between pre-decimal position and decimal places. In this setting, the sensor will also display integer values unless they produce a buffer overflow. ▪ **Counter:** Your script returns varying integer values. PRTG will show the difference between the values of two sensor scans. ⓘ A counter must return an integer, float values are not supported. ⓘ This sensor type does not support string values.
Channel Name	Enter a name for the channel in which the sensor shows returned values. Please enter a string. This is for display purposes only. You can change the name later in the sensor's channel settings 2782.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

ⓘ Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SETTINGS

Script	Shows the name of the script that the sensor executes with each scan. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Character Encoding	Define the character encoding you use in your script to correctly display the sensor message. Choose between: ▪ **UTF-8 (default)** ▪ **ASCII**
Parameters	If your script file catches command line parameters, you can define them here. You can use placeholders as well. For a full list of all placeholders please see the API documentation (**Application Programming Interface (API) Definition** 3174).

SENSOR SETTINGS

	Note: Please make sure you write the placeholders in quotes to ensure that they are working properly if their values contain blanks. Use single quotation marks '' with PowerShell scripts, and double quotes "" with all others. Please enter a string or leave the field empty.
Mutex Name	Define any desired mutex name for the process. PRTG will run all custom script sensors having the same mutex name serially (not simultaneously). This is useful if you use a lot of sensors and want to avoid high resource usage caused by processes running at the same time. Please enter a string or leave the field empty. For links to more information, please see the **More** 757 section below.
Unit String	Define a unit for the channel value. Please enter a string. This is for display purposes only and will be the default unit for a new channel. You can change the unit after sensor creation in the sensor's channel settings 2782.
Value Type	Shows the expected type of the returned value. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
If Value Changes	Define what this sensor will do when the sensor value changes. You can choose between: ▪ **Ignore changes (default)**: The sensor takes no action on change. ▪ **Trigger 'change' notification**: The sensor sends an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification 2791 whenever the sensor value changes.

SSH SPECIFIC

Connection Timeout (Sec.)	Define a timeout in seconds for the connection. This is the time the sensor will wait to establish a connection to the host. Keep this value as low as possible. The maximum value is **900** seconds (15 minutes). Please enter an integer value.

SSH SPECIFIC

Shell Timeout (Sec.)	Define a timeout in seconds for the shell response. This is the time in seconds the sensor will wait for the shell to return a response after it has sent its specific command (for example, cat /proc/loadavg). The maximum value is **300** seconds (5 minutes). Please enter an integer value.
SSH Port	Define which port this sensor uses for the SSH connection. Choose between: ▪ **Inherit port number from parent device (default)**: Use the port number as defined in the **Credentials for Linux/Solaris/Mac OS (SSH/WBEM) Systems** 365 section of the device this sensor is created on. ▪ **Enter custom port number**: Define a custom port number below and do not use the port number from the parent device settings.
Use Port Number	This field is only visible if you choose **Enter custom port number** above. Enter the port number (between 1 and 65535) that this sensor will use for the SSH connection. Please enter an integer value.
SSH Engine	Select the method you want to use to access data with this SSH sensor 3095. We strongly recommend that you use the default engine! For some time you still can use the legacy mode to ensure compatibility with your target systems. Choose between: ▪ **Inherit from parent device (default)**: Use the SSH engine that you have defined in the parent device settings or higher in the object hierarchy 118. If you did not change it, this is the recommended default engine. ▪ **Default**: This is the default monitoring method for SSH sensors. It provides best performance and security. It is set by default in objects that are higher in the hierarchy so usually you can keep the **Inherit from parent device (default)** option. ▪ **Compatibility Mode (deprecated)**: Try this legacy method only if the default mode does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions and is deprecated. We will remove this legacy option soon, so please try to get your SSH sensors running with the default SSH engine. ⓘ The option you select here overrides the selection of the SSH engine in a higher object (which is a parent device, group, probe, or root).
Result Handling	Define what PRTG will do with the sensor results. Choose between:

SSH SPECIFIC

- **Discard sensor result**: Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section Data Storage 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt") in case of error**: Store the last result of the sensor only if it throws an error.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.
- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings 2782 settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. ⓘ Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: Is there a shell script example for PRTG's SSH Script Sensor?

- https://kb.paessler.com/en/topic/39513

Information about custom scripts and executables

- **Application Programming Interface (API) Definition** 3174
- **Additional Sensor Types (Custom Sensors)** 2778

Knowledge Base: What is the Mutex Name in PRTG's EXE/Script Sensor's settings?

- https://kb.paessler.com/en/topic/6673

Knowledge Base: How and Where Does PRTG Store its Data?

- https://kb.paessler.com/en/topic/463

Knowledge Base: How can I test if parameters are correctly transmitted to my script when using an EXE/Script sensor?

- https://kb.paessler.com/en/topic/11283

Knowledge Base: For which sensor types do you recommend Windows Server 2012 R2 and why?

- https://kb.paessler.com/en/topic/64331

Knowledge Base: How can I show special characters with EXE/Script sensors?

- https://kb.paessler.com/en/topic/64817

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

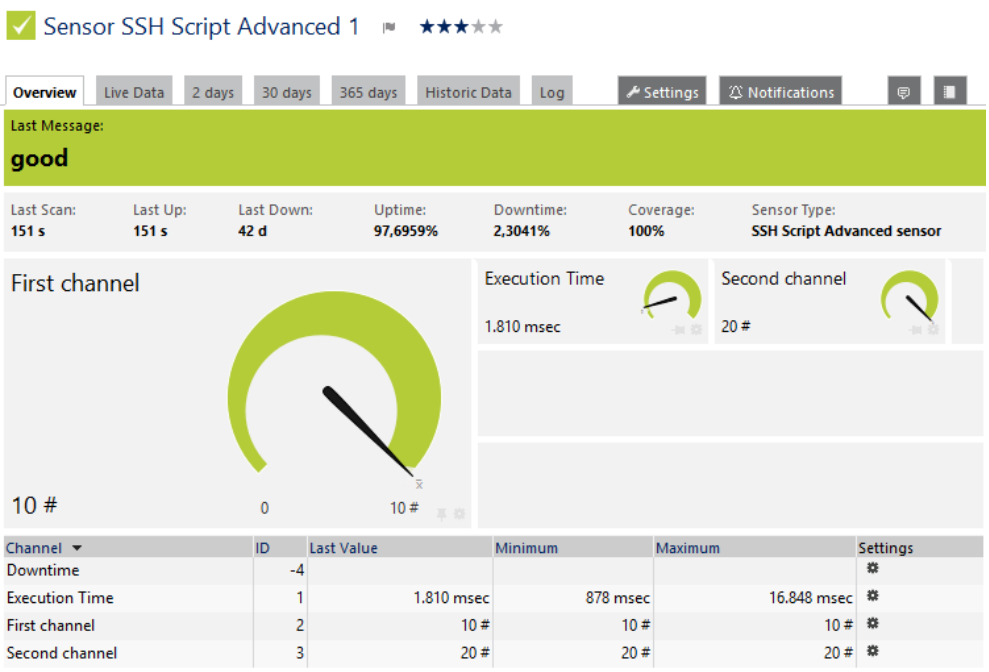
For more general information about settings, please see the **Object Settings** 188 section.

7.8.189 SSH Script Advanced Sensor

The SSH Script Advanced sensor connects to a Linux/Unix system via Secure Shell (SSH) and executes a script file located on the target system. This option is provided as part of the PRTG Application Programming Interface (API). For details about the return value format, please see the **Application Programming Interface (API) Definition**.

It can show the following:

- Execution time
- Values returned by the script in multiple channels. The return value of this sensor must be valid XML or JSON.



SSH Script Advanced Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/ssh_script_advanced.png

Remarks

- For details about the return value format please see the **Application Programming Interface (API) Definition**.
- For security reasons, the script file must be stored on the target system. Please make sure the script has executable rights.
- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.
- For this sensor type you must define credentials for Linux/Solaris/Mac OS (SSH/WBEM) systems on the device you want to use the sensor on.
- This sensor type cannot support all Linux/Unix and Mac OS distributions.

- For a general introduction to SSH monitoring, please see manual section **Monitoring via SSH** 3095.

Limited to 50 Sensor Channels

PRTG does not support more than 50 sensor channels officially. Depending on the data used with this sensor type, you might exceed the maximum number of supported sensor channels. In this case, PRTG will try to display all sensor channels. However, please be aware that you will experience limited usability and performance.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SENSOR SETTINGS

Script	Select a script file from the list. The dropdown menu will list all script files available in the /var/prtg/scriptsxml directory on the target Linux/Unix system. For a script file to appear in this list, please store the target file into this directory. Please make sure the script has executable rights. To show the expected sensor value and status 163, your files must return the expected XML or JSON format to standard output stdout. Values and message must be embedded in the XML or JSON. For detailed information on the expected return format and on how to build custom sensors, please see the PRG API documentation (**Application Programming Interface (API) Definition** 3174). There you will find detailed information on the **Custom Sensors** tab.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SETTINGS

Script	Shows the script that the sensor executes with each sensor. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Parameters	If your script file catches command line parameters, you can define them here. You can use placeholders as well. For a full list of all placeholders, please see the API documentation (**Application Programming Interface (API) Definition** 3174). Note: Please make sure you write the placeholders in quotes to ensure that they are working properly if their values contain blanks. Use single quotation marks '' with PowerShell scripts, and double quotes "" with all others. Please enter a string or leave the field empty.
Mutex Name	Define any desired mutex name for the process. PRTG will execute all custom script sensors having the same mutex name serially (not simultaneously). This is useful if you use a lot of sensors and want to avoid high resource usage caused by processes running at the same time. Please enter a string or leave the field empty.

SENSOR SETTINGS

For links to more information, please see the **More** 757 section below.

SSH SPECIFIC

Connection Timeout (Sec.)

Define a timeout in seconds for the connection. This is the time the sensor will wait to establish a connection to the host. Keep this value as low as possible. The maximum value is **900** seconds (15 minutes). Please enter an integer value.

Shell Timeout (Sec.)

Define a timeout in seconds for the shell response. This is the time in seconds the sensor will wait for the shell to return a response after it has sent its specific command (for example, cat /proc/loadavg). The maximum value is **300** seconds (5 minutes). Please enter an integer value.

SSH Port

Define which port this sensor uses for the SSH connection. Choose between:

- **Inherit port number from parent device (default)**: Use the port number as defined in the **Credentials for Linux/Solaris/Mac OS (SSH/WBEM) Systems** 365 section of the device this sensor is created on.
- **Enter custom port number**: Define a custom port number below and do not use the port number from the parent device settings.

Use Port Number

This field is only visible if you choose **Enter custom port number** above. Enter the port number (between 1 and 65535) that this sensor will use for the SSH connection. Please enter an integer value.

SSH Engine

Select the method you want to use to access data with this SSH sensor 3095. We strongly recommend that you use the default engine! For some time you still can use the legacy mode to ensure compatibility with your target systems. Choose between:

- **Inherit from parent device (default)**: Use the SSH engine that you have defined in the parent device settings or higher in the object hierarchy 118. If you did not change it, this is the recommended default engine.

SSH SPECIFIC

- **Default**: This is the default monitoring method for SSH sensors. It provides best performance and security. It is set by default in objects that are higher in the hierarchy so usually you can keep the **Inherit from parent device (default)** option.
- **Compatibility Mode (deprecated)**: Try this legacy method only if the default mode does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions and is deprecated. We will remove this legacy option soon, so please try to get your SSH sensors running with the default SSH engine.

The option you select here overrides the selection of the SSH engine in a higher object (which is a parent device, group, probe, or root).

Result Handling

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result**: Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section **Data Storage** 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt") in case of error**: Store the last result of the sensor only if it throws an error.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

SENSOR DISPLAY

Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Information about custom scripts and executables

- **Application Programming Interface (API) Definition** 3174
- **Additional Sensor Types (Custom Sensors)** 2778

Knowledge Base: What is the Mutex Name in PRTG's EXE/Script Sensor's settings?

- https://kb.paessler.com/en/topic/6673

Knowledge Base: How and Where Does PRTG Store its Data?

- https://kb.paessler.com/en/topic/463

Knowledge Base: How can I test if parameters are correctly transmitted to my script when using an EXE/Script sensor?

- https://kb.paessler.com/en/topic/11283

Knowledge Base: For which sensor types do you recommend Windows Server 2012 R2 and why?

- https://kb.paessler.com/en/topic/64331

Knowledge Base: How can I show special characters with EXE/Script sensors?

- https://kb.paessler.com/en/topic/64817

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

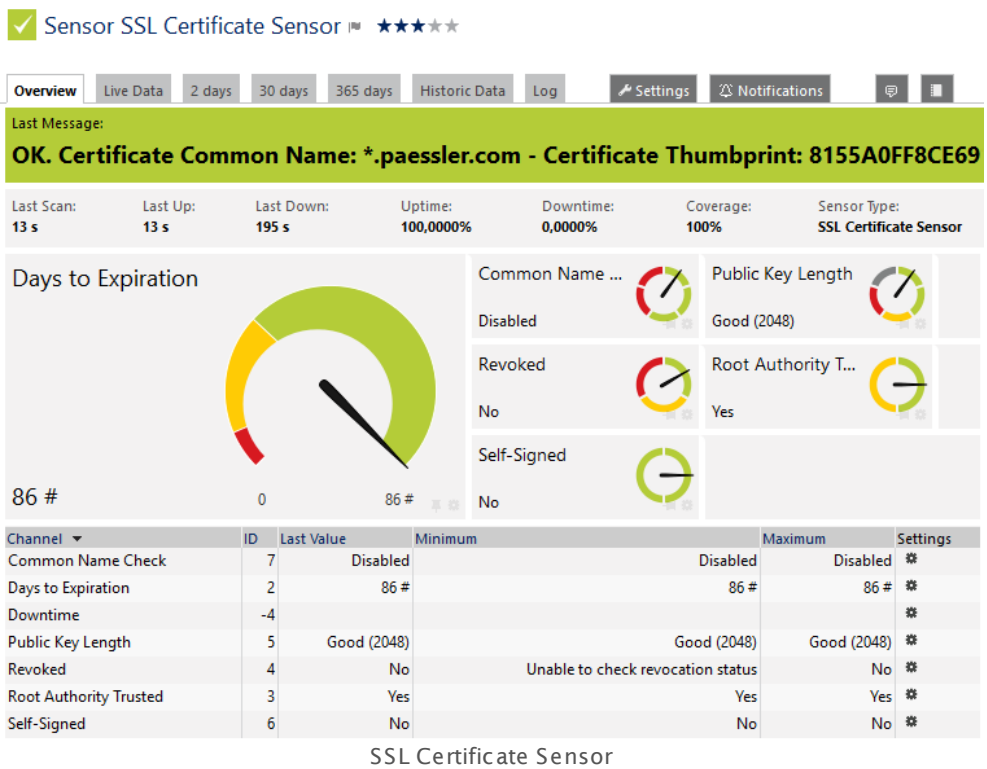
Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.190 SSL Certificate Sensor

The SSL Certificate sensor monitors the certificate of a secure Secure Sockets Layer (SSL)/ Transport Layer Security (TLS) connection. It can show the following:

- Days to expiration (with predefined lower warning and error limits)
- Public key length
  - RSA keys: **Warning** status 163 for 1024-bit keys (**Weak** security), **Up** status for 2048-bit keys (**Good** security) and longer (**Perfect** security); **Down** status for shorter keys (**Unsafe**)
  - ECC (Elliptic Curve Cryptography) keys: **Up** status 163 for 128-bit and 192-bit keys (**Good** security) and longer (**Perfect** security); **Down** status for shorter keys (**Unsafe**)
- If common name or subject alternative names match the host address or SNI (if certificate name validation is enabled)
- If the certificate has been revoked (failing to query the certificate revocation list results in a warning status)
- If the certificate is trusted as root authority
- If the certificate is self-signed
- Certificate common name (sensor message)
- Certificate thumbprint (sensor message)



SSL Certificate Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/ssl_certificate.png

Remarks

- Enter the DNS name in the parent device settings 360 exactly as written in your certificate. For example, enter "www.paessler.com" instead of "paessler.com". The short version might not work properly with this sensor.
- To check the revocation status of a certificate, the sensor uses the same proxy settings as configured for the Windows user account on which the PRTG probe runs. This is usually the Windows local "system" user account. If you use a proxy, for example, please edit these settings in the Internet Explorer on this system accordingly (on the computer running the probe; on all nodes if in a cluster).
- This sensor type has predefined limits for several metrics. You can change these limits individually in the channel settings. For detailed information about channel limits, please refer to the manual section **Sensor Channels Settings** 2782.
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.
- This sensor supersedes the deprecated HTTP Certificate Expiry sensor which is outdated. Please use the **SSL Certificate sensor** 2289 to monitor SSL certificates.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.

BASIC SENSOR SETTINGS

Parent Tags	Shows **Tags** [124] that this sensor inherits [124] from its parent device, group, and probe [118]. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** [124], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited [124] from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SSL CERTIFICATE SPECIFIC

Port	Enter the number of the port to which this sensor connects. Please enter an integer value. The default port is **443**.
Virtual Host (SNI Domain)	Define the host name that the sensor will try to query if your server presents multiple certificates on the same IP address and port combination. Please enter a string. If in the case of virtual hosting you need to identify the specific certificate for a specific domain while all domains use the same IP address, you can use Server Name Identification (SNI), which is an extension of Transport Layer Security (TLS). ⓘ If you enable the **Common Name Validation** below, the sensor will compare the common name and optionally alternative names with the SNI defined here. Leave this field empty to validate the common name with the host address of the parent device.
Certificate Name Validation	Define if you want the sensor to validate the certificate name. Choose between: ▪ **Do not compare common name with device address or SNI (default):** The sensor will not check if the certificate name is valid by comparing it with the address of the parent device or the defined SNI.

SSL CERTIFICATE SPECIFIC

- **Compare and show 'down' status if common name and address/SNI do not match:** Check the common name to validate the certificate. If you set an SNI domain above, the sensor will compare the common name with this SNI. If you leave the SNI field empty, the sensor will use the host address of the parent device. If common name and the checked address/SNI do not match, the sensor will show a **Down** status 163.
- **Compare and show 'down' status if common name/ alternative names and address/SNI do not match**: Check common name and Subject Alternative Names (SAN) to validate the certificate. If you set an SNI domain above, the sensor will compare common name and alternative names with the SNI. If you leave the SNI field empty, the sensor will use the host address of the parent device. If common name or alternative names and the checked address/SNI do not match, the sensor will show a **Down** status 163.

CONNECTION SPECIFIC

Use SOCKS Proxy (v5 only)	Define if you want to use a SOCKS proxy server for the sensor connection. Choose between: ▪ **Do not use SOCKS proxy (default)**: The sensor will connect directly to the target host without using a SOCKS proxy. ▪ **Use SOCKS proxy**: The sensors will connect using SOCKS5. Provide data for the SOCKS connection below. ⓘ Other SOCKS versions are not supported. ⓘ This sensor type only supports SOCKS5 proxies. HTTP proxies are not supported.
SOCKS Proxy Server	This field is only visible if you choose **Use SOCKS proxy**. Enter the IP address or host name of the SOCKS5 proxy server that the sensor will use to connect.
SOCKS Proxy Server Port	This field is only visible if you choose **Use SOCKS proxy**. Enter the port number of the SOCKS5 proxy server that the sensor will use to connect.
SOCKS Proxy Server User	This field is only visible if you choose **Use SOCKS proxy**. If the SOCKS5 proxy server requires authentication, enter a username.

CONNECTION SPECIFIC

SOCKS Proxy Server Password	This field is only visible if you choose **Use SOCKS proxy**. If the SOCKS5 proxy server requires authentication, enter the password for the user you specify above.

DEBUG OPTIONS

Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section **Data Storage** 3226. You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

You can use the debug option to get a log file with information about the certificate chain. Additionally, certificates in the certificate chain are stored in the log folder (.cer files). This can help you, for example, if you have issues with the Root Authority Trusted channel of this sensor.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor.

SENSOR DISPLAY

- **Show channels independently (default)**: Show an own graph for each channel.
- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.191 SSL Security Check Sensor

The SSL Security Check sensor monitors the Secure Sockets Layer (SSL) connectivity to the port of a device. It tries to connect to the specified TCP/IP port number of a device with various SSL/TLS protocol versions and shows if a particular protocol is supported.

The sensor checks connectivity with the following protocols in particular channels 121 with the possible values **Accepted** (sensor can connect with this protocol) or **Denied** (sensor cannot connect with this protocol):

- **SSL 2.0**: weak security (warning if accepted, up if denied)
- **SSL 3.0**: weak security (warning if accepted, up if denied)
- **TLS 1.0**: weak security (warning if accepted, up if denied)
- **TLS 1.1**: strong security (up if accepted, otherwise gray)
- **TLS 1.2**: perfect security (up if accepted, otherwise gray)

The default primary channel **Security Rating** shows the connection security to the defined port with one of the following states 163:

- **Down**: There is no secure protocol available. The sensor cannot connect with one of the given protocols.
- **Warning** (weak): The sensor can connect with at least one of the weak protocols SSL 2.0, SSL 3.0, or TLS 1.0.
- **Up** (strong): The sensor can connect with a strong protocol only (TLS 1.1, TLS 1.2). Connecting with a weak protocol is not possible.

SSL Security Check Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/ssl_security_check.png

Remarks

- This sensor only checks accepted protocols, it does not consider the used ciphers.
- Knowledge Base: How do you determine the protocol security ratings of the SSL Security Check sensor?
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SSL SECURITY SPECIFIC

Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).
Port	Enter the number of the port to which this sensor connects. Please enter an integer value. The default port is 443.

Virtual Host (SNI Domain)	Enter a host name that the sensor will query. The sensor uses this host to connect if the target server presents multiple certificates on the same IP address and IP port when using Server Name Identification (SNI).

CONNECTION SPECIFIC

Use SOCKS Proxy (v5 only)	Define if you want to use a SOCKS proxy server for the sensor connection. Choose between: ▪ **Do not use SOCKS proxy (default)**: The sensor will connect directly to the target host without using a SOCKS proxy. ▪ **Use SOCKS proxy**: The sensors will connect using SOCKS5. Provide data for the SOCKS connection below. ⓘ Other SOCKS versions are not supported. ⓘ This sensor type only supports SOCKS5 proxies. HTTP proxies are not supported.
SOCKS Proxy Server	This field is only visible if you choose **Use SOCKS proxy**. Enter the IP address or host name of the SOCKS5 proxy server that the sensor will use to connect.
SOCKS Proxy Server Port	This field is only visible if you choose **Use SOCKS proxy**. Enter the port number of the SOCKS5 proxy server that the sensor will use to connect.
SOCKS Proxy Server User	This field is only visible if you choose **Use SOCKS proxy**. If the SOCKS5 proxy server requires authentication, enter a username.
SOCKS Proxy Server Password	This field is only visible if you choose **Use SOCKS proxy**. If the SOCKS5 proxy server requires authentication, enter the password for the user you specify above.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

SENSOR DISPLAY

	You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

SCANNING INTERVAL

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: How do you determine the protocol security ratings of the SSL Security Check sensor?

- https://kb.paessler.com/en/topic/71566

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

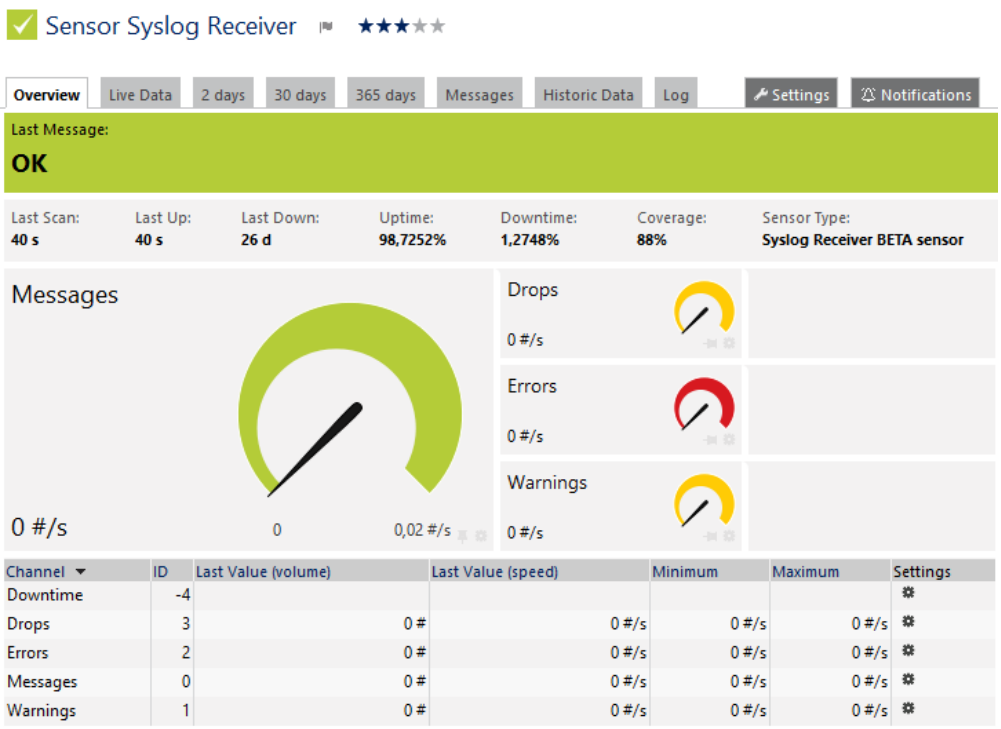
For more general information about settings, please see the **Object Settings** 188 section.

7.8.192 Syslog Receiver Sensor

The Syslog Receiver sensor receives and analyzes Syslog messages.

It shows the following:

- Number of received syslog messages per second
- Number of messages categorized as "warning" per second
- Number of messages categorized as "error" per second
- Number of dropped packets per second



Syslog Receiver Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/syslog_receiver.png

Remarks

- With the available filter options, you can define individually which types of messages the sensor will consider for monitoring, and which messages it will categorize as warning or error messages. Depending on the filters, received messages are counted in the respective channels.
- Add the sensor to the probe device to receive all messages of the system running the probe.
- Add the sensor to a specific device to receive all messages from this device directly. This makes this sensor type faster than just using source filters.

- You can use specific placeholders in email notification templates 2921 to see the messages when you receive an email notification. See the Knowledge Base: What placeholders can I use with PRTG?
- Sensor states 163 of this sensor type persist for one scanning interval only. If there is no warning or error message in the following scanning interval, the sensor will show an **up** status again. For a workaround, see this Knowledge Base article: How can I configure sensors using speed limits to keep the status for more than one interval?
- If you do not add the sensor to a probe device but to another device in PRTG, be careful with the configuration: Ensure that the IP address or DNS name of the parent device matches the proper sender. For example, if you want to receive messages from a Storage Area Network (SAN), you might have to add a device to PRTG using the IP address of a specific array member that sends the messages. Providing a DNS name that points to the IP address of a whole group might not work for SANs.
- This sensor type cannot be used in cluster mode. You can set it up on a local probe or remote probe only, not on a cluster probe.
- For a general introduction to the receiver's configuration, please see manual section **Monitoring Syslogs and SNMP Traps** 3125.
- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SYSLOG SPECIFIC

Listen on Port	Enter the number of the port on which the sensor waits for Syslog messages. The default port is **514**. Please enter an integer value. We recommend that you use the default value.
Purge Messages After	Define how long PRTG stores received Syslog messages for analysis. Choose a period of time from the dropdown list.

FILTER

Include Filter	Define if you want to filter Syslog messages. If you leave this field empty or use the keyword "any", the sensor will process all data. To include specific types of messages only, define filters using a special syntax. For more information, see section **Filter Rules** 2318.

FILTER

Exclude Filter	Define which types of Syslog messages the sensor will discard and not process. To exclude specific types of messages, define filters using a special syntax. For more information, see section **Filter Rules** 2318.
Warning Filter	Define which types of Syslog messages count for the **Warnings** channel. To categorize received messages as warning messages, define filters using a special syntax. For more information, see section **Filter Rules** 2318. Messages are collected until a scanning interval ends. as long as the scanning interval is running, no status change will happen. By default, the sensor will turn into a **Warning** status after a scanning interval has finished and there was at least one warning message (and no error message) during this interval. The status will remain **Warning** at least until the succeeding scanning interval has finished. If in this scanning interval no warning or error message occurred, the status of the sensor will turn **Up** again after the interval.
Error Filter	Define which types of syslog messages will count for the **Errors** channel. To categorize received messages as error messages, define filters using a special syntax. For more information, see section **Filter Rules** 2318. Messages are collected until a scanning interval ends. As long as the scanning interval is running, no status change will happen. By default, the sensor will turn into a **Down** status after a scanning interval has finished and there was at least one error message during this interval. The status will remain **Down** at least until the succeeding scanning interval has finished. If the sensor did not receive any warning or error message in this scanning interval, the status of the sensor will turn **Up** again after the interval.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor.

SENSOR DISPLAY

- **Show channels independently (default)**: Show an own graph for each channel.
- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. ⓘ To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

DEBUGGING	
Log Data to Disk	Define if the probe will write a log file of the received data to the data folder (see **Data Storage** 3226) to the disk for debugging purposes. Choose between: ▪ **Off (recommended)**: Do not write additional log files. Recommended for normal use cases. ▪ **On**: Write log files for all data received. ⚠ Use with caution! When enabled, huge data files can be created. Please use for a short time and for debugging purposes only.

Filter Rules for Syslog Messages

Filter rules are used for the include, exclude, warning, and error definition fields of the Syslog Receiver sensor. They are based on the following format:

```
field[filter]
```

You can use various filters suitable to your needs. Include and exclude filters define which messages to monitor. Warning and error filters define how to categorize received messages. Provide these filters in the sensor settings as formulas. Formulas are fields which you can combine with boolean operators (AND, OR, NOT) and brackets.

Field	Parameter	Example
source[ip]	the IP address where the messages will be received from; masks and ranges are also possible	▪ source[10.0.23.50] ▪ source[10.0.23.10-50] ▪ source[10.0.23.10/255]
facility[number]	any number or range from 0 to 23 specifying the type of program sending the message	▪ facility[2] ▪ facility[5-7] ▪ facility[5] OR facility[6]
severity[number]	any number or range from 0 (emergency) to 7 (debug) specifying the type of message	▪ severity[4] ▪ severity[1-3] ▪ severity[1] AND severity[2]

hostname [text]	any string specifying the hostname of a device in the message	▪ hostname [www.example.com]
tag[text]	any string specifying the tag of a program or process in the message	▪ tag[su]
appname [text]	any string specifying the appname part of the message	▪ appname[myproc] ▪ appname[demo] AND msgid[m42]
procid [text]	any string specifying the process identifier part of the message	▪ procid[1860]
msgid[text]	any string specifying the message identifier part of the message	▪ msgid[ID47]
message [parttext]	any string specifying the message part of the message (substring will match; case insensitive!)	▪ message[Error]
data [id ,param,value]	checks the SD-ID block of the message's structured data for a parameter matching the given value	▪ data [exampleSDID@12345,eventSource,Application]
data [parttext]	checks if the given substring matches on structured data as displayed in the corresponding table	▪ data [exampleSDID@1234]
data [id,param]	checks if the parameter exists in the given ID element	▪ data [exampleSDID@1234,eventSource]

String parameters (except the substring in **message**) have to match exactly the particular parts of the message. They are case sensitive!

Messages Tab: Review and Analyze Syslog Messages

PRTG stores received Syslog messages as common files in the data folder (see section **Data Storage** 3226). To review and analyze all received messages, you can access the most recent data directly in a table list 207 in the PRTG web interface. You can access this list via the **Overview** tab of the sensors.

Received syslog messages are only shown after an (automatic) page refresh following to a sensor scan in the table on the **Overview** tab (default for auto refresh 2909 is 30 seconds).

For more details and further filter options, click the **Messages** tab of the Syslog Receiver sensor. You will see all received messages in a table list 207. On the top, you have display filter options to drill down into the data for specific events of your interest. The filters are the same as available in the sensor settings, but you can define them without using formulas. Provide the desired parameters and PRTG loads the filtered list automatically.

You can automatically add a filter by clicking the content of a column.

Advanced Filter Settings

You can open advanced filter settings by clicking the gear icon in the **Filter** row. The **Advanced Filter** will appear in a popup window. In the text field, you can define a filter using the syntax as given in section **Filter Rules for Syslog Messages** 2318. If you have provided filter parameters on the **Messages** tab, the advanced filter will already include them as a corresponding formula with the correct syntax. You can adjust this filter to your needs. You can also copy the automatically created and manually adjusted formula for usage in the filter fields of the sensor settings.

More

Video Tutorial: Create and Configure a Syslog Receiver Sensor in PRTG

- https://www.paessler.com/support/videos/prtg-advanced/syslog-receiver

Knowledge Base: How can I configure sensors using speed limits to keep the status for more than one interval?

- https://kb.paessler.com/en/topic/73212

Knowledge Base: What placeholders can I use with PRTG?

- https://kb.paessler.com/en/topic/373

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

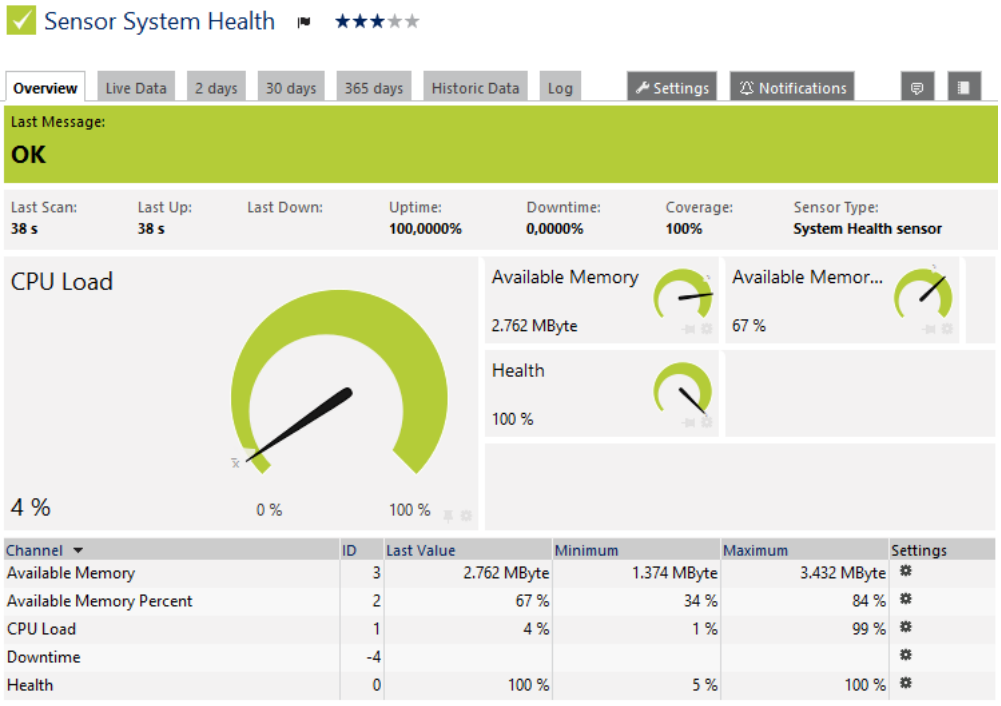
For more general information about settings, please see the **Object Settings** 188 section.

7.8.193 System Health Sensor

The System Health sensor monitors internal PRTG parameters. It shows the status of the system on which a probe runs. PRTG creates this sensor type automatically and cannot be deleted.

It checks various parameters of your PRTG system that can affect the quality of the monitoring results:

- **Health**: This index value sums up the probe state into a value between 100% (healthy) and 0% (failing). Frequent or repeated health values below 100% should be investigated.
- **Available Memory**: This channel shows the amount of free memory available on the system. This value should not fall below 500 MB. This way, PRTG can still request resources during report generation, auto-discoveries, and other issues.
- **Available Memory Percent**: This channel shows the free memory available on the system in percent.
- **System CPU Load**: This channel shows the current percentage CPU load on the system with the probe. Extensive CPU load can lead to false, incomplete, and incorrect monitoring results. This value should usually stay below 50%.



System Health Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/system_health.png

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel.

SENSOR DISPLAY

	▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. ⓘ This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.

SCANNING INTERVAL

- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

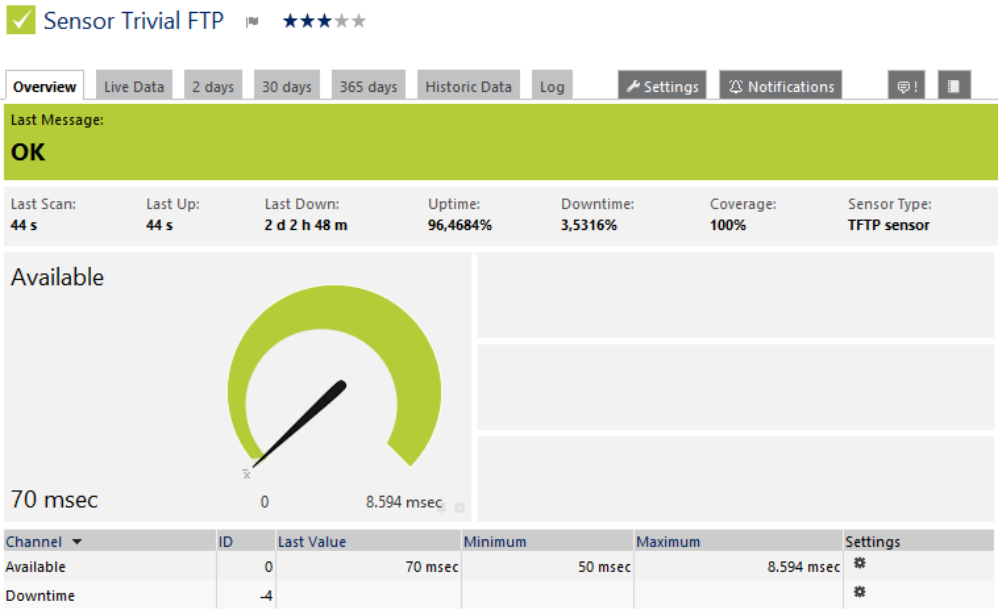
Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.194 TFTP Sensor

The TFTP sensor monitors a Trivial File Transfer Protocol (TFTP) server and checks if a certain file is available for download.

- It shows the response time of the server.



TFTP Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/tftp.png

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SPECIFIC

Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).
Port	Enter the number of the port the TFTP service is running on. The sensor connects to this port. Please enter an integer value.
Filename	Enter the name of the file that this sensor checks. If this file name is not available on the server, the sensor shows a **Down** status 163. Please enter a string.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

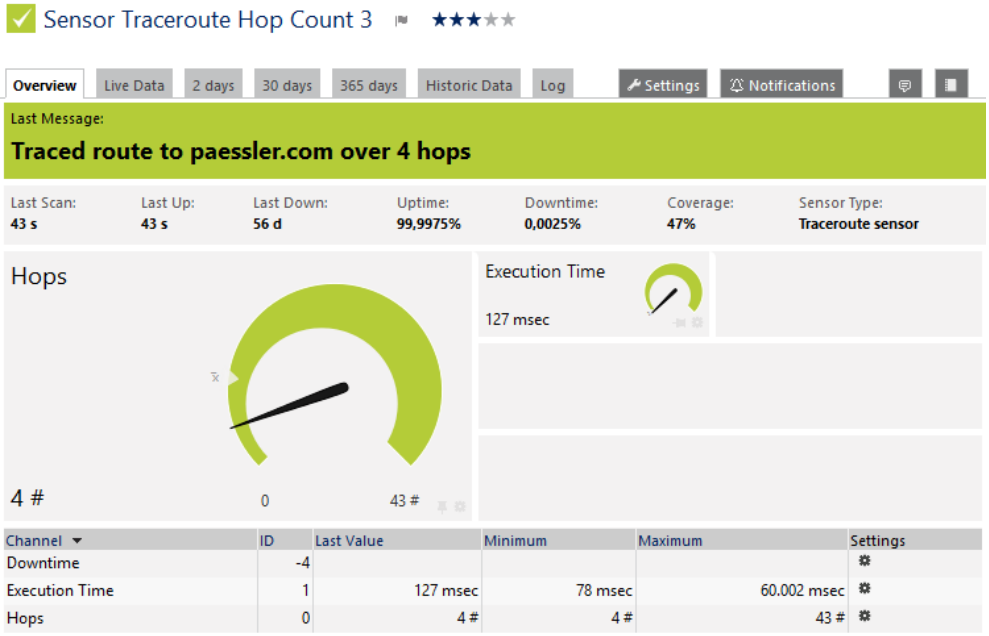
For more general information about settings, please see the **Object Settings** 188 section.

7.8.195 Traceroute Hop Count Sensor

The Traceroute Hop Count sensor traces the number of hops needed from the probe system the sensor is running on to the **IP Address/DNS Name** defined in the sensor's parent device.

It shows the following:

- Execution time
- Number of hops
- If the number of hops (the route) changes, you can additionally define another sensor status [163].



Traceroute Hop Count Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/traceroute_hop_count.png

Remarks

- Requires [2336] .NET 4.0 or 4.5 to be installed on the probe system. If the sensor shows the error PE087, please additionally install .NET 3.5 on the probe system.
- We recommend Windows 2012 R2 on the probe system for best performance of this sensor.
- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.

Requirement: .NET Framework

This sensor type requires the Microsoft .NET Framework to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the remote probe 3196. If the framework is missing, you cannot create this sensor.

Required .NET version (with latest updates): .NET 4.0 (Client Profile is sufficient), .NET 4.5, or .NET 4.6.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/60543

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

BASIC SENSOR SETTINGS

	You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SETTINGS

If Route Changes	Define what to do if the route has changed since the last check. Choose between: ▪ **Ignore**: Do not perform any action. ▪ **Set sensor to "Warning"**: Set the sensor to **Warning** status. ▪ **Set sensor to "Error"**: Set the sensor to **Down** status.

DEBUG OPTIONS

Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section **Data Storage** 3226. You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: Which .NET version does PRTG require?

- https://kb.paessler.com/en/topic/60543

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.196 VMware Datastore (SOAP) Sensor

The VMware Datastore (SOAP) sensor monitors the disk usage of a VMware data store using Simple Object Access Protocol (SOAP). It can show the following:

- Available capacity in bytes: This is the physically or virtually available size of the data store.
- Free space in bytes and percent: This is the disk space that is not used by virtual machines. Used disk space can be either thick-provisioned or used from thin-provisioned virtual disks.
- Uncommitted bytes: This is the disk space that is provisioned for thin-provisioned virtual machines but not used yet.
- Total provisioned disk space in percent: This is the sum of all potentially used disk space of thin-provisioned and thick-provisioned VM hard drives (uncommitted bytes plus used bytes).
- Accessibility of the data store

VMware Datastore (SOAP) Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/vmware_datastore_soap.png

Remarks

- Requires 2345 .NET 4.0 or higher to be installed on the probe system.
- For this sensor type you must define credentials for VMware servers on the device you want to use the sensor on. Ensure you enter a user with sufficient access rights to obtain statistics (read-only usually works).
- The parent device must be a VMware ESXi server version 5.0, 5.1, 5.5, or 6.0 or vCenter.

- We recommend Windows 2012 R2 on the probe system for best performance of this sensor.
- This sensor type supersedes the outdated SSH VMWare ESX(i) Disk sensor. We recommend that you use this new sensor to monitor VMware data stores.
- Knowledge Base: I cannot add VMware sensors because of "wrong" password although it is correct. What can I do?
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.
- This sensor type has predefined limits for several metrics. You can change these limits individually in the channel settings. For detailed information about channel limits, please refer to the manual section **Sensor Channels Settings** 2782.

Requirement: .NET Framework

This sensor type requires the Microsoft .NET Framework to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the remote probe 3196. If the framework is missing, you cannot create this sensor.

Required .NET version (with latest updates): .NET 4.0 (Client Profile is sufficient), .NET 4.5, or .NET 4.6.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/60543

Settings on VMware Host System

If you set up this sensor on different probes (for example, when using remote probes 3196 or when running a cluster 116 setup), you might need to change the settings of your VMware host, so it accepts more incoming connections. Otherwise you might get connection timeouts when running plenty of VMware sensors with a short scanning interval.

For details about this setting, please see **More** section below.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the data stores you want to monitor. PRTG creates one sensor for each data store you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

DATASTORE SETTINGS

Datastore	Select all data stores for which you want to add a sensor. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DATASTORE SETTINGS

MoID	Shows the Managed Object ID (MoID) of the data store that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

DEBUG OPTIONS

Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section **Data Storage** 3226. You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel.

SENSOR DISPLAY

	▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. ⓘ This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.

SCANNING INTERVAL

- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: How can I increase the connection limit on VMware systems?

- https://kb.paessler.com/en/topic/30643

Knowledge Base: Monitoring ESXi 5.1 and higher: Handshake Failure on Windows XP/Server 2003

- https://kb.paessler.com/en/topic/59173

Knowledge Base: For which sensor types do you recommend Windows Server 2012 R2 and why?

- https://kb.paessler.com/en/topic/64331

Knowledge Base: I cannot add VMware sensors because of "wrong" password although it is correct. What can I do?

- https://kb.paessler.com/en/topic/66794

Knowledge Base: Which .NET version does PRTG require?

- https://kb.paessler.com/en/topic/60543

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

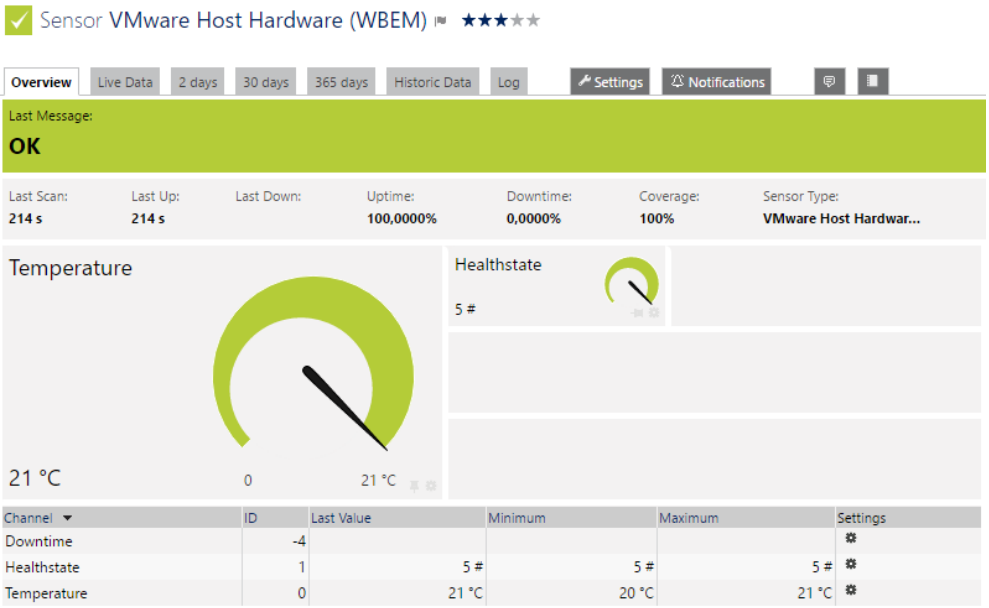
7.8.197 VMware Host Hardware (WBEM) Sensor

The VMware Host Hardware sensor monitors hardware information of an ESX/ESXi server using Web-Based Enterprise Management (WBEM).

It can show the following, depending on the selected ESX component:

- Health status
- Temperature
- Power
- Fan rotations per minute (RPM)
- Battery voltage

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



VMware Host Hardware (WBEM) Sensor

Click here to enlarge: https://media-s3.paessler.com/prtg-screenshots/vmware_host_hardware_wbem.png

Remarks

- The parent device must be a VMware ESXi server version 5.0, 5.1, 5.5, or 6.0.
- For this sensor type you must define credentials for Linux/Solaris/Mac OS (SSH/WBEM) systems on the device you want to use the sensor on.
- We recommend Windows 2012 R2 on the probe system for best performance of this sensor.
- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the ESX components you want to monitor. PRTG creates one sensor for each hardware element you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

ESX SERVER ELEMENTS

ESX Element	Select the hardware elements you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	Enter one or more **Tags**, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

ESX SERVER ELEMENTS

Element	Shows the ESX element that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Automatic Sensor State	Define if the sensor will change its status dependent on the health state reading. Choose between: ▪ **Set sensor state automatically to 'Warning' or 'Down'**: Set the sensor to a **Warning** or **Down** status when the server returns respective values. The sensor will additionally change to a **Down** status if the connection to the server fails. ▪ **Just report the current reading, ignore Server Health Value**: Never change the sensor's status dependent on the values returned by the server. The sensor will only change to a **Down** status if the connection to the server fails.
Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result.

ESX SERVER ELEMENTS

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section **Data Storage** 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. ⓘ Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

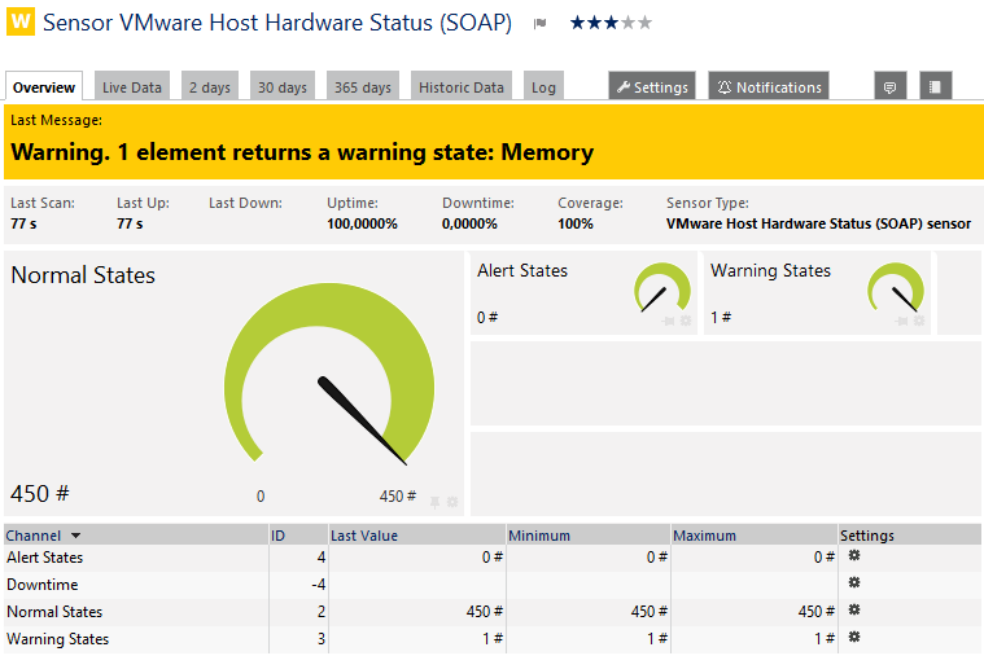
For more general information about settings, please see the **Object Settings** 188 section.

7.8.198 VMware Host Hardware Status (SOAP) Sensor

The VMware Host Hardware Status (SOAP) sensor monitors the hardware status of a VMware host server using Simple Object Access Protocol (SOAP).

- It shows the total number of items in "Normal", "Warning," and "Alert" status, just as the vSphere client reports.

This sensor is intended to give you a general status overview for your host. Any states other than "Normal" will be reported in the sensor message.



VMware Host Hardware Status (SOAP) Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/vmware_host_hardware_status_soap.png

Remarks

- Requires 2363 .NET 4.0 or higher to be installed on the probe system.
- For this sensor type you must define credentials for VMware servers on the device you want to use the sensor on. Ensure you enter a user with sufficient access rights to obtain statistics (read-only usually works).
- This sensor only shows items that report an actual status, so you might see more "sensors" in your vSphere client than the number of states available in the channels of this PRTG sensor.
- The parent device must be a VMware ESXi server version 5.0, 5.1, 5.5, or 6.0. We recommend that you do not use this sensor type on your vCenter. Reliable hardware information can only be provided when this sensor is created on your physical host server as parent device.
- We recommend Windows 2012 R2 on the probe system for best performance of this sensor.

- Knowledge Base: I cannot add VMware sensors because of "wrong" password although it is correct. What can I do?
- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.

Requirement: .NET Framework

This sensor type requires the Microsoft .NET Framework to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the remote probe 3196. If the framework is missing, you cannot create this sensor.

Required .NET version (with latest updates): .NET 4.0 (Client Profile is sufficient), .NET 4.5, or .NET 4.6.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/60543

Settings on VMware Host System

If you set up this sensor on different probes (for example, when using remote probes 3196 or when running a cluster 116 setup), you might need to change the settings of your VMware host, so it accepts more incoming connections. Otherwise you might get connection timeouts when running plenty of VMware sensors with a short scanning interval.

For details about this setting, please see **More** section below.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the VMware hosts you want to monitor. PRTG creates on sensor for each host server you select in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

VMWARE HOST SETTINGS

Host Server	Select the host server you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

VMWARE HOST SETTINGS

MoID	Shows the Managed Object ID (MoID) of the host that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Known Warnings	Enter one or more semicolon (;) separated warning messages from the VMware host that you want to ignore. Messages that you enter here will not affect the sensor status. Please enter a string or leave the field empty. We strongly recommend that you use this filter for known issues only. For example, various systems (mainly HP and IBM systems) return unknown states because of errors in the the vendors' CIM extensions. Because of this, you might not get an **Up** status 163 for this sensor at all although your vSphere client does not show warnings. In this case, use this filter option and enter the known warning message(s), for example, Power Supply 7;Power Supply 8
Known Errors	Enter one or more semicolon (;) separated error messages from the VMware host that you want to ignore. Messages that you enter here will not affect the sensor status. Please enter a string or leave the field empty. We strongly recommend that you use this filter for known issues only. For example, various systems (mainly HP and IBM systems) return unknown states because of errors in the the vendors' CIM extensions. Because of this, you might not get an **Up** status 163 for this sensor at all although your vSphere client does not show errors. In this case, use this filter option and enter the known error message(s), for example, Power Supply 7;Power Supply 8

DEBUG OPTIONS

Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result.

DEBUG OPTIONS

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section **Data Storage** 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.
- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. ⓘ Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: How can I increase the connection limit on VMware systems?

- https://kb.paessler.com/en/topic/30643

Knowledge Base: Monitoring ESXi 5.1 and higher: Handshake Failure on Windows XP/Server 2003

- https://kb.paessler.com/en/topic/59173

Knowledge Base: For which sensor types do you recommend Windows Server 2012 R2 and why?

- https://kb.paessler.com/en/topic/64331

Knowledge Base: I cannot add VMware sensors because of "wrong" password although it is correct. What can I do?

- https://kb.paessler.com/en/topic/66794

Knowledge Base: Which .NET version does PRTG require?

- https://kb.paessler.com/en/topic/60543

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.199 VMware Host Performance (SOAP) Sensor

The VMware Host Performance (SOAP) sensor monitors a VMware host server using Simple Object Access Protocol (SOAP).

It can show the following:

- CPU usage in percent
- CPU ready in percent
- Network usage
- Disk usage
- Disk read and write speed
- Active memory in bytes
- Consumed memory in bytes and percent
- Used memory swap
- Disk and data store latency (read and write)
- Network received and transmitted speed
- Power status

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

VMware Host Performance (SOAP) Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/vmware_host_performance_soap.png

Remarks

- Requires 2374 .NET 4.0 or higher to be installed on the probe system.
- For this sensor type you must define credentials for VMware servers on the device you want to use the sensor on. Ensure you enter a user with sufficient access rights to obtain statistics (read-only usually works).

- The parent device must be a VMware ESXi server version 5.0, 5.1, 5.5, or 6.0. We recommend that you do not use this sensor type on your vCenter. Reliable hardware information can only be provided when this sensor is created on your physical host server as parent device.
- We recommend Windows 2012 R2 on the probe system for best performance of this sensor.
- Knowledge Base: I cannot add VMware sensors because of "wrong" password although it is correct. What can I do?
- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.

Requirement: .NET Framework

This sensor type requires the Microsoft .NET Framework to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the remote probe 3196. If the framework is missing, you cannot create this sensor.

Required .NET version (with latest updates): .NET 4.0 (Client Profile is sufficient), .NET 4.5, or .NET 4.6.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/60543

Settings on VMware Host System

If you set up this sensor on different probes (for example, when using remote probes 3196 or when running a cluster 116 setup), you might need to change the settings of your VMware host, so it accepts more incoming connections. Otherwise you might get connection timeouts when running plenty of VMware sensors with a short scanning interval.

For details about this setting, please see **More** section below.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

VMWARE HOST SETTINGS

MoID	Shows the Managed Object ID (MoID) of the host that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

DEBUG OPTIONS

Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result.

DEBUG OPTIONS

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section **Data Storage** 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.
- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: How can I increase the connection limit on VMware systems?

- https://kb.paessler.com/en/topic/30643

Knowledge Base: Monitoring ESXi 5.1 and higher: Handshake Failure on Windows XP/Server 2003

- https://kb.paessler.com/en/topic/59173

Knowledge Base: For which sensor types do you recommend Windows Server 2012 R2 and why?

- https://kb.paessler.com/en/topic/64331

Knowledge Base: I cannot add VMware sensors because of "wrong" password although it is correct. What can I do?

- https://kb.paessler.com/en/topic/66794

Knowledge Base: Which .NET version does PRTG require?

- https://kb.paessler.com/en/topic/60543

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.200 VMware Virtual Machine (SOAP) Sensor

The VMware Virtual Machine (SOAP) sensor monitors a virtual machine on a VMware host server using Simple Object Access Protocol (SOAP).

It shows the following:

- CPU usage in percent
- CPU ready in percent
- Active memory in bytes
- Consumed memory in bytes and percent
- Disk read and write speed
- Read and write latency
- Network usage (total, received, and transmitted bytes per second)

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

Channel	ID	Last Value	Minimum	Maximum	Settings
CPU ready (Percent)	10	0,63 %	0,04 %	6,865 %	
CPU usage	2	4,48 %	0 %	46,49 %	
Datastore total ReadLatency	8	0 msec	0 msec	65 msec	
Datastore total WriteLatency	3	0 msec	14 msec	473 msec	
Disk read	11	0 Mbit/s	0 Mbit/s	92 Mbit/s	
Disk usage	13	0 Mbit/s	0 Mbit/s	255 Mbit/s	
Disk write	14	0 Mbit/s	0 Mbit/s	177 Mbit/s	
Downtime	-4				
Memory active	4	184 MByte	0 MByte	6.083 MByte	
Memory consumed	5	6.011 MByte	3.327 MByte	6.012 MByte	
Memory consumed (Percent)	12	97,84 %	54,15 %	97,85 %	
Network received	7	36 KByte/s	0 KByte/s	8.314 KByte/s	
Network transmitted	6	4 KByte/s	0 KByte/s	7.990 KByte/s	
Network usage	9	41 KByte/s	0 KByte/s	16.304 KByte/s	
Power	15	2 #	1 #	18 #	

VMware Virtual Machine (SOAP) Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/vmware_virtual_machine_soap.png

Remarks

- Requires 2384 .NET 4.0 or higher to be installed on the probe system.
- For this sensor type you must define credentials for VMware servers on the device you want to use the sensor on. Ensure you enter a user with sufficient access rights to obtain statistics (read-only usually works).
- We recommend that you use vCenter as parent device. When the monitored VM changes the host server via vMotion, PRTG can continue monitoring in this case. The sensor can monitor VMware ESXi server version 5.0, 5.1, 5.5, or 6.0.
- We recommend Windows 2012 R2 on the probe system for best performance of this sensor.

- For VMware virtual machines, disk usage channels are only available as of virtual hardware version 8.
- Knowledge Base: I cannot add VMware sensors because of "wrong" password although it is correct. What can I do?
- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.

Requirement: .NET Framework

This sensor type requires the Microsoft .NET Framework to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the remote probe 3196. If the framework is missing, you cannot create this sensor.

Required .NET version (with latest updates): .NET 4.0 (Client Profile is sufficient), .NET 4.5, or .NET 4.6.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/60543

Settings on VMware Host System

If you set up this sensor on different probes (for example, when using remote probes 3196 or when running a cluster 116 setup), you might need to change the settings of your VMware host, so it accepts more incoming connections. Otherwise you might get connection timeouts when running plenty of VMware sensors with a short scanning interval.

For details about this setting, please see **More** section below.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

PRTG requests a full list of all virtual machines configured on the device. Because of this, it may take a few seconds before the dialog is loaded.

Select the VMware virtual machines you want to monitor. PRTG creates one sensor for each virtual machine you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

VIRTUAL MACHINE SETTINGS

Virtual Machine	You see a list of all virtual machines (VMs) available on the host server on this device, including the ones that are not running. All VMs are listed by name and the OS they are running on. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

VMWARE VIRTUAL MACHINE SETTINGS

MoID	Shows the Managed Object ID (MoID) of the virtual machine that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Handling of "Powered Off" VM	Define how the sensor will react to a virtual machine that is powered off. Choose between: • **Ignore "powered off" state (default)**: The sensor will not change to a **Down** status 163 if the virtual machine is powered off. It will report zero values instead. • **Alarm when VM is "powered off"**: The sensor will change to a **Down** 163 status if the virtual machine is powered off. Note: While in Down status, a sensor does not record any data in any of its channels.

DEBUG OPTIONS

Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section **Data Storage** 3226. You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: How can I increase the connection limit on VMware systems?

- https://kb.paessler.com/en/topic/30643

Knowledge Base: Monitoring ESXi 5.1 and higher: Handshake Failure on Windows XP/Server 2003

- https://kb.paessler.com/en/topic/59173

Knowledge Base: For which sensor types do you recommend Windows Server 2012 R2 and why?

- https://kb.paessler.com/en/topic/64331

Knowledge Base: I cannot add VMware sensors because of "wrong" password although it is correct. What can I do?

- https://kb.paessler.com/en/topic/66794

Knowledge Base: Which .NET version does PRTG require?

- https://kb.paessler.com/en/topic/60543

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

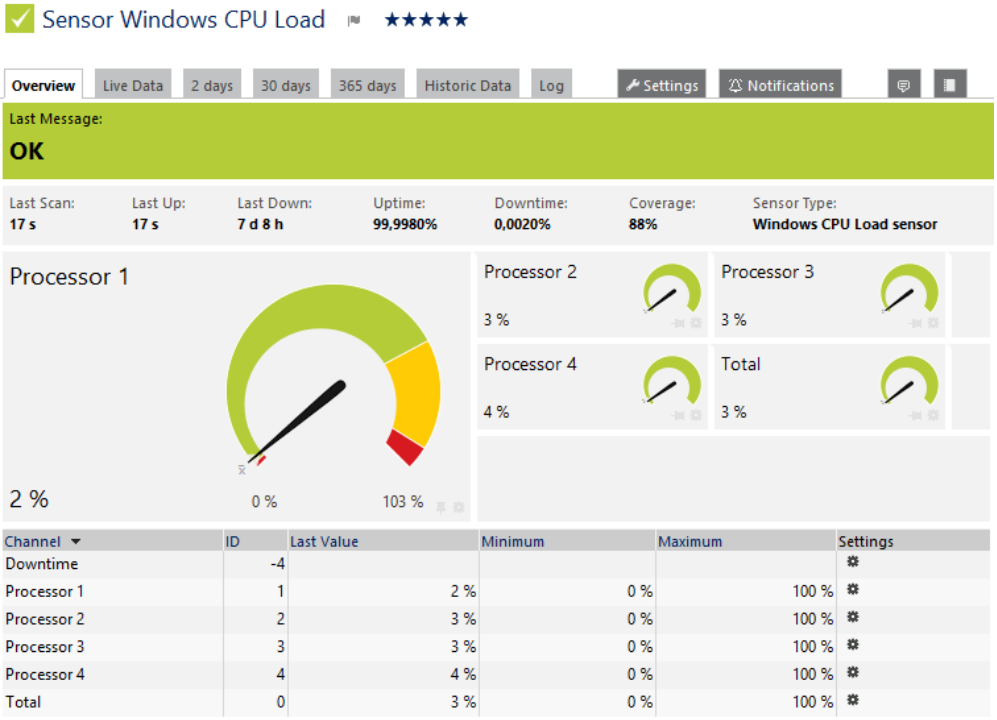
Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.201 Windows CPU Load Sensor

The Windows CPU Load sensor monitors the CPU load on a computer via Windows Management Instrumentation (WMI) or Windows Performance Counters, as configured in the "Windows Compatibility Options" of the parent device.

- It shows the CPU usage of all processors and the total load in percent.



Windows CPU Load Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/windows_cpu_load.png

Remarks

- Requires 2394 Windows credentials in the parent device settings 360.
- Requires 2394 Windows 2008 or later on the probe system.
- Requires 2394 the Windows Remote Registry service to be running on the target computer.
- Can use a hybrid approach 2394 to query monitoring data: Performance counters as standard approach and WMI as fallback.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Requirement: Windows Credentials

Requires credentials for Windows systems to be defined for the device you want to use the sensor on. In the parent device's 365 **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. Otherwise, a connection via Performance Counters will not be possible. However, WMI connections may still work.

Hybrid Approach: Performance Counters and WMI

By default, this sensor type uses Windows Management Instrumentation (WMI) to request monitoring data. You can change the default behavior to a hybrid approach in the **Windows Compatibility Options** of the parent device's settings 372 on which you create this sensor: if you choose this option, the sensor will first try to query data via Windows Performance Counters and use WMI as a fallback if Performance Counters are not available. When running in fallback mode, the sensor will re-try to connect via Performance Counters after 24 hours.

Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per probe 111. Above this number, please consider using multiple **Remote Probes** 3196 for load balancing.

For a general introduction to the technology behind WMI, please see **Monitoring via WMI** 3092 section.

Requirement: Windows Version

In order for this sensor to work with Windows Performance Counters, please make sure a Windows version 2008 or later is installed on the computer running the PRTG probe: This is either on the local system (on every node, if on a cluster probe), or on the system running a remote probe 3196.

Requirement: Remote Registry Service

In order for this sensor to work with Windows Performance Counters, please make sure the Remote Registry Windows service is running on the target computer. If you fail to do so, a connection via Performance Counters will not be possible. However, WMI connections may still work.

To enable the service, please log in to the respective computer and open the services manager (for example, via services.msc). In the list, find the respective service and set its Start Type to Automatic.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DEBUG OPTIONS

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result**: Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section Data Storage 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

WMI ALTERNATIVE QUERY

Errors and Invalid Data

This is an extended help field only. PRTG's WMI sensors are equipped with the most efficient and accurate WMI queries. However, Microsoft has changed (and will continue to do so in the future) some WMI classes over the various Windows/ServicePack/ patchlevel versions, resulting in errors like "class not valid" or "invalid data". Wherever possible, PRTG features an alternative query that might work in your specific configuration. If you keep getting errors for this sensor, please try enabling the alternative query method below.

Alternative Query

Choose the method PRTG uses to query via WMI. For compatibility reasons, you can enable an alternative query method. We recommend that you use the default value. You can choose between:

- **Use default (recommended)**: Use PRTG's standard method to query WMI. This is the best setting in most cases.
- **Use alternative (if default does not work)**: Use an alternative method to query WMI. If you keep getting errors with the default setting, please try this setting.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: My Windows sensors do not work when using direct Performance Counter access. What can I do?

- https://kb.paessler.com/en/topic/47263

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.202 Windows IIS 6.0 SMTP Received Sensor

The Windows IIS 6.0 SMTP Receiver Sensor monitors Microsoft's Internet Information Services regarding the number of received emails for an IIS 6.0 SMTP service (Exchange 2003) using Windows Management Instrumentation (WMI) or Windows Performance Counters, as configured in the "Windows Compatibility Options" of the parent device.

- It shows the number and bytes of received messages.

Remarks

- Requires 2403 Windows credentials in the parent device settings 360.
- Requires 2404 Windows 2008 or later on the probe system.
- Requires 2404 the Windows Remote Registry service to be running on the target computer.
- Can use a hybrid approach 2403 to query monitoring data: Performance counters as standard approach and WMI as fallback.
- This service is not used by Exchange Server 2007 and higher. Exchange Server 2007 uses its own SMTP stack implemented in the Microsoft Exchange Transport service.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Requirement: Windows Credentials

Requires credentials for Windows systems to be defined for the device you want to use the sensor on. In the parent device's 365 **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. Otherwise, a connection via Performance Counters will not be possible. However, WMI connections may still work.

Hybrid Approach: Performance Counters and WMI

By default, this sensor type uses Windows Management Instrumentation (WMI) to request monitoring data. You can change the default behavior to a hybrid approach in the **Windows Compatibility Options** of the parent device's settings 372 on which you create this sensor: if you choose this option, the sensor will first try to query data via Windows Performance Counters and use WMI as a fallback if Performance Counters are not available. When running in fallback mode, the sensor will re-try to connect via Performance Counters after 24 hours.

Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per probe 111. Above this number, please consider using multiple **Remote Probes** 3196 for load balancing.

For a general introduction to the technology behind WMI, please see **Monitoring via WMI** 3092 section.

Requirement: Windows Version

In order for this sensor to work with Windows Performance Counters, please make sure a Windows version 2008 or later is installed on the computer running the PRTG probe: This is either on the local system (on every node, if on a cluster probe), or on the system running a remote probe 3196.

Requirement: Remote Registry Service

In order for this sensor to work with Windows Performance Counters, please make sure the Remote Registry Windows service is running on the target computer. If you fail to do so, a connection via Performance Counters will not be possible. However, WMI connections may still work.

To enable the service, please log in to the respective computer and open the services manager (for example, via services.msc). In the list, find the respective service and set its Start Type to Automatic.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DEBUG OPTIONS

Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section **Data Storage** 3226. You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

SENSOR DISPLAY

	You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

SCANNING INTERVAL

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: My Windows sensors do not work when using direct Performance Counter access. What can I do?

- https://kb.paessler.com/en/topic/47263

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.203 Windows IIS 6.0 SMTP Sent Sensor

The Windows IIS 6.0 SMTP Sent Sensor monitors Microsoft's Internet Information Services regarding the number of sent emails for an IIS 6.0 SMTP service (Exchange 2003) using Windows Management Instrumentation (WMI) or Windows Performance Counters, as configured in the "Windows Compatibility Options" of the parent device.

It shows the following:

- Number and bytes of sent messages
- Number of retries per second for sent messages

Remarks

- Requires 2412 Windows credentials in the parent device settings 360.
- Requires 2413 Windows 2008 or later on the probe system.
- Requires 2413 the Windows Remote Registry service to be running on the target computer.
- Can use a hybrid approach 2412 to query monitoring data: Performance counters as standard approach and WMI as fallback.
- This service is not used by Exchange Server 2007 and higher. Exchange Server 2007 uses its own SMTP stack implemented in the Microsoft Exchange Transport service.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Requirement: Windows Credentials

Requires credentials for Windows systems to be defined for the device you want to use the sensor on. In the parent device's 365 **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. Otherwise, a connection via Performance Counters will not be possible. However, WMI connections may still work.

Hybrid Approach: Performance Counters and WMI

By default, this sensor type uses Windows Management Instrumentation (WMI) to request monitoring data. You can change the default behavior to a hybrid approach in the **Windows Compatibility Options** of the parent device's settings 372 on which you create this sensor: if you choose this option, the sensor will first try to query data via Windows Performance Counters and use WMI as a fallback if Performance Counters are not available. When running in fallback mode, the sensor will re-try to connect via Performance Counters after 24 hours.

Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per probe 111. Above this number, please consider using multiple **Remote Probes** 3196 for load balancing.

For a general introduction to the technology behind WMI, please see **Monitoring via WMI** 3092 section.

Requirement: Windows Version

In order for this sensor to work with Windows Performance Counters, please make sure a Windows version 2008 or later is installed on the computer running the PRTG probe: This is either on the local system (on every node, if on a cluster probe), or on the system running a remote probe 3196.

Requirement: Remote Registry Service

In order for this sensor to work with Windows Performance Counters, please make sure the Remote Registry Windows service is running on the target computer. If you fail to do so, a connection via Performance Counters will not be possible. However, WMI connections may still work.

To enable the service, please log in to the respective computer and open the services manager (for example, via services.msc). In the list, find the respective service and set its Start Type to Automatic.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.

BASIC SENSOR SETTINGS

Parent Tags	Shows **Tags** [124] that this sensor inherits [124] from its parent device, group, and probe [118]. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** [124], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited [124] from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DEBUG OPTIONS

Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section **Data Storage** [3226]. You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: My Windows sensors do not work when using direct Performance Counter access. What can I do?

- https://kb.paessler.com/en/topic/47263

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

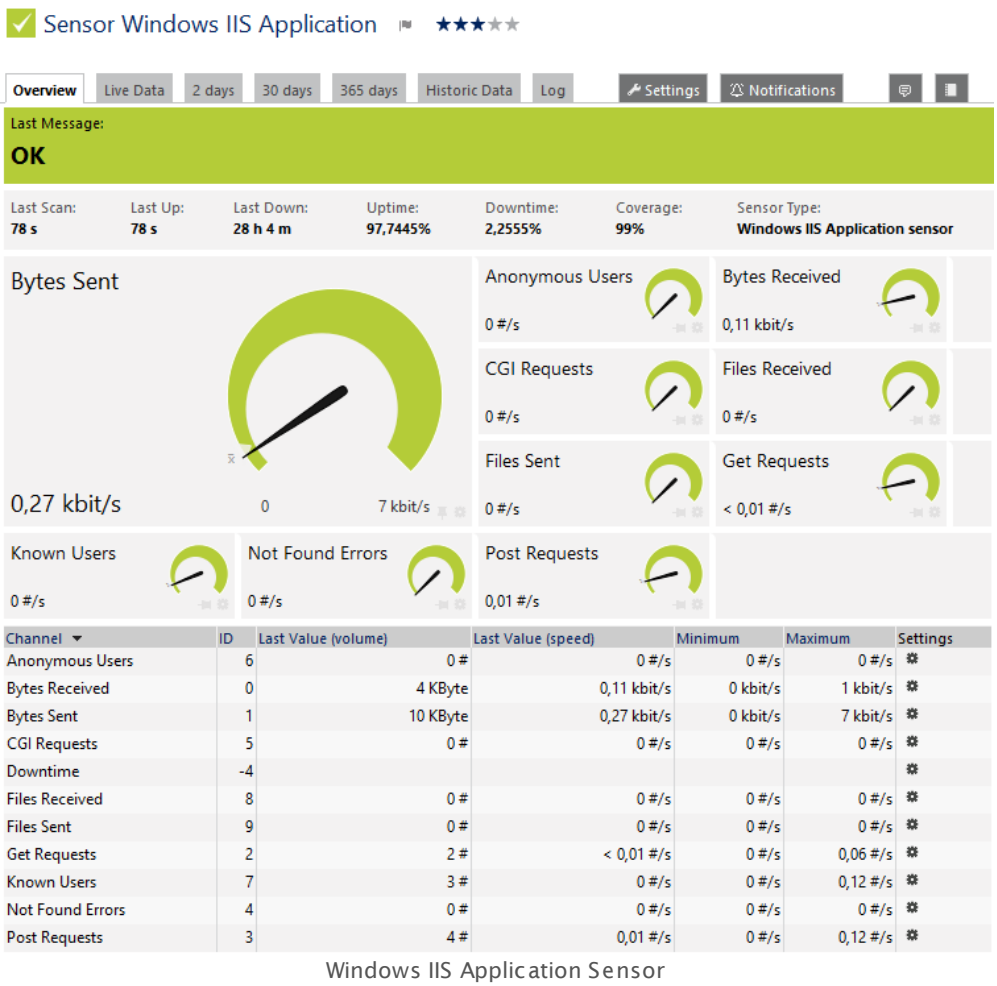
For more general information about settings, please see the **Object Settings** 188 section.

7.8.204 Windows IIS Application Sensor

The Windows IIS Application sensor monitors a Microsoft Internet Information Services server via Windows Management Instrumentation (WMI). It can also monitor applications that use IIS, such as Microsoft SharePoint or Microsoft Reporting Services (SSRS).

It shows the following:

- Sent and received bytes per second
- Number of sent and received files per second
- Number of anonymous and known users per second
- Number of Common Gateway Interface (CGI) requests per second
- Number of GET and POST requests per second
- Number of not found errors per second



Windows IIS Application Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/windows_iis_application.png

Remarks

- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per probe 111. Above this number, please consider using multiple **Remote Probes** 3196 for load balancing.
- For a general introduction to the technology behind WMI, please see manual section **Monitoring via WMI** 3092.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the web service instances you want to monitor. PRTG creates one sensor for each instance you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

WMI INTERNET INFORMATION SERVICES

Specify Instance	You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

WMI INTERNET INFORMATION SERVICES

Instance	Shows the name of the web service instance that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

DEBUG OPTIONS

Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result.

DEBUG OPTIONS

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section **Data Storage** 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. ⓘ Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

My WMI sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/1043

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

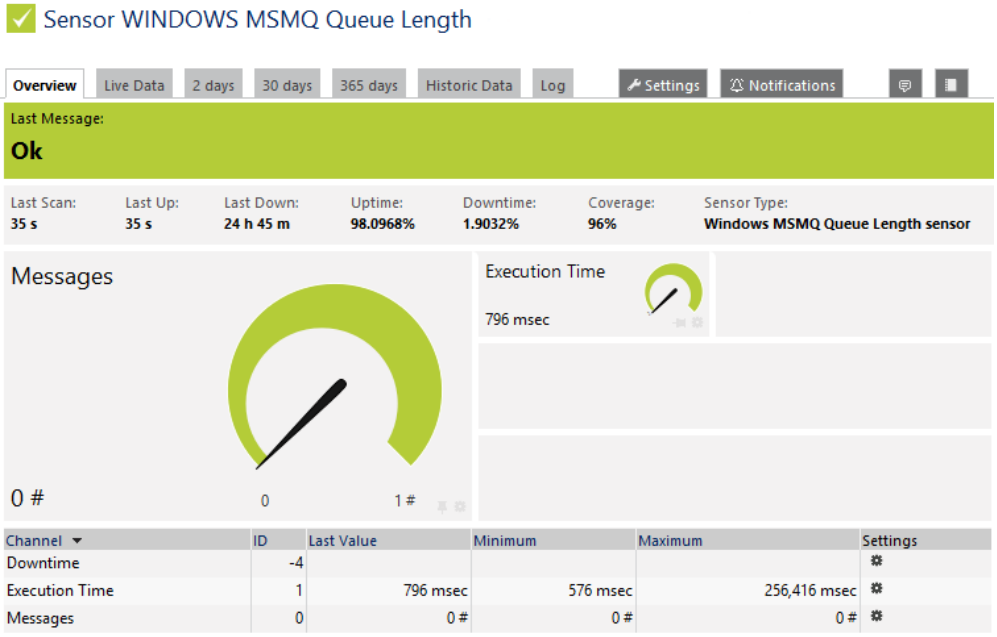
For more general information about settings, please see the **Object Settings** 188 section.

7.8.205 Windows MSMQ Queue Length Sensor

The Windows MSMQ Queue Length sensor reads the number of messages in a Microsoft Message Queue of the parent device.

It shows the following:

- Total number of messages in the queue
- Execution time



Windows MSMQ Queue Length Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/windows_msmq_queue_length.png

Remarks

- Requires 2431 .NET 4.0 or 4.5 to be installed on the probe system.
  If the sensor shows the error PE087, please additionally install .NET 3.5 on the probe system.
- Requires 2431 Windows credentials in the parent device settings 360.
- Requires 2431 the MSMQ service to be running on both the probe and the target system.
- We recommend Windows 2012 R2 on the probe system for best performance of this sensor.
- Knowledge Base: How do I activate Message Queuing in my Windows installation?
- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Requirement: .NET Framework

This sensor type requires the Microsoft .NET Framework to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the remote probe 3196. If the framework is missing, you cannot create this sensor.

Required .NET version (with latest updates): .NET 4.0 (Client Profile is sufficient), .NET 4.5, or .NET 4.6.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/60543

Requirement: Windows Credentials

Requires credentials for Windows systems to be defined for the device you want to use the sensor on. In the parent device's 365 **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

If you use local credentials, please make sure that the same Windows user accounts (with the same username and password) exist on both the system running the PRTG probe and the target computer. Otherwise the sensor cannot connect correctly.

Requirement: Message Queuing Service

In order for this sensor to work, the MSMQ "Message Queuing" service must be started both on the target system and on the computer running the PRTG probe: Either on the local system (on every node, if on a cluster probe), or on the system running the remote probe 3196. Additionally, the MSMQ "Message Queuing" service must also be started on the target computer.

To enable the service, please log in to the respective computer and open the services manager (for example, via services.msc). In the list, find the respective service and set its Start Type to Automatic.

Depending on your Windows version you may first need to install the Microsoft Message Queue (MSMQ) Server.

When installing Microsoft Message Queue (MSMQ) Server, make sure you install it including the Directory Service. Depending on your Windows installation this might have a different name, such as

- MSMQ Active Directory Domain Service Integration
- Directory Service Integration
- Active Directory Integration

For details, please see **More** 2439 section below.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the message queues you want to monitor. PRTG creates one sensor for each queue you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SENSOR SETTINGS

Message Queue	You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items. If there are no message queues available, you will see a corresponding message. ⓘ This sensor cannot monitor sub-queues.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

ⓘ Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.

BASIC SENSOR SETTINGS

Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SETTINGS

Message Queue	Shows the name of the queue that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Message Queue Type	Shows the type of the queue that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Min. Message Age	Optionally define an age in minutes the message has to be old to be counted. If set, messages younger than this age are not regarded. If you leave this field blank, the sensor will not check for the message age. Please enter an integer value or leave the field empty.
If Value Changes	Define what this sensor will do when the sensor value changes. You can choose between: ▪ **Ignore changes (default)**: The sensor takes no action on change.

SENSOR SETTINGS

- **Trigger 'change' notification**: The sensor sends an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification 2791 whenever the sensor value changes.

DEBUG OPTIONS

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result**: Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section **Data Storage** 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.

SCANNING INTERVAL

- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies [2822] in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector [210] to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** [360] or in the superior **Group Settings** [334].

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: How do I activate Message Queuing in my Windows installation?

- https://kb.paessler.com/en/topic/25963

Knowledge Base: Which .NET version does PRTG require?

- https://kb.paessler.com/en/topic/60543

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

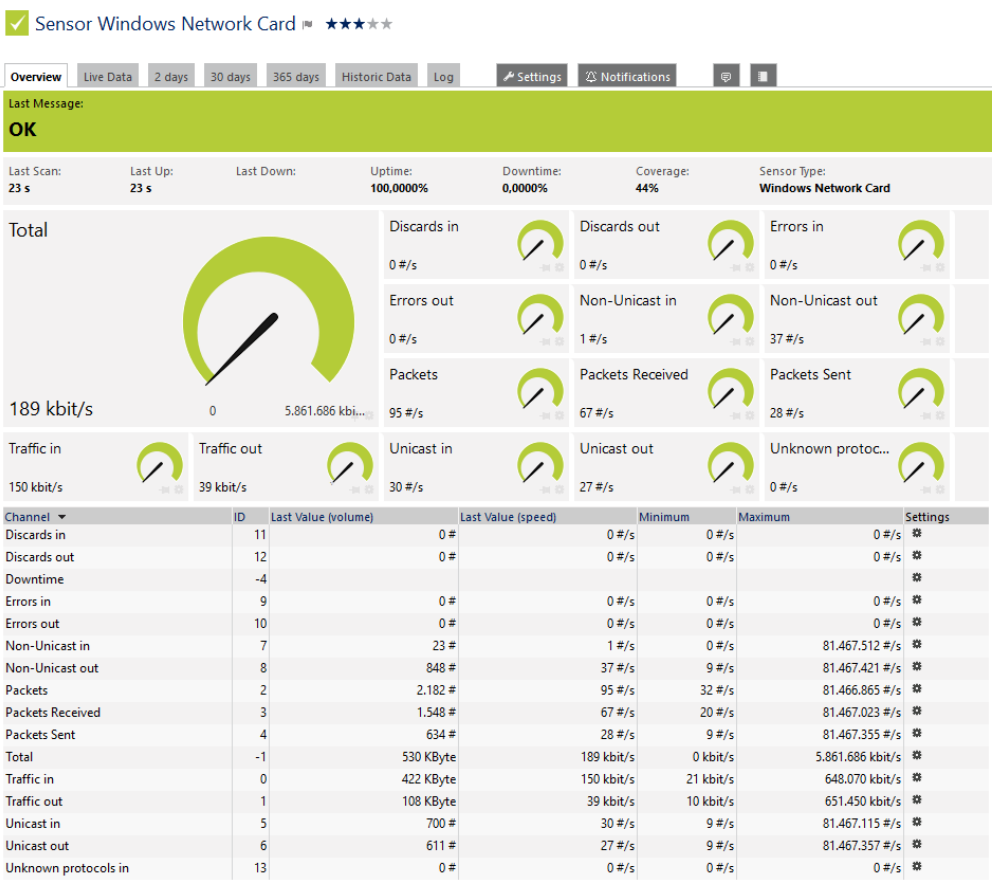
7.8.206 Windows Network Card Sensor

The Windows Network Card sensor monitors bandwidth usage and traffic of a network interface using Windows Management Instrumentation (WMI) or Windows Performance Counters, as configured in the "Windows Compatibility Options" of the parent device.

It can show the following:

- Total traffic on the network card
- Traffic in and traffic out
- Number of received and sent packets
- Total number of packets
- Number of discards (in and out)
- Number of errors (in and out)
- Number of unicast packets (in and out)
- Number of non-unicast packets (in and out)
- Number of unknown protocols (in)

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Channel	ID	Last Value (volume)	Last Value (speed)	Minimum	Maximum	Settings
Discards in	11	0 #	0 #/s	0 #/s	0 #/s	
Discards out	12	0 #	0 #/s	0 #/s	0 #/s	
Downtime	-4					
Errors in	9	0 #	0 #/s	0 #/s	0 #/s	
Errors out	10	0 #	0 #/s	0 #/s	0 #/s	
Non-Unicast in	7	23 #	1 #/s	0 #/s	81.467.512 #/s	
Non-Unicast out	8	848 #	37 #/s	9 #/s	81.467.421 #/s	
Packets	2	2.182 #	95 #/s	32 #/s	81.466.865 #/s	
Packets Received	3	1.548 #	67 #/s	20 #/s	81.467.023 #/s	
Packets Sent	4	634 #	28 #/s	9 #/s	81.467.355 #/s	
Total	-1	530 KByte	189 kbit/s	0 kbit/s	5.861.686 kbit/s	
Traffic in	0	422 KByte	150 kbit/s	21 kbit/s	648.070 kbit/s	
Traffic out	1	108 KByte	39 kbit/s	10 kbit/s	651.450 kbit/s	
Unicast in	5	700 #	30 #/s	9 #/s	81.467.115 #/s	
Unicast out	6	611 #	27 #/s	9 #/s	81.467.357 #/s	
Unknown protocols in	13	0 #	0 #/s	0 #/s	0 #/s	

Windows Network Card Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/windows_network_card.png

Remarks

- Requires 2443 Windows credentials in the parent device settings 360.
- Requires 2443 Windows 2008 or later on the probe system to work with Windows Performance Counters.
- Requires 2443 the Windows Remote Registry service to be running on the target computer.
- Can use a hybrid approach 2443 to query monitoring data: Performance counters as standard approach and WMI as fallback.
- Requires Windows 2008 / Windows 7 or later to be able to monitor 64-bit counters of the class "Network Adapter" (virtual network interfaces). On older target systems the sensor can only monitor 32-bit counters of the class "Network Interface" (the physical interface) and will show less channels.
- This sensor type supports teamed network adapters ("NIC teaming") on Windows Server 2012.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Requirement: Windows Credentials

Requires credentials for Windows systems to be defined for the device you want to use the sensor on. In the parent device's 365 **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. Otherwise, a connection via Performance Counters will not be possible. However, WMI connections may still work.

Hybrid Approach: Performance Counters and WMI

By default, this sensor type uses Windows Management Instrumentation (WMI) to request monitoring data. You can change the default behavior to a hybrid approach in the **Windows Compatibility Options** of the parent device's settings 372 on which you create this sensor: if you choose this option, the sensor will first try to query data via Windows Performance Counters and use WMI as a fallback if Performance Counters are not available. When running in fallback mode, the sensor will re-try to connect via Performance Counters after 24 hours.

Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per probe 111. Above this number, please consider using multiple **Remote Probes** 3196 for load balancing.

For a general introduction to the technology behind WMI, please see **Monitoring via WMI** 3092 section.

Requirement: Windows Version

In order for this sensor to work with Windows Performance Counters, please make sure a Windows version 2008 or later is installed on the computer running the PRTG probe: This is either on the local system (on every node, if on a cluster probe), or on the system running a remote probe 3196.

Requirement: Remote Registry Service

In order for this sensor to work with Windows Performance Counters, please make sure the Remote Registry Windows service is running on the target computer. If you fail to do so, a connection via Performance Counters will not be possible. However, WMI connections may still work.

To enable the service, please log in to the respective computer and open the services manager (for example, via services.msc). In the list, find the respective service and set its Start Type to Automatic.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the network cards you want to monitor PRTG creates one sensor for each interface you select in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SENSOR SPECIFIC

Network Interface	Select the network card(s) you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	Enter one or more **Tags**, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SPECIFIC

Selected Interface	Shows the name of the network card that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

DEBUG OPTIONS

Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section **Data Storage**. You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how to show different channels for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. You cannot use this option in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782). Manual scaling is not possible if you choose this option. ▪ **Show in and out traffic as positive and negative area chart**: Show channels for incoming and outgoing traffic as positive and negative area chart. This will visualize your traffic in a clear way. You cannot use this option in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782). Manual scaling is not possible if you choose this option. You cannot show a positive/negative chart for a channel if you choose to display its data in percent of maximum (available in the **Sensor Channels Settings** 2782).
Stack Unit	This setting is only available if you choose **Stack channels on top of each other** above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. ⓘ Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: My Windows sensors do not work when using direct Performance Counter access. What can I do?

- https://kb.paessler.com/en/topic/47263

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

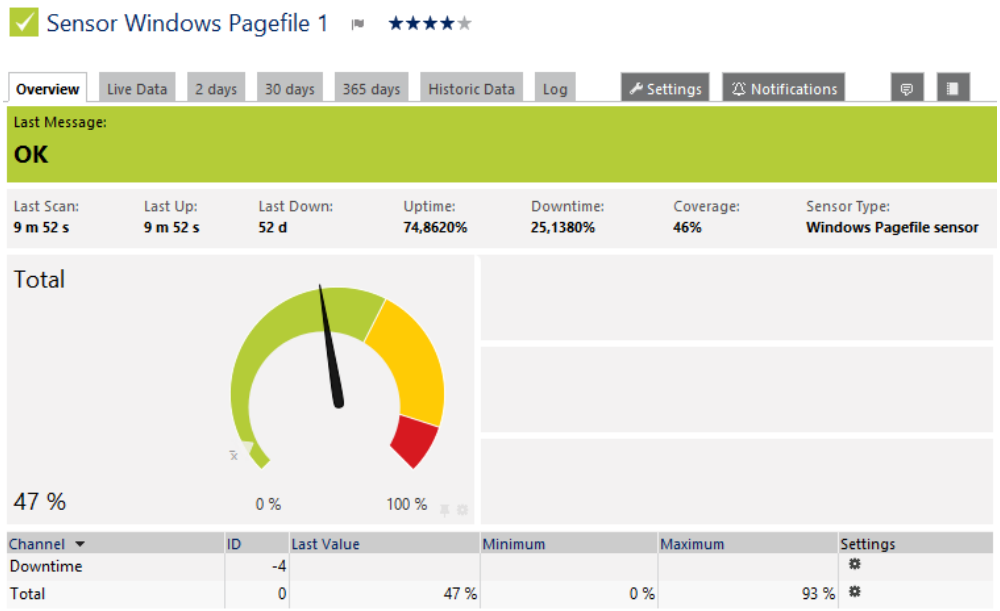
Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.207 Windows Pagefile Sensor

The Windows Pagefile sensor monitors the Windows pagefile usage via Windows Management Instrumentation (WMI) or Windows Performance Counters, as configured in the "Windows Compatibility Options" of the parent device.

- It shows the pagefile usage in percent.



Windows Pagefile Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/windows_pagefile.png

Remarks

- This sensor does not work with Windows 2000, because the respective WMI class does not exist on this operating system!
- Requires 2453 Windows credentials in the parent device settings 360.
- Requires 2453 Windows 2008 or later on the probe system.
- Requires 2453 the Windows Remote Registry service to be running on the target computer.
- Can use a hybrid approach 2453 to query monitoring data: Performance counters as standard approach and WMI as fallback.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Requirement: Windows Credentials

Requires credentials for Windows systems to be defined for the device you want to use the sensor on. In the parent device's 365 **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. Otherwise, a connection via Performance Counters will not be possible. However, WMI connections may still work.

Hybrid Approach: Performance Counters and WMI

By default, this sensor type uses Windows Management Instrumentation (WMI) to request monitoring data. You can change the default behavior to a hybrid approach in the **Windows Compatibility Options** of the parent device's settings 372 on which you create this sensor: if you choose this option, the sensor will first try to query data via Windows Performance Counters and use WMI as a fallback if Performance Counters are not available. When running in fallback mode, the sensor will re-try to connect via Performance Counters after 24 hours.

Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per probe 111. Above this number, please consider using multiple **Remote Probes** 3196 for load balancing.

For a general introduction to the technology behind WMI, please see **Monitoring via WMI** 3092 section.

Requirement: Windows Version

In order for this sensor to work with Windows Performance Counters, please make sure a Windows version 2008 or later is installed on the computer running the PRTG probe: This is either on the local system (on every node, if on a cluster probe), or on the system running a remote probe 3196.

Requirement: Remote Registry Service

In order for this sensor to work with Windows Performance Counters, please make sure the Remote Registry Windows service is running on the target computer. If you fail to do so, a connection via Performance Counters will not be possible. However, WMI connections may still work.

To enable the service, please log in to the respective computer and open the services manager (for example, via services.msc). In the list, find the respective service and set its Start Type to Automatic.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DEBUG OPTIONS

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result**: Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section Data Storage 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.
- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings 2782 settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. ⓘ Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: My Windows sensors do not work when using direct Performance Counter access. What can I do?

- https://kb.paessler.com/en/topic/47263

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.208 Windows Physical Disk I/O Sensor

The Windows Physical Disk I/O sensor monitors the input/output parameters of a hard disk on a Windows system via Windows Management Instrumentation (WMI) or Windows Performance Counters, as configured in the "Windows Compatibility Options" of the parent device.

The sensor provides the following information:

- Disk Latency
- Disk Bandwidth
- Disk queue data
- Disk IOs

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

Windows Physical Disk I/O Sensor

Click here to enlarge: https://media-s3.paessler.com/prtg-screenshots/Windows_Physical_Disk_IO.png

Remarks

- Currently, this sensor type is in beta status. The methods of operating can change at any time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.
- Requires 2463 Windows credentials in the parent device settings 360.
- Requires 2463 Windows 2008 or later on the probe system.
- Requires 2463 the Windows Remote Registry service to be running on the target computer.

- Can use a hybrid approach 2463 to query monitoring data: Performance counters as standard approach and WMI as fallback.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Requirement: Windows Credentials

Requires credentials for Windows systems to be defined for the device you want to use the sensor on. In the parent device's 365 **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. Otherwise, a connection via Performance Counters will not be possible. However, WMI connections may still work.

Hybrid Approach: Performance Counters and WMI

By default, this sensor type uses Windows Management Instrumentation (WMI) to request monitoring data. You can change the default behavior to a hybrid approach in the **Windows Compatibility Options** of the parent device's settings 372 on which you create this sensor: if you choose this option, the sensor will first try to query data via Windows Performance Counters and use WMI as a fallback if Performance Counters are not available. When running in fallback mode, the sensor will re-try to connect via Performance Counters after 24 hours.

Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per probe 111. Above this number, please consider using multiple **Remote Probes** 3196 for load balancing.

For a general introduction to the technology behind WMI, please see **Monitoring via WMI** 3092 section.

Requirement: Windows Version

In order for this sensor to work with Windows Performance Counters, please make sure a Windows version 2008 or later is installed on the computer running the PRTG probe: This is either on the local system (on every node, if on a cluster probe), or on the system running a remote probe 3196.

Requirement: Remote Registry Service

In order for this sensor to work with Windows Performance Counters, please make sure the Remote Registry Windows service is running on the target computer. If you fail to do so, a connection via Performance Counters will not be possible. However, WMI connections may still work.

To enable the service, please log in to the respective computer and open the services manager (for example, via services.msc). In the list, find the respective service and set its Start Type to Automatic.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the physical disk(s) you want to monitor. PRTG creates one sensor for each disk you select in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

WINDOWS PHYSICAL DISK SPECIFIC

Physical Disk(s)	Select the disk(s) you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.

BASIC SENSOR SETTINGS

Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

WINDOWS PHYSICAL DISK SPECIFIC

Physical Disk(s)	Shows the disk this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

DEBUG OPTIONS

Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section **Data Storage** 3226.

DEBUG OPTIONS

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

The result of this sensor is only written to disk if you use **WMI only (recommended)** as **Preferred Data Source**, as defined in the Windows Compatibility Options 372 of the parent device.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply. If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply. If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: My Windows sensors do not work when using direct Performance Counter access. What can I do?

- https://kb.paessler.com/en/topic/47263

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

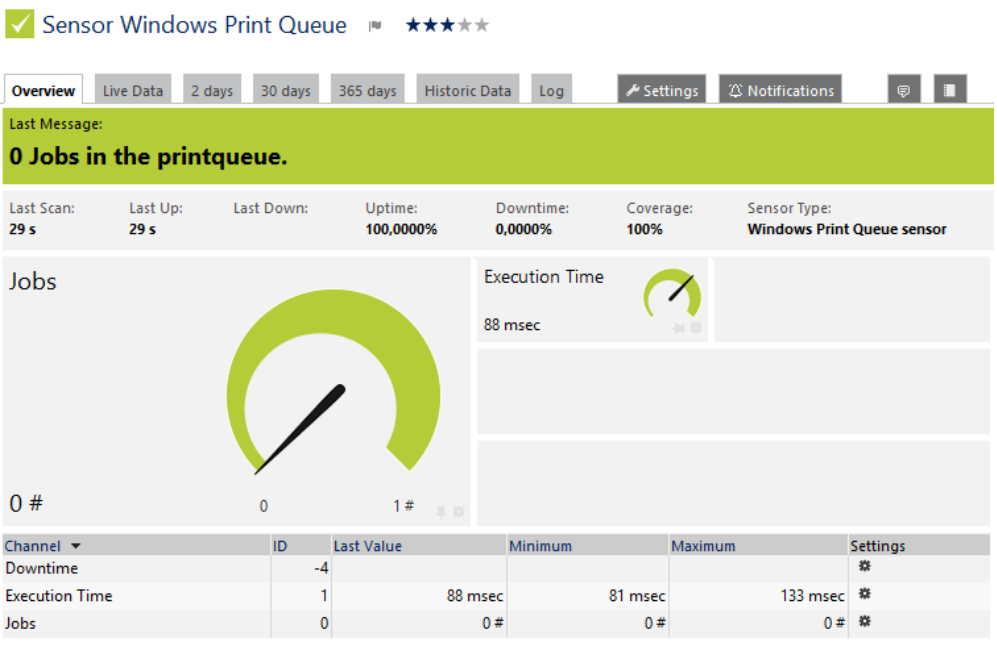
7.8.209 Windows Print Queue Sensor

The Windows Print Queue sensor reads the print queue on its parent device and returns the number of jobs in the print queue. It can monitor queues for all printers that are installed locally. For example, you can use this sensor to monitor all print queues on your Windows print server and retrieve information about all available jobs that are in the queue longer than defined.

It shows the following:

- Number of jobs in the queue
- Execution time

Additionally, this sensor can change to a defined status if there is a printer problem. See section **Sensor Settings** 2474 for available parameters.



Windows Print Queue Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/windows_print_queue.png

Remarks

- Requires 2473 .NET 4.0 or higher to be installed on the probe system. If the sensor shows the error PE087, please additionally install .NET 3.5 on the probe system.
- Requires 2473 Windows credentials in the parent device settings 360.
- Requires 2473 the Print Spooler Windows service to be running on the target device.
- We recommend Windows 2012 R2 on the probe system for best performance of this sensor.
- You can add a 'change' trigger 2921 to this sensor to get a notification when the number of jobs in the queue changes.

- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Requirement: .NET Framework

This sensor type requires the Microsoft .NET Framework to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the remote probe 3196. If the framework is missing, you cannot create this sensor.

Required .NET version (with latest updates): .NET 4.0 (Client Profile is sufficient), .NET 4.5, or .NET 4.6.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/60543

Requirement: Windows Credentials

Requires credentials for Windows systems to be defined for the device you want to use the sensor on. In the parent device's 365 **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

If you use local credentials, please make sure that the same Windows user accounts (with the same username and password) exist on both the system running the PRTG probe and the target computer. Otherwise the sensor cannot connect correctly.

Requirement: Print Spooler Service

In order for this sensor to work, the Spooler "Print Spooler" service must be started on the target computer.

To enable the service, please log in to the respective computer and open the services manager (for example, via services.msc). In the list, find the respective service and set its Start Type to Automatic.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the print queues you want to monitor. PRTG creates one sensor for each task you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SENSOR SETTINGS

Print Queue	You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items. If there are no print queues available, you see a corresponding message. If a printer name changes after you create a sensor for its queue, please add the sensor anew.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.

BASIC SENSOR SETTINGS

Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SETTINGS

Print Queue	Shows the name of the task that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Advanced Status Option	You can optionally define specific **Sensor States** 163 for several return messages of the monitored printer. Choose between: ▪ **Hide**: Do not define sensor states for specific return messages. ▪ **Show**: If you choose this option, you can define sensor states for various messages that the monitored printer reports.
Door Open Manual Feed Required Needs User Intervention Offline Out of Memory Out of Paper Paper Jammed Paper Problem Paused Printer Error	These settings are only available if you select the advanced status option above. For each reported problem of the monitored printer, you can define the status that the sensor shows. Choose between: ▪ **Ignore**: The sensor remains in the current status if this message is reported by the printer. ▪ **Warning**: The sensor shows a **Warning** status if this message is reported by the printer. ▪ **Error**: The sensor shows a **Down** status if this message is reported by the printer.

SENSOR SETTINGS

Printer Not Available

Toner Low

Toner Out

Min. Print Job Age (Sec.)

Optionally define the age of the print job in seconds. If set, jobs younger than this value are not regarded. If you leave this field blank, the sensor will not check for the print job age. Please enter an integer value or leave the field empty.

DEBUG OPTIONS

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result**: Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section Data Storage 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

SENSOR DISPLAY

Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. ⓘ To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: Which .NET version does PRTG require?

- https://kb.paessler.com/en/topic/60543

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

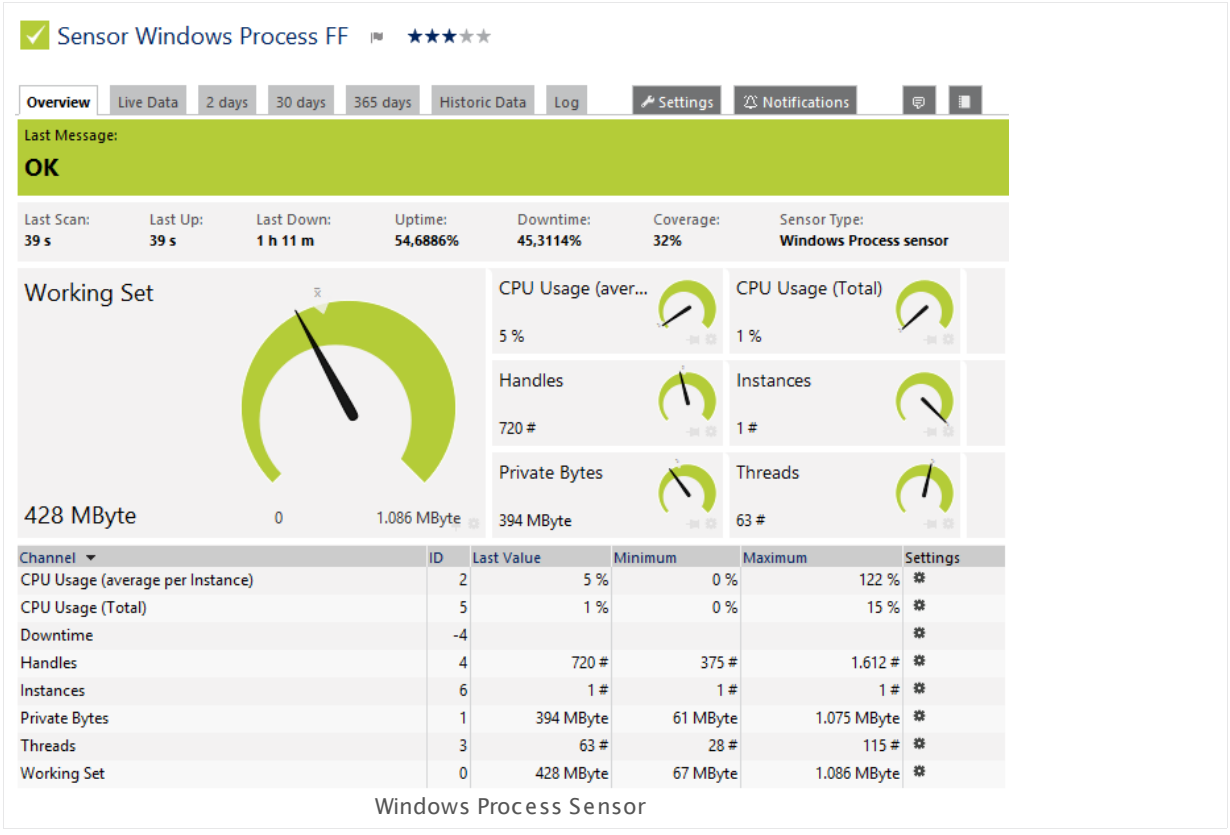
7.8.210 Windows Process Sensor

The Windows Process sensor monitors a Windows process using Windows Management Instrumentation (WMI) or Windows Performance Counters, as configured in the "Windows Compatibility Options" of the parent device.

It shows the following parameters about the process:

- Absolute working set in bytes
- Private bytes
- Number of threads
- Number of handles
- Number of instances
- Average CPU usage (if there are multiple instances running)
- Total CPU usage

For the "total CPU usage" value of a process, all CPU usage values are summed up. The total is divided by the number of all CPUs and the maximum value is 100%. This corresponds to the CPU usage of all instances of this specific process. Regarding the "per instance" value, the summed up CPU usage value is divided by the number of all instances. It shows the average CPU usage of a single instance of the process on one CPU.



Windows Process Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/windows_process.png

Remarks

- Requires 2484 Windows credentials in the parent device settings 360.
- Requires 2485 Windows 2008 or later on the probe system.
- Requires 2485 the Windows Remote Registry service to be running on the target computer.
- Does not support 64-bit processes 2484 on devices with the address "localhost", "127.0.0.1", "::1". Use the IP address in the network instead.
  This sensor cannot show values above 4 GB for 64-bit processes if you run the probe on a 64-bit Windows system. Please add this sensor to a probe running on a 32-bit Windows to monitor 64-bit processes.
- Can uss a hybrid approach 2485 to query monitoring data: Performance counters as standard approach and WMI as fallback.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Monitoring 64-bit Processes

This sensor type does not support 64-bit processes on devices with the address **localhost**, **127.0.0.1** (IPv4 address), or **::1** (IPv6 address) in PRTG. This is the case for probe devices, for example. The sensor works on all other target devices in your network. So if you want to monitor 64-bit processes on your local machine, add this device 275 to PRTG with one of the IP addresses under which it is reachable in the local network (for example, 10.0.10.20 instead of 127.0.0.1) and create the sensor on this device.

This sensor type cannot show values above 4 GB for 64-bit processes if you run the PRTG probe with this sensor on a 64-bit Windows system. The WoW64 (Windows 32-bit on Windows 64-bit) emulation layer for 32-bit applications like PRTG limits monitoring values from 64-bit systems or processes to 4 GB and caps off greater values. To avoid this issue that is caused by Windows and to correctly monitor 64-bit processes, please add this sensor to a probe that runs on a 32-bit Windows system.

Requirement: Windows Credentials

Requires credentials for Windows systems to be defined for the device you want to use the sensor on. In the parent device's 365 **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. Otherwise, a connection via Performance Counters will not be possible. However, WMI connections may still work.

Hybrid Approach: Performance Counters and WMI

By default, this sensor type uses Windows Management Instrumentation (WMI) to request monitoring data. You can change the default behavior to a hybrid approach in the **Windows Compatibility Options** of the parent device's settings 372 on which you create this sensor: if you choose this option, the sensor will first try to query data via Windows Performance Counters and use WMI as a fallback if Performance Counters are not available. When running in fallback mode, the sensor will re-try to connect via Performance Counters after 24 hours.

Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per probe 111. Above this number, please consider using multiple **Remote Probes** 3196 for load balancing.

For a general introduction to the technology behind WMI, please see **Monitoring via WMI** 3092 section.

Requirement: Windows Version

In order for this sensor to work with Windows Performance Counters, please make sure a Windows version 2008 or later is installed on the computer running the PRTG probe: This is either on the local system (on every node, if on a cluster probe), or on the system running a remote probe 3196.

Requirement: Remote Registry Service

In order for this sensor to work with Windows Performance Counters, please make sure the Remote Registry Windows service is running on the target computer. If you fail to do so, a connection via Performance Counters will not be possible. However, WMI connections may still work.

To enable the service, please log in to the respective computer and open the services manager (for example, via services.msc). In the list, find the respective service and set its Start Type to Automatic.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

WINDOWS PROCESS MONITOR

Executable	Enter the name of the process that you want to monitor. Provide the name of an executable file without the .exe extension (for example, enter firefox to monitor firefox.exe). The sensor goes into a **Down** status if the process is not active on the device.

DEBUG OPTIONS

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result**: Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section Data Storage 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.
- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings 2782 settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. ⓘ Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: My Windows sensors do not work when using direct Performance Counter access. What can I do?

- https://kb.paessler.com/en/topic/47263

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

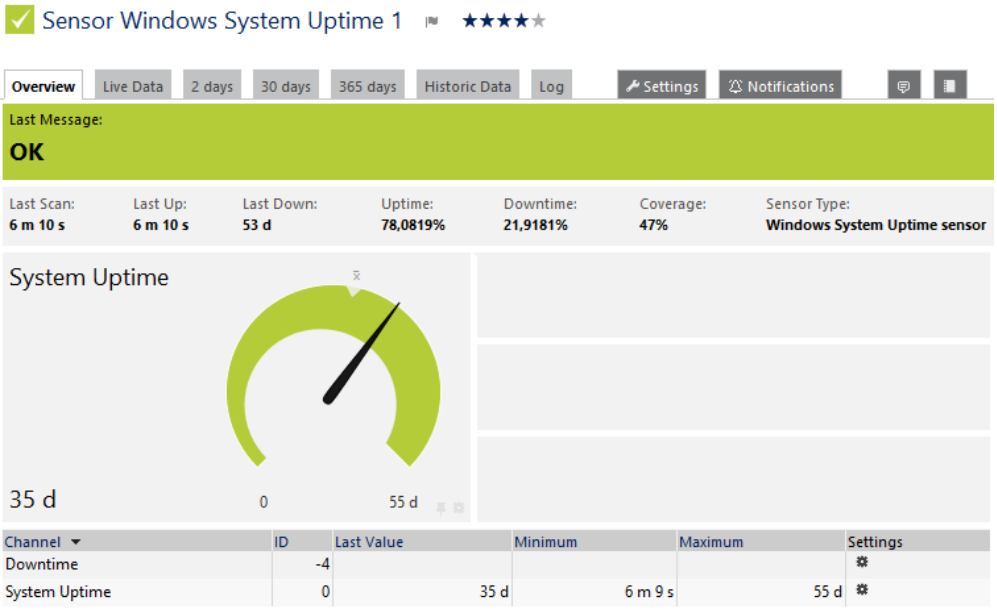
Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.211 Windows System Uptime Sensor

The Windows System Uptime sensor monitors the uptime of a Windows system using Windows Management Instrumentation (WMI) or Windows Performance Counters, as configured in the "Windows Compatibility Options" of the parent device.

- It shows the total uptime of the system in days, hours, minutes.



Windows System Uptime Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/windows_system_uptime.png

Remarks

- Requires 2493 Windows credentials in the parent device settings 360.
- Requires 2494 Windows 2008 or later on the probe system.
- Requires 2494 the Windows Remote Registry service to be running on the target computer.
- Can use a hybrid approach 2494 to query monitoring data: Performance counters as standard approach and WMI as fallback.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Requirement: Windows Credentials

Requires credentials for Windows systems to be defined for the device you want to use the sensor on. In the parent device's 365 **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. Otherwise, a connection via Performance Counters will not be possible. However, WMI connections may still work.

Hybrid Approach: Performance Counters and WMI

By default, this sensor type uses Windows Management Instrumentation (WMI) to request monitoring data. You can change the default behavior to a hybrid approach in the **Windows Compatibility Options** of the parent device's settings 372 on which you create this sensor: if you choose this option, the sensor will first try to query data via Windows Performance Counters and use WMI as a fallback if Performance Counters are not available. When running in fallback mode, the sensor will re-try to connect via Performance Counters after 24 hours.

Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per probe 111. Above this number, please consider using multiple **Remote Probes** 3196 for load balancing.

For a general introduction to the technology behind WMI, please see **Monitoring via WMI** 3092 section.

Requirement: Windows Version

In order for this sensor to work with Windows Performance Counters, please make sure a Windows version 2008 or later is installed on the computer running the PRTG probe: This is either on the local system (on every node, if on a cluster probe), or on the system running a remote probe 3196.

Requirement: Remote Registry Service

In order for this sensor to work with Windows Performance Counters, please make sure the Remote Registry Windows service is running on the target computer. If you fail to do so, a connection via Performance Counters will not be possible. However, WMI connections may still work.

To enable the service, please log in to the respective computer and open the services manager (for example, via services.msc). In the list, find the respective service and set its Start Type to Automatic.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DEBUG OPTIONS

Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result.

DEBUG OPTIONS

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section Data Storage 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. ⓘ Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: My Windows sensors do not work when using direct Performance Counter access. What can I do?

- https://kb.paessler.com/en/topic/47263

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

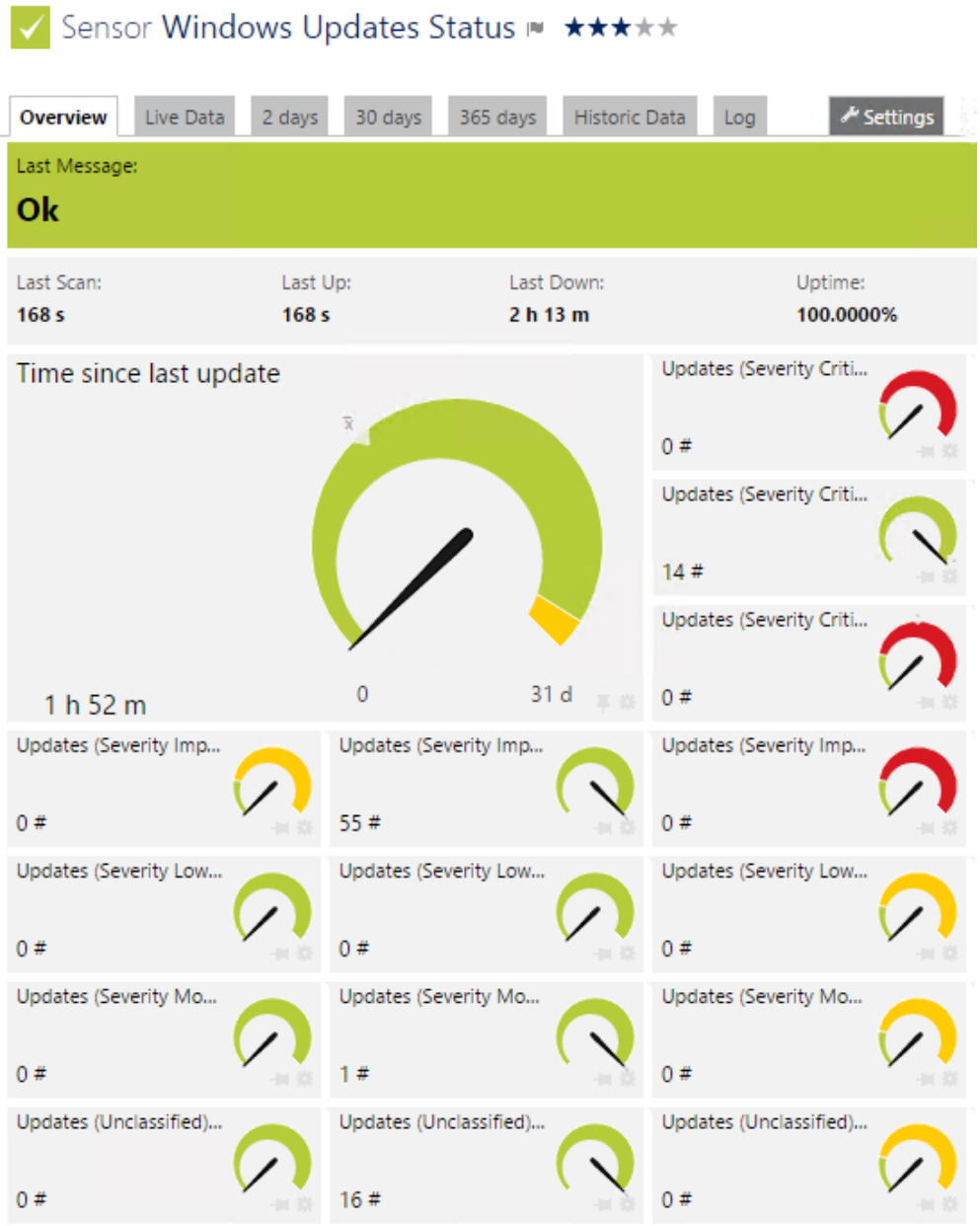
7.8.212 Windows Updates Status (Powershell) Sensor

The Windows Updates Status (Powershell) sensor monitors the status of Windows updates on a computer and counts the available and installed Windows updates—either from Microsoft or from the local Windows Server Update Services (WSUS) server.

It can show the following:

- Elapsed time since the last update
- Installed Windows updates
- Missing Windows updates
- Hidden updates
- All updates are listed with their severity.

You can find the considered updates in Server Manager (WSUS) under **Roles | Windows Server Update Services | Update Services | Computers | Reports**.



Windows Updates Status (Powershell) Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/windows_updates_status_powershell.png

Remarks

- Requires 2504 .NET 4.0 or higher to be installed on the probe system.
- Requires 2504 Remote PowerShell to be enabled on the target system and PowerShell 2.0 on the probe system.
- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.

- The minimum scanning interval for this sensor is **1 hour**.
- Knowledge Base: PowerShell Sensors: FAQ
- If the sensor cannot determine the "Time since last update" (for example, because the list of updates is empty), it will show the value **-1s** and turn into a **Warning** status 163.
- We recommend that you set the scanning interval 2507 of this sensor to at least 12 hours to limit the load on the server being monitored.
- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Requirement: .NET Framework

This sensor type requires the Microsoft .NET Framework to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the remote probe 3196. If the framework is missing, you cannot create this sensor.

Required .NET version (with latest updates): .NET 4.0 (Client Profile is sufficient), .NET 4.5, or .NET 4.6.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/60543

Requirement: Remote PowerShell

The Windows Updates Status (Powershell) sensor uses PowerShell commands. To monitor devices with this sensor, **Remote PowerShell** access has to be enabled on the target computer. Also ensure that you have installed **PowerShell 2.0** or later on your probe machine.

In larger environments, the default memory limit for the remote shell might be insufficient and you might see the error message "The WSMan provider host process did not return a proper response". In this case, increase the memory limit for Remote PowerShell.

For detailed information, please see **More** 1000 section below.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SPECIFIC

Port	Enter the number of the port to which this sensor connects. Please enter an integer value. The default port is **5985**.

DEBUG OPTIONS

Sensor Result	Define what PRTG will do with the sensor results. Choose between:

DEBUG OPTIONS

- **Discard sensor result**: Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section **Data Storage** 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.
- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

This sensor type has a fixed minimum scanning interval for performance reasons. You cannot run the sensor in shorter intervals than this minimum interval. Consequently, shorter scanning intervals as defined in **System Administration—Monitoring** 2955 are not available for this sensor.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices**	**Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: How do I enable and use remote commands in Windows PowerShell?

- https://kb.paessler.com/en/topic/44453

Knowledge Base: My Powershell sensor returns an error message. What can I do?

- https://kb.paessler.com/en/topic/59473

Knowledge Base: "No Logon Servers Available" when Using PowerShell Sensors

- https://kb.paessler.com/en/topic/59745

Knowledge Base: How can I increase memory for Remote PowerShell?

- https://kb.paessler.com/en/topic/61922

Knowledge Base: Which .NET version does PRTG require?

- https://kb.paessler.com/en/topic/60543

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

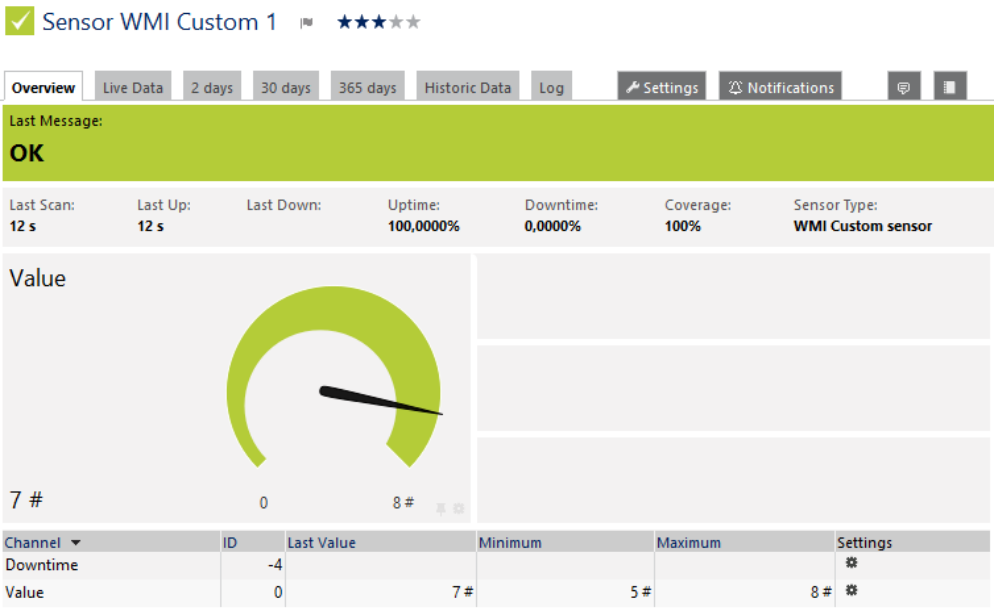
7.8.213 WMI Custom Sensor

The WMI Custom Sensor performs a custom query via Windows Management Instrumentation (WMI).

- It shows the retrieved value.

Your Windows Management Instrumentation Query Language (WQL) query code must be stored in a file on the system of the probe the sensor is created on. If used on a remote probe, the file must be stored on the system running the remote probe. In a cluster setup, please copy the file to every cluster node.

Save the file with the query into the **\Custom Sensors\WMI WQL scripts** subfolder of your PRTG installation. See the section **Data Storage** [3226] for more information about how to find this path.



WMI Custom Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/wmi_custom.png

Remarks

- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per probe [111]. Above this number, please consider using multiple **Remote Probes** [3196] for load balancing.
- For a general introduction to the technology behind WMI, please see manual section **Monitoring via WMI** [3092].

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

CUSTOM QUERY SPECIFIC

Channel Name	Enter a name for the channel in which PRTG shows the received data. This name will be displayed in graphs and tables. Please enter a string. You can change the name later in the sensor's channel settings 2782.
WQL File	Select a file from the list that this sensor will use. The sensor executes it with every scanning interval. The menu contains WQL scripts from the **\Custom Sensors\WMI WQL scripts** subfolder of your PRTG installation. Please store your script there. If used on a remote probe, you must store the file on the system running the remote probe. If used on a cluster probe, you must store the file on all servers running a cluster node. For more information on how to find this path, please see **Data Storage** 3226 section. Your query must return an integer or float value. Strings are not supported!

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

CUSTOM QUERY SPECIFIC

Namespace	Enter the namespace for the query.
WQL File	Shows the WQL file that this sensor executes with every scanning interval. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Placeholder <#PH1>	In your WQL script, you can use up to three placeholders that you can assign a value to in this field. Please enter a string for variable **<#PH1>** or leave the field empty.
Placeholder <#PH2>	In your WQL script, you can use up to three placeholders that you can assign a value to in this field. Please enter a string for variable **<#PH2>** or leave the field empty.
Placeholder <#PH3>	In your WQL script, you can use up to three placeholders that you can assign a value to in this field. Please enter a string for variable **<#PH3>** or leave the field empty.

CUSTOM QUERY SPECIFIC

If Value Changes	Define what this sensor will do when the sensor value changes. You can choose between: ▪ **Ignore changes (default)**: The sensor takes no action on change. ▪ **Trigger 'change' notification**: The sensor sends an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification 2791 whenever the sensor value changes.
Unit String	Enter a unit for the data that the sensor receives from your script. This is for displaying purposes only. The unit will be displayed in graphs and tables. Please enter a string.
Multiplication	Define a multiplier for the received values. By default, this is set to **1** in order to not change received values. Please enter an integer value.
Division	Define a divisor for the received values. By default, this is set to **1** in order to not change received values. Please enter an integer value.

DEBUG OPTIONS

Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section **Data Storage** 3226. You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

▪ **Additional Sensor Types (Custom Sensors)** 2778

Knowledge Base: How do I properly configure a WMI Custom Sensor?

▪ https://kb.paessler.com/en/topic/163

Knowledge Base: How do I create a WMI Custom Sensor?

▪ https://kb.paessler.com/en/topic/2743

Knowledge Base: Which WQL queries are used by PRTG's WMI sensors?

▪ https://kb.paessler.com/en/topic/8783

Knowledge Base: How can I monitor a Windows service on Windows 2000?

▪ https://kb.paessler.com/en/topic/36483

My WMI sensors don't work. What can I do?

▪ https://kb.paessler.com/en/topic/1043

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

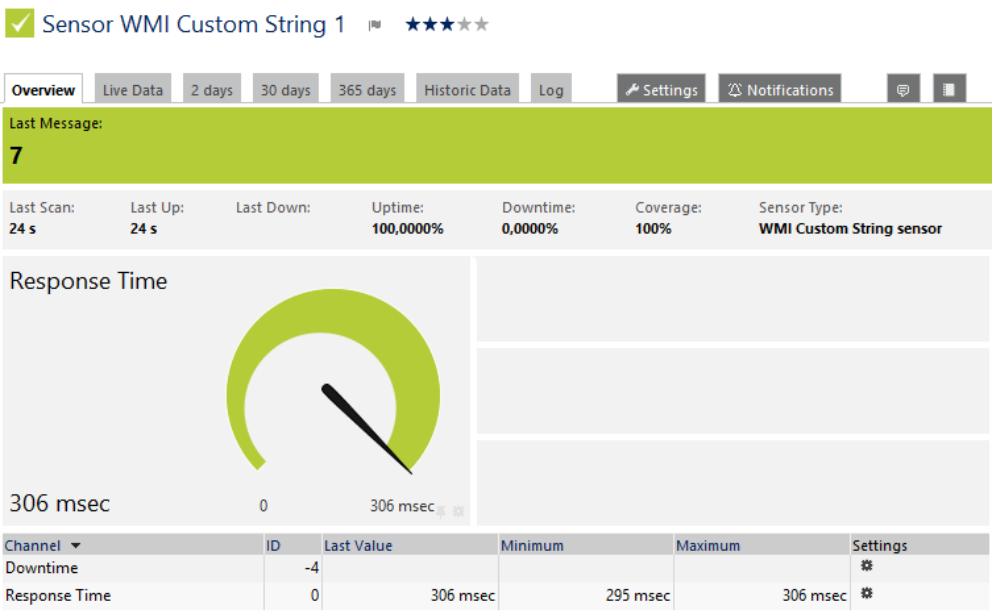
For more general information about settings, please see the **Object Settings** 188 section.

7.8.214 WMI Custom String Sensor

The WMI Custom String sensor performs a custom string query via Windows Management Instrumentation (WMI).

- It shows the retrieved string value in the sensor message.
- It also shows the response time.

Your Windows Management Instrumentation Query Language (WQL) query code must be stored in a file on the system of the probe the sensor is created on. If used on a remote probe, the file must be stored on the system running the remote probe. In a cluster setup, please copy the file to every cluster node.



WMI Custom String Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/wmi_custom_string.png

Remarks

- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per probe 111. Above this number, please consider using multiple **Remote Probes** 3196 for load balancing.
- For a general introduction to the technology behind WMI, please see manual section **Monitoring via WMI** 3092.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

CUSTOM QUERY SPECIFIC

Channel Name	Enter a name for the channel in which the received data will be presented. The name will be displayed in graphs and tables. Please enter a string. You can change the name later in the sensor's channel settings 2782.
WQL File	Select a file that will be used for this sensor from the dropdown menu. It will be executed with every scanning interval. The menu contains WQL scripts from the **\Custom Sensors\WMI WQL scripts** subfolder of your PRTG installation. Please store your script there. If used on a remote probe, the file must be stored on the system running the remote probe. If used on a cluster probe, you must store the file on all servers running a cluster node! For more information on how to find this path, please see **Data Storage** 3226 section.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.

BASIC SENSOR SETTINGS

Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

CUSTOM QUERY SPECIFIC

Namespace	Enter the namespace for the query.
WQL File	Shows the name of the file that this sensor uses. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Placeholder <#PH1>	In your WQL script, you can use up to three placeholders that you can assign a value to in this field. Please enter a string for variable **<#PH1>** or leave the field empty.
Placeholder <#PH2>	In your WQL script, you can use up to three placeholders that you can assign a value to in this field. Please enter a string for variable **<#PH2>** or leave the field empty.
Placeholder <#PH3>	In your WQL script, you can use up to three placeholders that you can assign a value to in this field. Please enter a string for variable **<#PH3>** or leave the field empty.
Unit String	Enter a unit for the data that will be received by your script. This is for displaying purposes only. The unit will be displayed in graphs and tables. Please enter a string.

CUSTOM QUERY SPECIFIC

If Value Changes	Define what this sensor will do when the sensor value changes. You can choose between: ▪ **Ignore changes (default)**: The sensor takes no action on change. ▪ **Trigger 'change' notification**: The sensor sends an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification 2791 whenever the sensor value changes.
Response Must Include	Define which string must be part of the data that is received form the WMI object. You can either enter plain text or a **Regular Expression** 3193. If the data does not include the search pattern, the sensor will be set to an error state. Please enter a string or leave the field empty.
Response Must Not Include	Define which string must not be part of the data that is received form the WMI object. You can either enter plain text or a **Regular Expression** 3193. If the data does include the search pattern, the sensor will be set to an error state. Please enter a string or leave the field empty.
For Keyword Search Use	Define the format of the search expression you entered above. ▪ **Plain Text**: Search for the string as plain text. The characters * and ? work here as placeholders, whereas * stands for no or any number of characters and ? stands for exactly one character (as known from Windows search). This behavior cannot be disabled, so the literal search for these characters is not possible with plain text search. ▪ **Regular Expression**: Treat the search pattern as a **Regular Expression** 3193.
Maximum Length of String	Define the maximum allowed length of the string that will be received from the WMI object. If it is longer than this value, the sensor will be set to an error status. Please enter an integer value or leave the field empty.
Extract Number Using Regular Expression	Define if you want to filter out a numeric value from the string received from the WMI object. You can convert this into a float value, in order to use it with channel limits (see **Sensor Channels Settings** 2782). ▪ **No extraction**: Do not extract a float value. Use the result as a string value.

CUSTOM QUERY SPECIFIC

	▪ **Extract a numeric value using a regular expression**: Use a regular expression to identify a numeric value in the string and convert it to a float value. Define below. See also the example 2531 below.
Regular Expression	This setting is only visible if number extraction is enabled above. Enter a **Regular Expression** 3193 to identify the numeric value you want to extract from the string returned by the WMI object. You can use capturing groups here. Make sure the expression returns numbers only (including decimal and thousands separators). The result will be further refined by the settings below.
Index of Capturing Group	This setting is only visible if number extraction is enabled above. If your regular expression uses capturing groups, specify which one will be used to capture the number. Please enter an integer value or leave the field empty.
Decimal Separator	This setting is only visible if number extraction is enabled above. Define which character to use as decimal separator for the number extracted above. Please enter a string or leave the field empty.
Thousands Separator	This setting is only visible if number extraction is enabled above. Define which character to use as thousands separator for the number extracted above. Please enter a string or leave the field empty.
Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section **Data Storage** 3226. You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

Example: Number Extraction with Regular Expression

If you want to extract a number in the response string using a regular expression, please note that the index for captures in this sensor is based on 1 (**not on 0**). Furthermore, capturing groups are not created automatically. The example below will illustrate this issue.

Consider the following string as returned by a request for CPU usage:

```
5 Sec (3.49%), 1 Min (3.555%), 5 Min (3.90%)
```

Assuming you would like to filter for the number 3.555, i.e., the percentage in the second parentheses. Then enter the following regex in the **Regular Expression** field:

```
(\d+\.\d+).*?(\d+\.\d+).*?(\d+\.\d+)
```

As **Index of Capturing Group** enter 3. This will extract the desired number 3.555.

The index has to be 3 in this case because the capturing groups here are the following:

- Group 1 contains "3.49%), 1 Min (3.555), 5 Min (3.90"

- Group 2 contains "3.49"
- Group 3 contains "3.555"
- Group 4 contains "3.90"

Please keep in mind this note about index and capturing groups when using number extraction.

It is not possible to match an empty string with the PRTG regex sensor search.

More

My WMI sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/1043

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

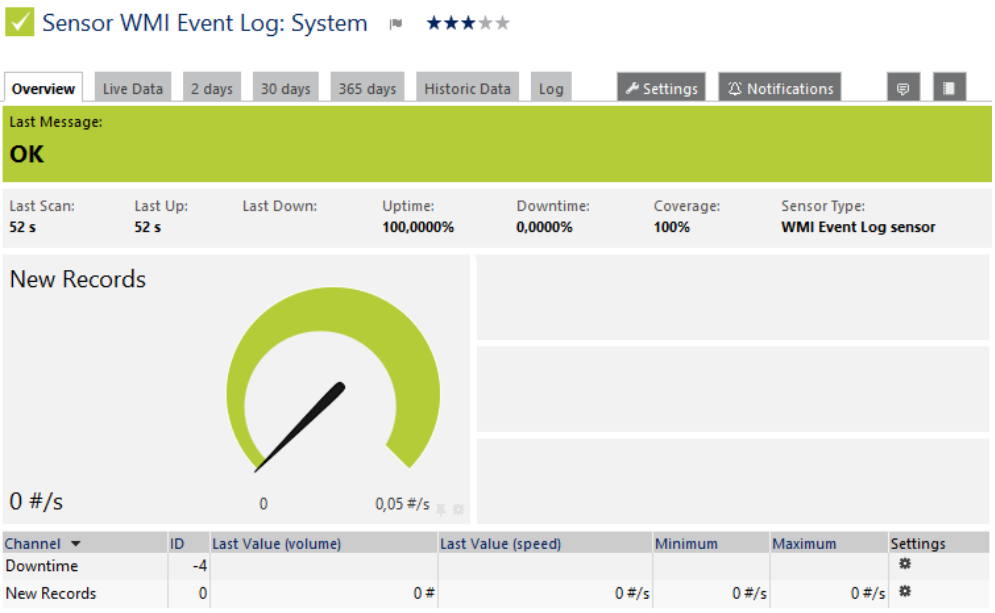
For more general information about settings, please see the **Object Settings** 188 section.

7.8.215 WMI Event Log Sensor

The WMI Event Log sensor monitors a specific Windows logfile using Windows Management Instrumentation (WMI).

- It shows the number of new records per second.

You can set the sensor to a desired status individually according to a new event log entry. For details and how to find out the correct filter, see section **More** 2542.



WMI Event Log Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/wmi_event_log.png

Remarks

- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per probe 111. Above this number, please consider using multiple **Remote Probes** 3196 for load balancing.
- For a general introduction to the technology behind WMI, please see manual section **Monitoring via WMI** 3092.
- Knowledge Base: My Event Log sensor ignores changes in the event log. What can I do?
- Knowledge Base: How can I configure sensors using speed limits to keep the status for more than one interval?
- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the log files you want to monitor. PRTG creates one sensor for each log you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

WMI EVENT LOG MONITOR

Log File	The Windows event log provides several different logfiles. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.

BASIC SENSOR SETTINGS

Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

WMI EVENT LOG MONITOR

Log File	Shows the Windows logfile that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section **Data Storage** 3226. You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

FILTER EVENT LOG ENTRIES

Event Type	Specify the type of event that this sensor processes. Other event types cannot be processed. Choose between the following event types: ▪ **Any** ▪ **Error** ▪ **Warning** ▪ **Information** ▪ **Security Audit Success** ▪ **Security Audit Failure**
Filter by Source	Filter all received events for a certain event source. If you enable this option, this sensor only processes messages that match the defined value. Choose between: • **Off**: Do not filter by event source. • **On**: Enable filtering by event source.
Match String (Event Source)	This field is only visible if you enable source filtering above. Enter the source that the events come from. Only events from a source matching this string are regarded, other events are ignored. Please enter a string.
Filter by ID	Filter all received events for a certain event ID. If you enable this option, this sensor processes only messages that match the defined value(s). Choose between: • **Off**: Do not filter by event ID. • **On**: Enable filtering by event ID.
Match Values (Event ID)	This field is only visible if you enable ID filtering above. Enter an event ID that the events must have. Only events with an ID that matches this value are regarded. The Event Log (Windows API) Sensor 677 supports more than one event ID. Using this sensor type, you can enter a comma separated list of event IDs to filter for more than one ID. The WMI Event Log Sensor 2533 supports filtering for only one ID.
Filter by Category	Filter all received events for a certain event category. If you enable this option, this sensor only processes messages that match the defined value. Choose between: • **Off**: Do not filter by event category.

FILTER EVENT LOG ENTRIES

	• **On**: Enable filtering by event category.
Match String (Event Category)	This field is only visible if you enable category filtering above. Enter a category that the events must have. Only events with a category that matches this string are regarded. Please enter a string.
Filter by User	Filter all received events for a certain event user. If you enable this option, this sensor only processes messages that match the defined value. Choose between: • **Off**: Do not filter by event user. • **On**: Enable filtering by event user.
Match String (Event User)	This field is only visible if you enable user filtering above. Enter a username that the events must to be assigned to. Only events with a username that matches this string are regarded. Please enter a string.
Filter by Computer	Filter all received events for a certain event computer. If you enable this option, this sensor only processes messages that match the defined value. Choose between: • **Off**: Do not filter by event computer. • **On**: Enable filtering by event computer.
Match String (Event Computer)	This field is only visible if you enable computer filtering above. Enter a computer name that the events must be assigned to. Only events with a computer name that matches this string are regarded. Please enter a string.
Filter by Message	Filter all received events for a certain event message. If you enable this option, this sensor only processes messages that match the defined value. Choose between: • **Off**: Do not filter by event message. • **On**: Enable filtering by event message.
Match String (Event Message)	This field is only visible if you enable message filtering above. Enter a message that the event must contain. Only events with a message matching this string are regarded. Please enter a string.

For the **WMI Event Log Sensor**, you can use the percent sign (%) as placeholder for any or no character (as known from the asterisk sign (*) in Windows search) in combination with a substring. For example, you can enter **%RAS%** for any event source containing the string **RAS**.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: My Event Log sensor ignores changes in the event log. What can I do?

- https://kb.paessler.com/en/topic/59803

Knowledge Base: How can I configure sensors using speed limits to keep the status for more than one interval?

- https://kb.paessler.com/en/topic/73212

My WMI sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/1043

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

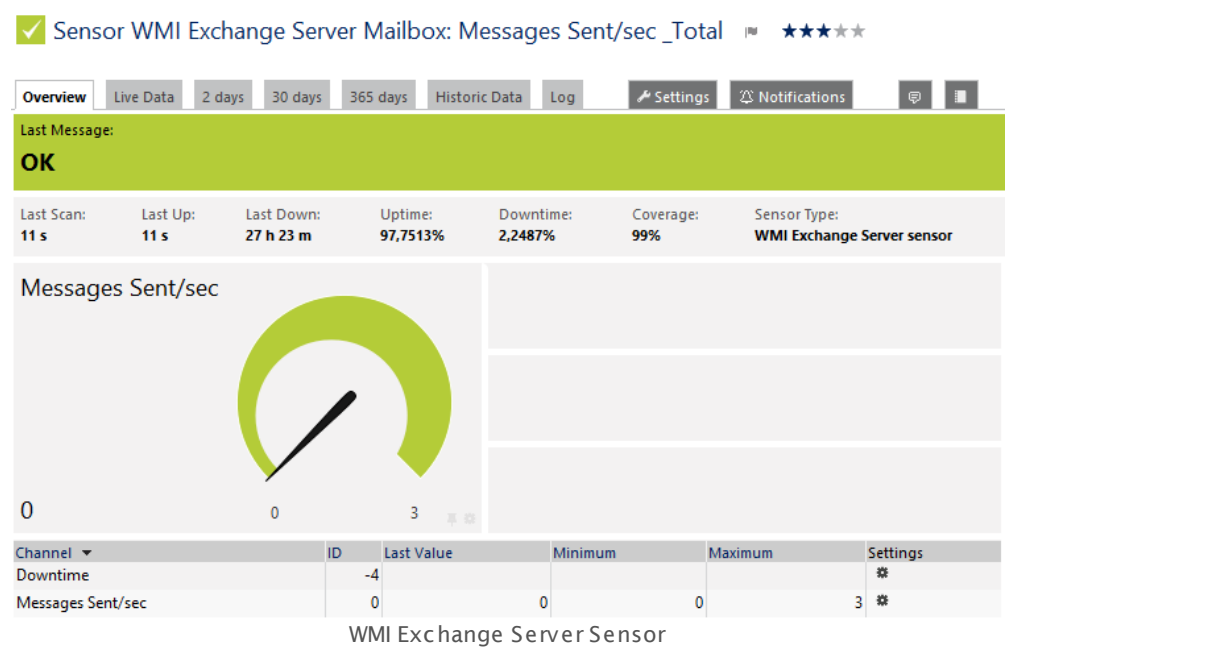
7.8.216 WMI Exchange Server Sensor

The WMI Exchange Server sensor monitors a Microsoft Exchange Server 2003, 2007, 2010, or 2013 using Windows Management Instrumentation (WMI).

It can show the following:

- Queue size
- Average delivery time
- Logon operations per second
- Sent, delivered, and submitted messages per second
- Messages queued for submission
- Remote Procedure Call (RPC) packets operations per second
- RPC latency, requests, and slow packets
- RPC sent, slow, outstanding, and failed requests (store interface)
- Read and write bytes RPC clients per second
- Number of active and anonymous users
- Database page faults per second
- Log record stalls per second
- Log threads waiting
- Database cache size in bytes and miss in percent
- Current unique users (OWA)
- Average response time (OWA)

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



WMI Exchange Server Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/wmi_exchange_server.png

Remarks

- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per probe 111. Above this number, please consider using multiple **Remote Probes** 3196 for load balancing.
- For a general introduction to the technology behind WMI, please see manual section **Monitoring via WMI** 3092.

Existing former "WMI Exchange Server 2003/2007 Sensors" from previous PRTG versions will continue to monitor your Exchange server in PRTG 9, but newly added Exchange server sensors will be of the "WMI Exchange Server Sensor" type, which is able to monitor Exchange servers regardless of their version.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the performance counters of the Exchange server you want to monitor. PRTG creates one sensor for each performance counter you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

EXCHANGE SERVER DATA READINGS ACCESSIBLE USING WMI

Performance Counter

You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

The available options depend on your Exchange server configuration. PRTG shows all possible performance counters with name and instance description (if available).

You might be able to select aspects regarding:

- **SMTP Server**: Queue Lengths
- **MSExchangeIS Mailbox**: Queue Sizes, Delivery Times, Operations, Messages
- **MSExchangeIS Public**: Queue Sizes, Delivery Times, Operations, Messages
- **MSExchangeIS**: Packets, Operations, Clients, Latency, Requests, Users
- **MS Exchange RPC Client Access**: Active User Count, User Count, Connection Count
- **MS Exchange OWA**: Current Unique Users, Average Response Time

Depending on your Exchange server version, not all counters might be available.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

READINGS ACCESSIBLE USING WMI

Display Name Instance	These fields show the parameters that are used to query data for this sensor from the target device.Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
WMI Class	
Counter	
Time Stamp	
Time Frequency	
Counter Type	
Sensor Result	Define what PRTG will do with the sensor results. Choose between:

READINGS ACCESSIBLE USING WMI

- **Discard sensor result**: Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section **Data Storage** 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.
- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. ⓘ Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

My WMI sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/1043

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.217 WMI Exchange Transport Queue Sensor

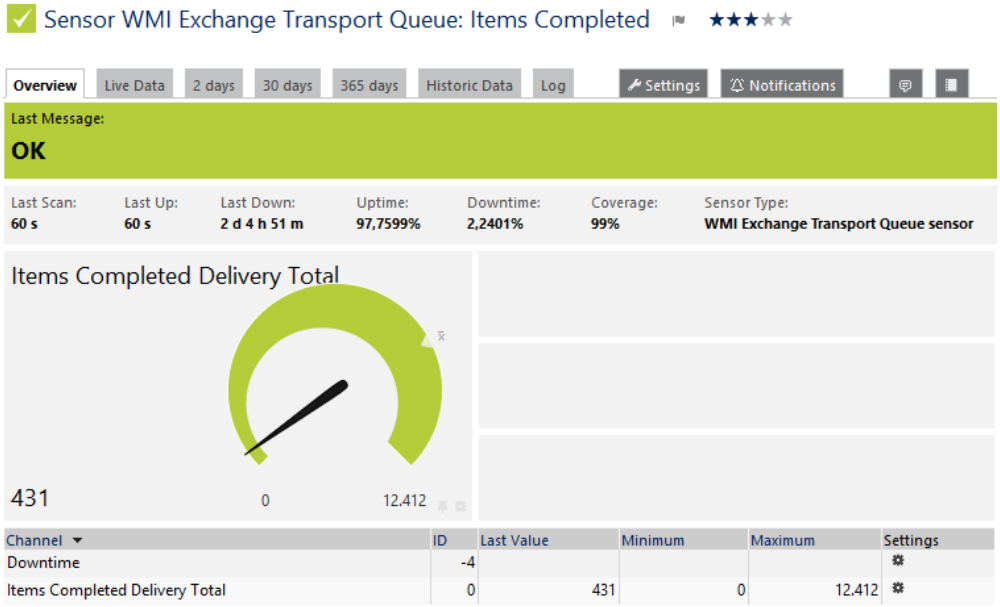
The WMI Exchange Server sensor monitors the length of transport queues of a Microsoft Exchange Server 2003, 2007, 2010, or 2013 using Windows Management Instrumentation (WMI). It shows the same information as shown in Windows System Monitor ('perfmon'). See section **More** 2563 below for an explanation of the transport queue types.

This sensor can show the following:

- Active Mailbox Delivery Queue Length
- Active Non-Smtp Delivery Queue Length
- Active Remote Delivery Queue Length
- Aggregate Delivery Queue Length (All Queues)
- Aggregate Shadow Queue Length
- Categorizer Job Availability
- Items Completed Delivery Per Second
- Items Completed Delivery Total
- Items Deleted By Admin Total
- Items Queued For Delivery Expired Total
- Items Queued for Delivery Per Second
- Items Queued For Delivery Total
- Items Resubmitted Total
- Largest Delivery Queue Length
- Messages Completed Delivery Per Second
- Messages Completed Delivery Total
- Messages Completing Categorization
- Messages Deferred Due To Local Loop
- Messages Deferred during Categorization
- Messages Queued For Delivery
- Messages Queued for Delivery Per Second
- Messages Queued For Delivery Total
- Messages Submitted Per Second
- Messages Submitted Total
- Poison Queue Length
- Retry Mailbox Delivery Queue Length
- Retry Non-Smtp Delivery Queue Length
- Retry Remote Delivery Queue Length

- Shadow Queue Auto Discards Total
- Submission Queue Items Expired Total
- Submission Queue Length
- Unreachable Queue Length

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



WMI Exchange Transport Queue Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/wmi_exchange_transport_queue.png

Remarks

- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per probe 111. Above this number, please consider using multiple **Remote Probes** 3196 for load balancing.
- For a general introduction to the technology behind WMI, please see manual section **Monitoring via WMI** 3092.
- Knowledge Base: Types of Transport Queues in Microsoft Exchange

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the transport queues you want to monitor. PRTG creates on sensor for each queue you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

WMI EXCHANGE TRANSPORT QUEUE SPECIFIC

MSExchangeTransport Queues	You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items. The available options depend on your Exchange server configuration. PRTG shows all possible queues with names and instance descriptions (if available). For performance reasons, we recommend to only select necessary items!

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

READINGS ACCESSIBLE USING WMI

Display Name Instance	These fields show the parameters that are used to query data for this sensor from the target device.Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
WMI Class	
Counter	
Time Stamp	
Time Frequency	
Counter Type	
Sensor Result	Define what PRTG will do with the sensor results. Choose between:

READINGS ACCESSIBLE USING WMI

- **Discard sensor result**: Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section **Data Storage** 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.
- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. ⓘ Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: Types of Transport Queues in Microsoft Exchange

- https://kb.paessler.com/en/topic/55413

My WMI sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/1043

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

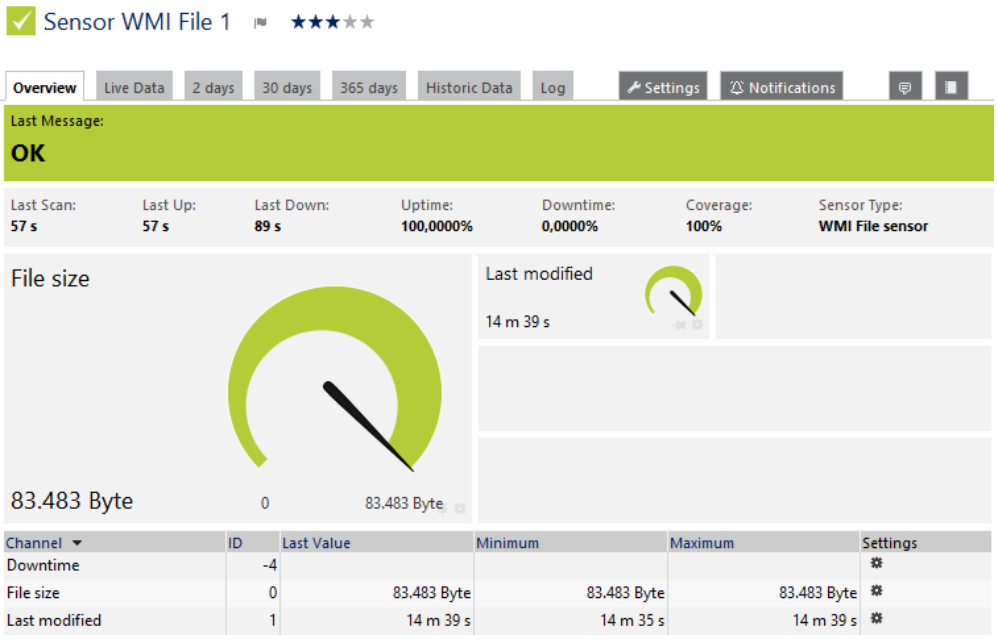
For more general information about settings, please see the **Object Settings** 188 section.

7.8.218 WMI File Sensor

The WMI File sensor monitors a file using Windows Management Instrumentation (WMI).

It shows the following:

- File size
- Elapsed time since its last modification



WMI File Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/wmi_file.png

Remarks

- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per probe 111. Above this number, please consider using multiple **Remote Probes** 3196 for load balancing.
- For a general introduction to the technology behind WMI, please see manual section **Monitoring via WMI** 3092.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

WMI FILE MONITOR

File Name	Enter the name of the file that this sensor checks. Enter the full local path. The file must exist on the computer your local or remote probe is running on. UNC paths are not allowed here. For example, when you create this sensor on a device under the local probe, the file has to be accessible on the local system.
If Timestamp Changes	Define what to do when the timestamp of the file changes. You can choose between: ▪ **Ignore changes (default)**: The sensor takes no action on change. ▪ **Trigger 'change' notification**: The sensor sends an internal message indicating that the timestamp has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification 2791 whenever the timestamp changes.

DEBUG OPTIONS

Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section **Data Storage** 3226. You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

My WMI sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/1043

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

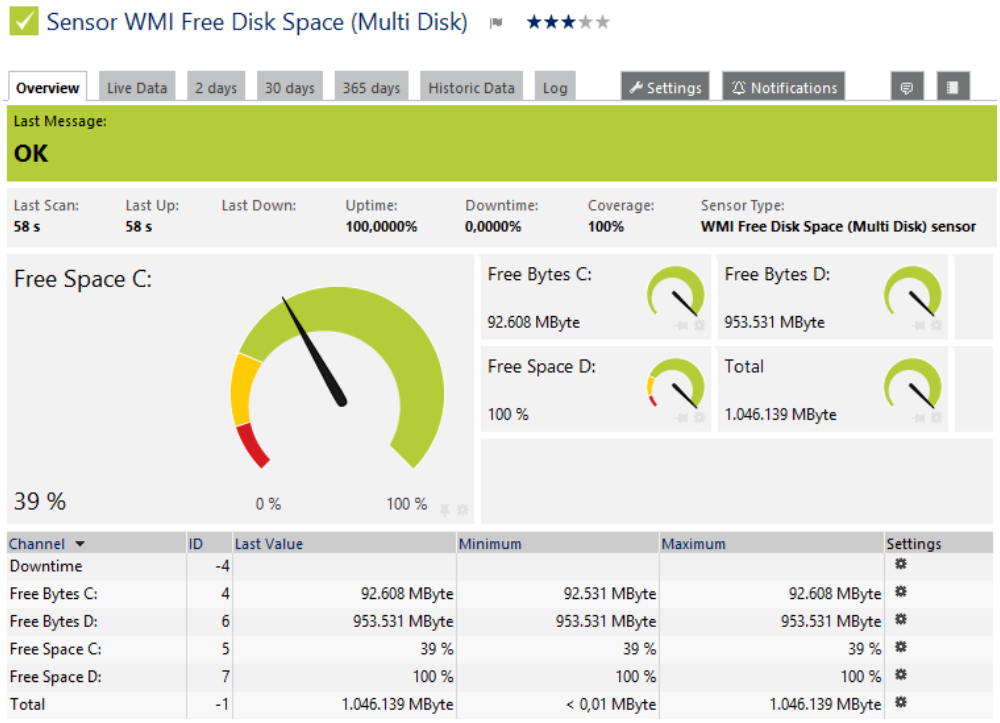
7.8.219 WMI Free Disk Space (Multi Disk) Sensor

The WMI Free Disk Space (Multi Disk) sensor monitors the free disk space of one or multiple drive(s) using Windows Management Instrumentation (WMI).

It shows the following:

- Free disk space in percent and bytes for each disk
- Disk space of a system in total

This sensor monitors logical partitions of a hard or fixed disk drive. PRTG identifies logical disks by their drive letter, such as C.



WMI Free Disk Space (Multi Disk) Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/wmi_free_disk_space_multi_disk.png

Remarks

- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per probe 111. Above this number, please consider using multiple **Remote Probes** 3196 for load balancing.
- For a general introduction to the technology behind WMI, please see manual section **Monitoring via WMI** 3092.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

WMI DISK FREE CONFIGURATION

Drive	Select the drive(s) you want to monitor from the dropdown menu. We recommend that you use the default value. You can choose **All** to monitor all available drives, or you can choose one specific drive letter to monitor a single drive only. The data in the dropdown menu may also contain drive letters that do not exist on your device. The drive setting cannot be changed once the sensor is created.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	Enter one or more **Tags**, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

WMI DISK FREE CONFIGURATION

Drive	Shows the drive(s) that this sensor monitors. This is either **All** or a specific drive letter. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SET LIMITS CHECKED AGAINST ALL DISKS

In this section you can set limits that are valid for all channels and all drives. By entering limits, you can define when the sensor will enter a **Warning** or **Down** status, depending on the data provided by all drives that this sensor monitors. If you want to define limits for separate channels individually, please use the limit settings in the sensor **Channel** settings.

All limits that you define here are valid in addition to the limits defined in the particular **Channels** settings! The limits are valid simultaneously, so the first limit that is breached applies.

Percentage Limit Check	Enable or disable a limit check for the free space in percentage channels of all drives. By default, percentage limits are enabled with lower warning and lower error limit. Choose between:

SET LIMITS CHECKED AGAINST ALL DISKS

- **Only use the limits in the settings of the percentage channels**: Do not define sensor limits which are valid for all percentage channels. The sensor only uses limits which you define in the settings of the particular "free space in percent" channels to determine the status.
- **Use the limits of both the sensor and the channel settings**: Define limits for the sensor which are valid for all drives (percentage channels). Additional fields appear below. The sensor enters a **Warning** or **Down** status when free space limits are undercut or overrun.

Upper Error Limit

This field is only visible if you enable percentage limit check above. Specify an upper limit in percent for a **Down** status. If the free disk space of one of your drives overruns this percent value, the sensor switches to **Down**. Please enter an integer value or leave the field empty.

The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the **Sensor Channels Settings** 2782. The limits set here and in the channel settings are valid simultaneously!

Upper Warning Limit

This field is only visible if you enable percentage limit check above. Specify an upper limit in percent for a **Warning** status. If the free disk space of one of your drives overruns this percent value, the sensor switches to **Warning**. Please enter an integer value or leave the field empty.

The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the **Sensor Channels Settings** 2782. The limits set here and in the channel settings are valid simultaneously!

Lower Warning Limit

This field is only visible if you enable percentage limit check above. Specify a lower limit in percent for a **Warning** status. If the free disk space of one of your drives undercuts this percent value, the sensor switches to warning. Please enter an integer value or leave the field empty.

The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the **Sensor Channels Settings** 2782. The limits set here and in the channel settings are valid simultaneously!

Lower Error Limit

This field is only visible if you enable percentage limit check above. Specify a lower limit in percent for a **Down** status. If the free disk space of one of your drives undercuts this percent value, the sensor switches to **Down**. Please enter an integer value or leave the field empty.

SET LIMITS CHECKED AGAINST ALL DISKS

The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the Sensor Channels Settings 2782. The limits set here and in the channel settings are valid simultaneously!

Size Limit Check

Enable or disable a limit check for the free bytes channels of all drives. By default, byte size limits are not enabled for drives. Choose between:

- **Only use the limits in the settings of the byte size channels**: Do not define sensor limits which are valid for all byte size channels. The sensor only uses limits which you define in the settings of the particular free space in bytes channels to determine the status.
- **Use the limits of both the sensor and the channel settings**: Define limits for the sensor which are valid for all drives (byte size channels). Additional fields appear below. The sensor enters a **Warning** or **Down** status when free space limits are undercut or overrun.

Upper Error Limit

This field is only visible if you enable byte limit check above. Specify an upper limit. Use the same unit as shown by the free bytes channels of this sensor (by default this is MByte). If the free disk space of one of your drives overruns this bytes value, the sensor switches to **Down**. Please enter an integer value or leave the field empty.

The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the Sensor Channels Settings 2782. The limits set here and in the channel settings are valid simultaneously!

Upper Warning Limit

This field is only visible if you enable byte limit check above. Specify an upper limit. Use the same unit as shown by the free bytes channels of this sensor (by default this is MByte). If the free disk space of one of your drives overruns this bytes value, the sensor switches to **Warning**. Please enter an integer value or leave the field empty.

The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the Sensor Channels Settings 2782. The limits set here and in the channel settings are valid simultaneously!

SET LIMITS CHECKED AGAINST ALL DISKS

Lower Warning Limit	This field is only visible if you enable byte limit check above. Specify a lower limit. Use the same unit as shown by the free bytes channels of this sensor (by default this is MByte). If the free disk space of one of your drives undercuts this bytes value, the sensor switches to **Warning**. Please enter an integer value or leave the field empty. The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the **Sensor Channels Settings** 2782. The limits set here and in the channel settings are valid simultaneously!
Lower Error Limit	This field is only visible if you enable byte limit check above. Specify a lower limit. Use the same unit as shown by the free bytes channels of this sensor (by default this is MByte). If the free disk space of one of your drives undercuts this bytes value, the sensor switches to **Down**. Please enter an integer value or leave the field empty. The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the **Sensor Channels Settings** 2782. The limits set here and in the channel settings are valid simultaneously!
Alarm on Missing/ Removed Disk	If a monitored disk is removed or not found, values are set to zero. Select the alarming approach in this case. Choose between: ▪ **Deactivate alarm (default)**: Select this option if you do not want an alarm for a removed disk. ▪ **Activate alarm**: Select this option if you want to be alerted if a monitored disk is removed.

DEBUG OPTIONS

Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result.

DEBUG OPTIONS

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section **Data Storage** 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.
- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

My WMI sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/1043

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.220 WMI HDD Health Sensor

The WMI HDD Health sensor connects to the parent device via Windows Management Instrumentation (WMI) and monitors the health of IDE disk drives on the target system, using Self-Monitoring, Analysis and Reporting Technology (S.M.A.R.T.). This is built into most modern IDE hard disk drives.

It can show the following, among others:

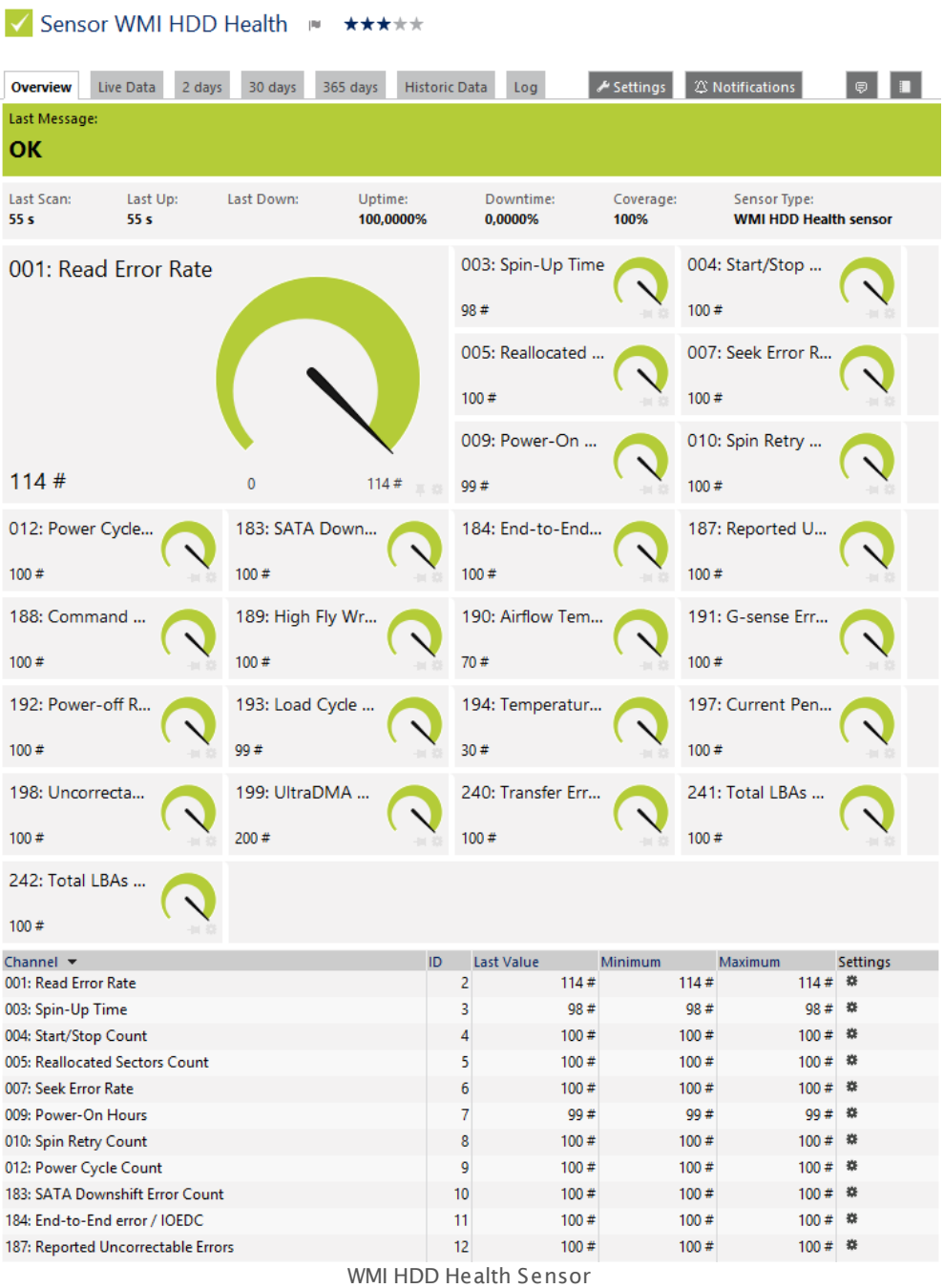
- Read Error Rate
- Spin-Up Time
- Start/Stop Count
- Reallocated Sectors Count
- Seek Error Rate
- Power-On Hours
- Spin Retry Count
- Calibration Retry Count
- Power Cycle Count
- Power-off Retract Count
- Load Cycle Count
- Temperature Celsius
- Reallocation Event Count
- Current Pending Sector Count
- Uncorrectable Sector Count
- UltraDMA CRC Error Count
- Write Error Rate
- Transfer Error Rate
- Total LBAs Written
- Total LBAs Read

Which channels the sensor actually shows might depend on the monitored device and the sensor setup. The channel names indicate the ID of the S.M.A.R.T. attribute, followed by a colon, and the typical meaning of the channel. The sensor can also show other attributes that the target device returns, but some channels will have the name **Unknown Channel**. This happens if PRTG cannot match the ID of a found attribute with an internally defined channel name.

Some vendors do not agree on attribute definitions and define meanings other than the common one.

Every attribute of a disk assumes a value. PRTG shows these attributes as channels with their last, minimum, and maximum value. These channel values change over time and indicate the disk health—higher values correspond to a better health. The disk's attributes come with a threshold, defined by the manufacturer of the drive. If a channel value is lower than this threshold, the sensor is automatically set to a **Warning** status. This indicates that the Self-Monitoring, Analysis and Reporting Technology (S.M.A.R.T.) status of the HDD might break soon.

There are no thresholds defined for some attributes and because of this they cannot be judged for a status other than **Up**. You can **Define Lookups** and use them with affected channels to get the desired status for a return value.



WMI HDD Health Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/wmi_hdd_health.png

Remarks

- This sensor officially requires Windows Vista or later on the target machine that holds the hard disk drives you want to monitor. The sensor may not work reliably if the target machine runs on Windows 2003 or Windows XP. Due to a known bug in those systems, the sensor may not be able to detect available hard disk drives.

- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per probe 111. Above this number, please consider using multiple **Remote Probes** 3196 for load balancing.
- For a general introduction to the technology behind WMI, please see manual section **Monitoring via WMI** 3092.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the IDE disks you want to monitor. PRTG creates one sensor for each IDE device you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SMART SPECIFIC

IDE Devices	You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items. . The items shown in the list are specific to the parent device you create the sensor on.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SMART SPECIFIC

Serial No.	Shows the serial number of the monitored disk. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Size (GB)	Shows the size of the monitored disk in gigabytes. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Name	Shows the name of the monitored disk. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).

DEBUG OPTIONS

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result**: Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section **Data Storage** 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.
- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

SENSOR DISPLAY

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.

SCANNING INTERVAL

- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.
	Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:
	▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

(i) To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

(i) Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

My WMI sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/1043

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.221 WMI Logical Disk I/O Sensor

The WMI Logical Disk I/O sensor monitors the disk usage of a logical disk or mount point on a Windows system using Windows Management Instrumentation (WMI).

The sensor provides the following information:

- Free space
- Disk latency
- Disk bandwidth
- Disk queue data
- Disk IOs

This sensor shows performance data from counters that monitor logical partitions of a hard drive. The system monitor identifies logical disk instances by their identifier, such as C, and the sensor reads the logical disk object in the system monitor and returns the values.

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

WMI Logical Disk I/O Sensor

Click here to enlarge: https://media-s3.paessler.com/prtg-screenshots/WMI_Logical_Disk_IO_Sensor.png

Remarks

- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per probe 111. Above this number, please consider using multiple **Remote Probes** 3196 for load balancing.
- For a general introduction to the technology behind WMI, please see manual section **Monitoring via WMI** 3092.
- This sensor type supports Windows Server 2008 R2 or later. It will not work on previous Windows versions (Windows Server 2008 or earlier).

- Currently, this sensor type is in beta status. The methods of operating can change at any time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the logical disks and mount points you want to monitor. PRTG creates one sensor for each counter you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

WMI LOGICAL DISK I/O SPECIFIC

Logical Disk(s)	Select the logical disks and mount points you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

WMI LOGICAL DISK I/O SPECIFIC

Logical Disk(s)	Shows the logical disk or mount point that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

DEBUG OPTIONS

Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result.

DEBUG OPTIONS

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section Data Storage 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.
- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings 2782 settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

My WMI sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/1043

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

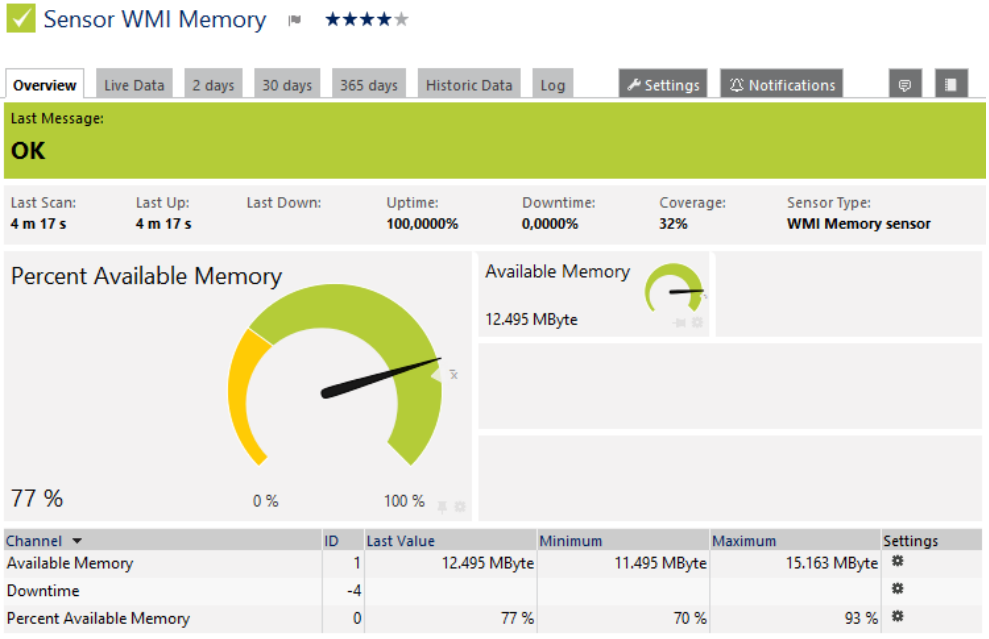
Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.222 WMI Memory Sensor

The WMI Memory sensor monitors available (free) system memory on Windows systems using Windows Management Instrumentation (WMI).

- It shows the available memory in percent and bytes.



WMI Memory Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/wmi_memory.png

Remarks

- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per probe 111. Above this number, please consider using multiple **Remote Probes** 3196 for load balancing.
- For a general introduction to the technology behind WMI, please see manual section **Monitoring via WMI** 3092.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DEBUG OPTIONS

Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result.

DEBUG OPTIONS

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section **Data Storage** 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

WMI ALTERNATIVE QUERY

Errors and Invalid Data	This is an extended help field only. PRTG's WMI sensors are equipped with the most efficient and accurate WMI queries. However, Microsoft has changed (and will continue to do so in the future) some WMI classes over the various Windows/ServicePack/ patchlevel versions, resulting in errors like "class not valid" or "invalid data". Wherever possible, PRTG features an alternative query that might work in your specific configuration. If you keep getting errors for this sensor, please try enabling the alternative query method below.
Alternative Query	Choose the method PRTG uses to query via WMI. For compatibility reasons, you can enable an alternative query method. We recommend that you use the default value. You can choose between: • **Use default (recommended)**: Use PRTG's standard method to query WMI. This is the best setting in most cases. • **Use alternative (if default does not work)**: Use an alternative method to query WMI. If you keep getting errors with the default setting, please try this setting.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

My WMI sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/1043

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.223 WMI Microsoft SQL Server 2005 Sensor (Deprecated)

IMPORTANT NOTICE

This sensor type is deprecated.

Monitoring of Microsoft SQL Server 2005 using PRTG is discontinued. It cannot be monitored with PRTG anymore with the latest updates of SQL Server 2005. The reason for this is a software update delivered by Microsoft in August 2012. The following updates cause this issue:

- **Security Update for SQL Server 2005 Service Pack 4 (KB2716429)**
- **Security Update for SQL Server 2005 Service Pack 4 (KB2716427)**

We have made reasonable effort to fix this from our side but we were unable to. We do not have instructions to circumvent this issue at this time. Please ask the vendor to fix this.

More

Knowledge Base: Why does my WMI Microsoft SQL Server 2005 Sensor not work anymore?

- https://kb.paessler.com/en/topic/44713

The WMI Microsoft SQL Server sensor monitors the performance of a Microsoft SQL server via Windows Management Instrumentation (WMI). This sensor can monitor **SQL General Statistics**, **Access Methods**, the **Buffer Manager**, the **Memory Manager**, the **Locks Manager**, and **SQL Statistics**. The channels that are actually available for a sensor depend on which performance counters you choose during setup.

CHANNEL OVERVIEW

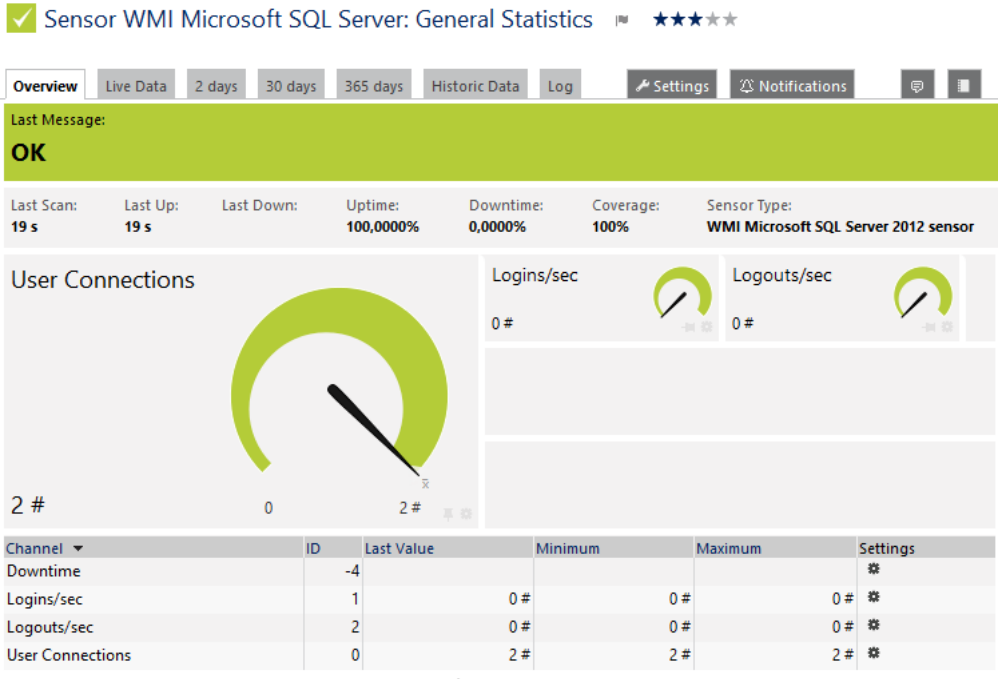
User Connections	Number of user connections. Because each user connection consumes some memory, configuring overly high numbers of user connections could affect throughput. Set user connections to the maximum expected number of concurrent users.
Logins	Total number of logins started per second.
Logouts	Total number of logout operations started per second.
Full Scans	Number of unrestricted full scans per second. These can be either base-table or full-index scans.

CHANNEL OVERVIEW

Page Splits	Number of page splits per second that occur as the result of overflowing index pages.
Table Lock Escalations	Number of times locks on a table were escalated.
Buffer Cache Hit Ratio	Percentage of pages found in the buffer cache without having to read from disk. The ratio is the total number of cache hits divided by the total number of cache lookups since an instance of SQL Server was started. After a long period of time, the ratio moves very little. Because reading from the cache is much less expensive than reading from disk, you want this ratio to be high. Generally, you can increase the buffer cache hit ratio by increasing the amount of memory available to SQL Server.
Database Pages	Number of pages in the buffer pool with database content.
Stolen Pages	Number of pages used for miscellaneous server purposes (including procedure cache).
Page Life Expectancy	Number of seconds a page will stay in the buffer pool without references.
Connection Memory (KB)	Total amount of dynamic memory the server is using for maintaining connections.
Optimizer Memory (KB)	Total amount of dynamic memory the server is using for query optimization.
Total Server Memory (KB)	Total amount of dynamic memory (in kilobytes) that the server is using currently.
Target Server Memory (KB)	Total amount of dynamic memory the server can consume.
SQL Cache Memory (KB)	Total amount of dynamic memory the server is using for the dynamic SQL cache.
Lock Requests	Number of new locks and lock conversions per second requested from the lock manager.
Deadlocks	Number of lock requests per second that resulted in a deadlock.
Average Wait Time	Average amount of wait time (in milliseconds) for each lock request that resulted in a wait.

CHANNEL OVERVIEW

Batch Requests	Number of Transact-SQL command batches received per second. This statistic is affected by all constraints (such as I/O, number of users, cache size, complexity of requests, and so on). High batch requests mean good throughput.
SQL Compilations	Number of SQL compilations per second. Indicates the number of times the compile code path is entered. Includes compiles due to recompiles. After SQL Server user activity is stable, this value reaches a steady state.
SQL Re-Compilations	Number of SQL recompiles per second. Counts the number of times recompiles are triggered. In general, you want the recompiles to be low.



WMI Microsoft SQL Server Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/wmi_microsoft_sql_server.png

Remarks

- This sensor can only be added to a device (computer) running a Microsoft SQL database.
- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.

- Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per probe 111. Above this number, please consider using multiple **Remote Probes** 3196 for load balancing.
- For a general introduction to the technology behind WMI, please see manual section **Monitoring via WMI** 3092.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the instances of the Microsoft SQL server you want to monitor. PRTG creates one sensor for each instance you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SQL SERVER SETTINGS

MS SQL Server Instance	You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items. Display name and service name are provided as returned by the SQL server.
SQL Server Version	Enter the version of the SQL server. Usually, you can keep the default value.

SQL COUNTER SPECIFIC

SQL Performance Counters	You see a list of different performance counters that the sensor can monitor for the instance(s) that you selected above. Every sensor that PRTG creates for the server instances monitors the performance counter you select here. Choose from: ▪ **General Statistics**: Read general performance counters. This shows the number of user connections, and the number of logins and logouts per second.

SQL COUNTER SPECIFIC

- **Access Methods**: Read access method counters. This shows the number of full scans, page splits, and table lock escalations (per second).
- **Buffer Manager**: Read buffer manager counters. This shows the buffer cache hit ratio in percent, and the number of database pages and stolen pages.
- **Memory Manager**: Read memory manager counters. This shows the connection memory, optimizer memory, total server memory, target server memory, and SQL cache memory (in kb).
- **Locks**: Read locks counters. This shows the number of lock requests and deadlocks (per second), and the average wait time.
- **SQL Statistics**: Read SQL statistics. This shows the number of batch requests, SQL compilations, and SQL re-compilations (per second).

Depending on your selection, PRTG creates a sensor with the specified channels.

To monitor several performance counters for an instance, please add the sensor several times.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	Enter one or more **Tags**, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SQL SERVER SETTINGS

Service	Shows the service that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Name	Shows the name of the server instance that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
WMI Class Name	Select whether PRTG selects the name of the WMI class used for monitoring automatically. Choose between: ▪ **Automatic**: Choose WMI class automatically. We recommend this setting. ▪ **Manual**: Manually enter a WMI class name. Use this if your server instance returns an error code in automatic mode.
WMI Class	This field is only shown if you enable manual WMI class selection above. This setting is intended for experienced users only. Enter the WMI class name that the sensor uses for monitoring your server instance.
Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result.

SQL SERVER SETTINGS

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section **Data Storage** 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SQL COUNTER SPECIFIC

SQL Performance Counters	Shows the performance counter that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel.

SENSOR DISPLAY

	▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. ⓘ This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.

SCANNING INTERVAL

- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. ⓘ To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

My WMI sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/1043

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.224 WMI Microsoft SQL Server 2008 Sensor

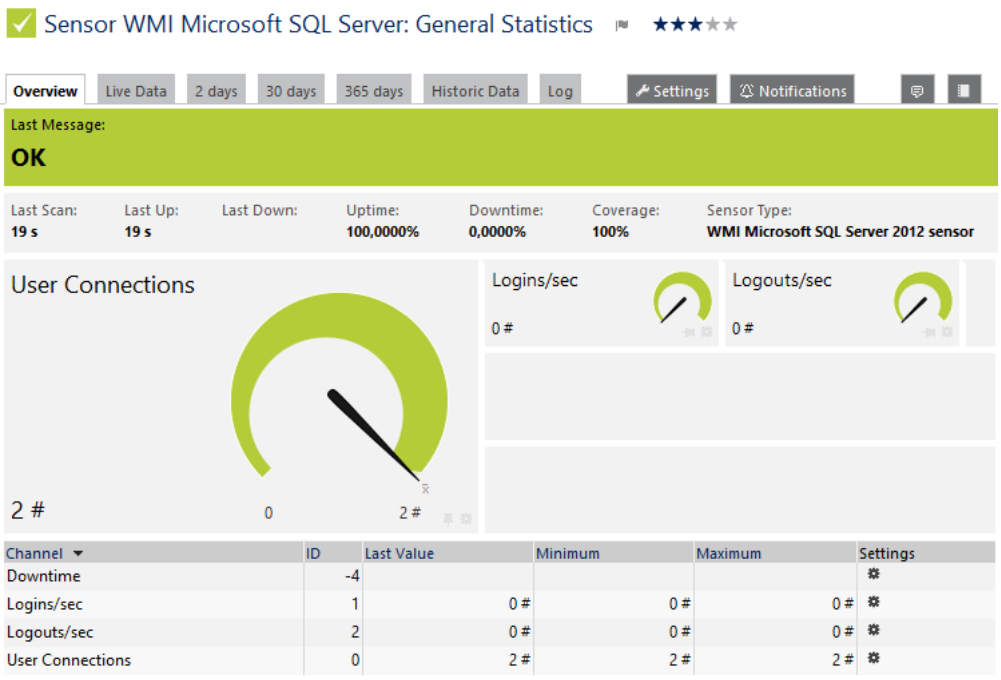
The WMI Microsoft SQL Server sensor monitors the performance of a Microsoft SQL server via Windows Management Instrumentation (WMI). This sensor can monitor **SQL General Statistics**, **Access Methods**, the **Buffer Manager**, the **Memory Manager**, the **Locks Manager**, and **SQL Statistics**. The channels that are actually available for a sensor depend on which performance counters you choose during setup.

CHANNEL OVERVIEW

User Connections	Number of user connections. Because each user connection consumes some memory, configuring overly high numbers of user connections could affect throughput. Set user connections to the maximum expected number of concurrent users.
Logins	Total number of logins started per second.
Logouts	Total number of logout operations started per second.
Full Scans	Number of unrestricted full scans per second. These can be either base-table or full-index scans.
Page Splits	Number of page splits per second that occur as the result of overflowing index pages.
Table Lock Escalations	Number of times locks on a table were escalated.
Buffer Cache Hit Ratio	Percentage of pages found in the buffer cache without having to read from disk. The ratio is the total number of cache hits divided by the total number of cache lookups since an instance of SQL Server was started. After a long period of time, the ratio moves very little. Because reading from the cache is much less expensive than reading from disk, you want this ratio to be high. Generally, you can increase the buffer cache hit ratio by increasing the amount of memory available to SQL Server.
Database Pages	Number of pages in the buffer pool with database content.
Stolen Pages	Number of pages used for miscellaneous server purposes (including procedure cache).
Page Life Expectancy	Number of seconds a page will stay in the buffer pool without references.
Connection Memory (KB)	Total amount of dynamic memory the server is using for maintaining connections.

CHANNEL OVERVIEW

Optimizer Memory (KB)	Total amount of dynamic memory the server is using for query optimization.
Total Server Memory (KB)	Total amount of dynamic memory (in kilobytes) that the server is using currently.
Target Server Memory (KB)	Total amount of dynamic memory the server can consume.
SQL Cache Memory (KB)	Total amount of dynamic memory the server is using for the dynamic SQL cache.
Lock Requests	Number of new locks and lock conversions per second requested from the lock manager.
Deadlocks	Number of lock requests per second that resulted in a deadlock.
Average Wait Time	Average amount of wait time (in milliseconds) for each lock request that resulted in a wait.
Batch Requests	Number of Transact-SQL command batches received per second. This statistic is affected by all constraints (such as I/O, number of users, cache size, complexity of requests, and so on). High batch requests mean good throughput.
SQL Compilations	Number of SQL compilations per second. Indicates the number of times the compile code path is entered. Includes compiles due to recompiles. After SQL Server user activity is stable, this value reaches a steady state.
SQL Re-Compilations	Number of SQL recompiles per second. Counts the number of times recompiles are triggered. In general, you want the recompiles to be low.



WMI Microsoft SQL Server Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/wmi_microsoft_sql_server.png

Remarks

- This sensor can only be added to a device (computer) running a Microsoft SQL database.
- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per probe 111. Above this number, please consider using multiple **Remote Probes** 3196 for load balancing.
- For a general introduction to the technology behind WMI, please see manual section **Monitoring via WMI** 3092.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the instances of the Microsoft SQL server you want to monitor. PRTG creates one sensor for each instance you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SQL SERVER SETTINGS

MS SQL Server Instance	You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items. Display name and service name are provided as returned by the SQL server.
SQL Server Version	Enter the version of the SQL server. Usually, you can keep the default value.

SQL COUNTER SPECIFIC

SQL Performance Counters	You see a list of different performance counters that the sensor can monitor for the instance(s) that you selected above. Every sensor that PRTG creates for the server instances monitors the performance counter you select here. Choose from: ▪ **General Statistics**: Read general performance counters. This shows the number of user connections, and the number of logins and logouts per second. ▪ **Access Methods**: Read access method counters. This shows the number of full scans, page splits, and table lock escalations (per second). ▪ **Buffer Manager**: Read buffer manager counters. This shows the buffer cache hit ratio in percent, and the number of database pages and stolen pages. ▪ **Memory Manager**: Read memory manager counters. This shows the connection memory, optimizer memory, total server memory, target server memory, and SQL cache memory (in kb). ▪ **Locks**: Read locks counters. This shows the number of lock requests and deadlocks (per second), and the average wait time. ▪ **SQL Statistics**: Read SQL statistics. This shows the number of batch requests, SQL compilations, and SQL re-compilations (per second). Depending on your selection, PRTG creates a sensor with the specified channels.

SQL COUNTER SPECIFIC

To monitor several performance counters for an instance, please add the sensor several times.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SQL SERVER SETTINGS

Service	Shows the service that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Name	Shows the name of the server instance that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
WMI Class Name	Select whether PRTG selects the name of the WMI class used for monitoring automatically. Choose between: ▪ **Automatic**: Choose WMI class automatically. We recommend this setting. ▪ **Manual**: Manually enter a WMI class name. Use this if your server instance returns an error code in automatic mode.
WMI Class	This field is only shown if you enable manual WMI class selection above. This setting is intended for experienced users only. Enter the WMI class name that the sensor uses for monitoring your server instance.
Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section **Data Storage** 3226. You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SQL COUNTER SPECIFIC

SQL Performance Counters	Shows the performance counter that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply. If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply. If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

My WMI sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/1043

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.225 WMI Microsoft SQL Server 2012 Sensor

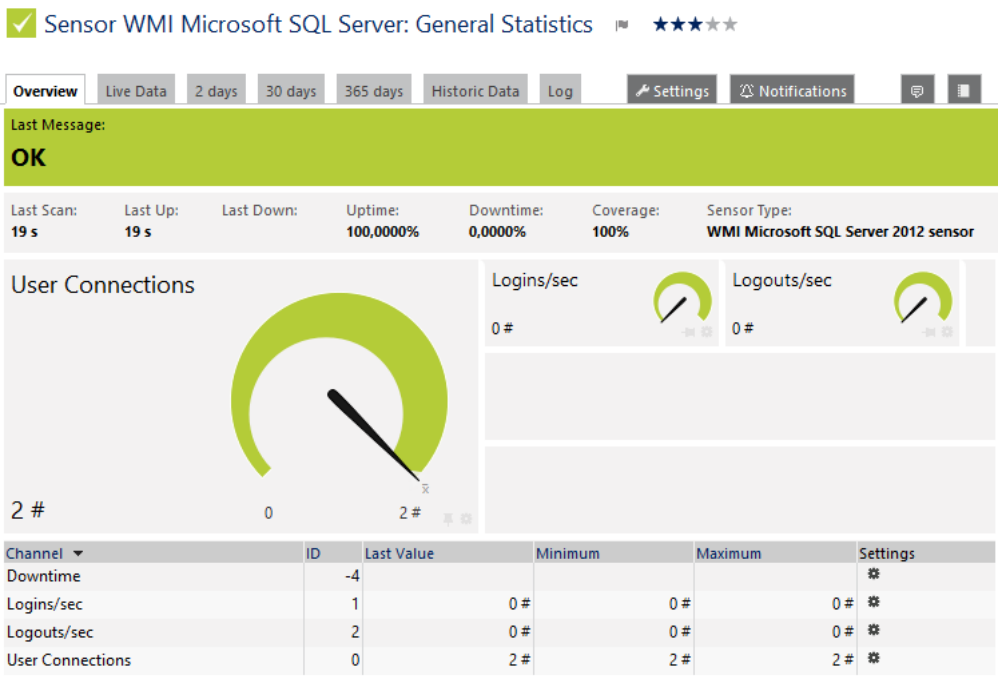
The WMI Microsoft SQL Server sensor monitors the performance of a Microsoft SQL server via Windows Management Instrumentation (WMI). This sensor can monitor **SQL General Statistics**, **Access Methods**, the **Buffer Manager**, the **Memory Manager**, the **Locks Manager**, and **SQL Statistics**. The channels that are actually available for a sensor depend on which performance counters you choose during setup.

CHANNEL OVERVIEW

User Connections	Number of user connections. Because each user connection consumes some memory, configuring overly high numbers of user connections could affect throughput. Set user connections to the maximum expected number of concurrent users.
Logins	Total number of logins started per second.
Logouts	Total number of logout operations started per second.
Full Scans	Number of unrestricted full scans per second. These can be either base-table or full-index scans.
Page Splits	Number of page splits per second that occur as the result of overflowing index pages.
Table Lock Escalations	Number of times locks on a table were escalated.
Buffer Cache Hit Ratio	Percentage of pages found in the buffer cache without having to read from disk. The ratio is the total number of cache hits divided by the total number of cache lookups since an instance of SQL Server was started. After a long period of time, the ratio moves very little. Because reading from the cache is much less expensive than reading from disk, you want this ratio to be high. Generally, you can increase the buffer cache hit ratio by increasing the amount of memory available to SQL Server.
Database Pages	Number of pages in the buffer pool with database content.
Stolen Pages	Number of pages used for miscellaneous server purposes (including procedure cache).
Page Life Expectancy	Number of seconds a page will stay in the buffer pool without references.
Connection Memory (KB)	Total amount of dynamic memory the server is using for maintaining connections.

CHANNEL OVERVIEW

Optimizer Memory (KB)	Total amount of dynamic memory the server is using for query optimization.
Total Server Memory (KB)	Total amount of dynamic memory (in kilobytes) that the server is using currently.
Target Server Memory (KB)	Total amount of dynamic memory the server can consume.
SQL Cache Memory (KB)	Total amount of dynamic memory the server is using for the dynamic SQL cache.
Lock Requests	Number of new locks and lock conversions per second requested from the lock manager.
Deadlocks	Number of lock requests per second that resulted in a deadlock.
Average Wait Time	Average amount of wait time (in milliseconds) for each lock request that resulted in a wait.
Batch Requests	Number of Transact-SQL command batches received per second. This statistic is affected by all constraints (such as I/O, number of users, cache size, complexity of requests, and so on). High batch requests mean good throughput.
SQL Compilations	Number of SQL compilations per second. Indicates the number of times the compile code path is entered. Includes compiles due to recompiles. After SQL Server user activity is stable, this value reaches a steady state.
SQL Re-Compilations	Number of SQL recompiles per second. Counts the number of times recompiles are triggered. In general, you want the recompiles to be low.



WMI Microsoft SQL Server Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/wmi_microsoft_sql_server.png

Remarks

- This sensor can only be added to a device (computer) running a Microsoft SQL database.
- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per probe 111. Above this number, please consider using multiple **Remote Probes** 3196 for load balancing.
- For a general introduction to the technology behind WMI, please see manual section **Monitoring via WMI** 3092.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the instances of the Microsoft SQL server you want to monitor. PRTG creates one sensor for each instance you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SQL SERVER SETTINGS

MS SQL Server Instance	You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items. Display name and service name are provided as returned by the SQL server.
SQL Server Version	Enter the version of the SQL server. Usually, you can keep the default value.

SQL COUNTER SPECIFIC

SQL Performance Counters	You see a list of different performance counters that the sensor can monitor for the instance(s) that you selected above. Every sensor that PRTG creates for the server instances monitors the performance counter you select here. Choose from: ▪ **General Statistics**: Read general performance counters. This shows the number of user connections, and the number of logins and logouts per second. ▪ **Access Methods**: Read access method counters. This shows the number of full scans, page splits, and table lock escalations (per second). ▪ **Buffer Manager**: Read buffer manager counters. This shows the buffer cache hit ratio in percent, and the number of database pages and stolen pages. ▪ **Memory Manager**: Read memory manager counters. This shows the connection memory, optimizer memory, total server memory, target server memory, and SQL cache memory (in kb). ▪ **Locks**: Read locks counters. This shows the number of lock requests and deadlocks (per second), and the average wait time. ▪ **SQL Statistics**: Read SQL statistics. This shows the number of batch requests, SQL compilations, and SQL re-compilations (per second). Depending on your selection, PRTG creates a sensor with the specified channels.

SQL COUNTER SPECIFIC

To monitor several performance counters for an instance, please add the sensor several times.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SQL SERVER SETTINGS

Service	Shows the service that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Name	Shows the name of the server instance that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
WMI Class Name	Select whether PRTG selects the name of the WMI class used for monitoring automatically. Choose between: ▪ **Automatic**: Choose WMI class automatically. We recommend this setting. ▪ **Manual**: Manually enter a WMI class name. Use this if your server instance returns an error code in automatic mode.
WMI Class	This field is only shown if you enable manual WMI class selection above. This setting is intended for experienced users only. Enter the WMI class name that the sensor uses for monitoring your server instance.
Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section **Data Storage** 3226. You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SQL COUNTER SPECIFIC

SQL Performance Counters	Shows the performance counter that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply. If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply. If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

My WMI sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/1043

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.226 WMI Microsoft SQL Server 2014 Sensor

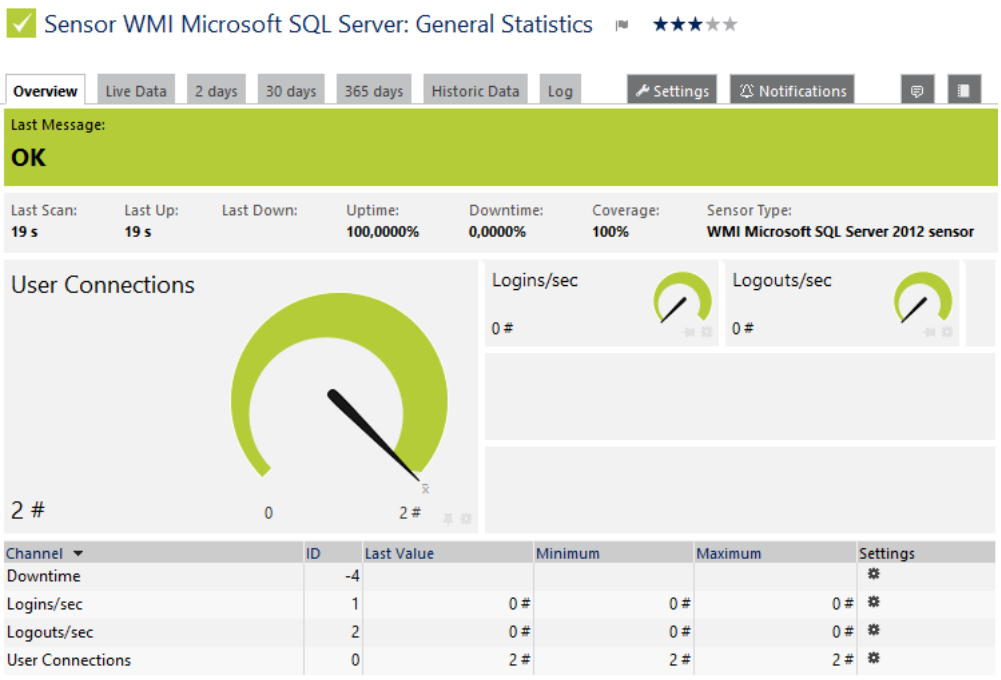
The WMI Microsoft SQL Server sensor monitors the performance of a Microsoft SQL server via Windows Management Instrumentation (WMI). This sensor can monitor **SQL General Statistics**, **Access Methods**, the **Buffer Manager**, the **Memory Manager**, the **Locks Manager**, and **SQL Statistics**. The channels that are actually available for a sensor depend on which performance counters you choose during setup.

CHANNEL OVERVIEW

User Connections	Number of user connections. Because each user connection consumes some memory, configuring overly high numbers of user connections could affect throughput. Set user connections to the maximum expected number of concurrent users.
Logins	Total number of logins started per second.
Logouts	Total number of logout operations started per second.
Full Scans	Number of unrestricted full scans per second. These can be either base-table or full-index scans.
Page Splits	Number of page splits per second that occur as the result of overflowing index pages.
Table Lock Escalations	Number of times locks on a table were escalated.
Buffer Cache Hit Ratio	Percentage of pages found in the buffer cache without having to read from disk. The ratio is the total number of cache hits divided by the total number of cache lookups since an instance of SQL Server was started. After a long period of time, the ratio moves very little. Because reading from the cache is much less expensive than reading from disk, you want this ratio to be high. Generally, you can increase the buffer cache hit ratio by increasing the amount of memory available to SQL Server.
Database Pages	Number of pages in the buffer pool with database content.
Stolen Pages	Number of pages used for miscellaneous server purposes (including procedure cache).
Page Life Expectancy	Number of seconds a page will stay in the buffer pool without references.
Connection Memory (KB)	Total amount of dynamic memory the server is using for maintaining connections.

CHANNEL OVERVIEW

Optimizer Memory (KB)	Total amount of dynamic memory the server is using for query optimization.
Total Server Memory (KB)	Total amount of dynamic memory (in kilobytes) that the server is using currently.
Target Server Memory (KB)	Total amount of dynamic memory the server can consume.
SQL Cache Memory (KB)	Total amount of dynamic memory the server is using for the dynamic SQL cache.
Lock Requests	Number of new locks and lock conversions per second requested from the lock manager.
Deadlocks	Number of lock requests per second that resulted in a deadlock.
Average Wait Time	Average amount of wait time (in milliseconds) for each lock request that resulted in a wait.
Batch Requests	Number of Transact-SQL command batches received per second. This statistic is affected by all constraints (such as I/O, number of users, cache size, complexity of requests, and so on). High batch requests mean good throughput.
SQL Compilations	Number of SQL compilations per second. Indicates the number of times the compile code path is entered. Includes compiles due to recompiles. After SQL Server user activity is stable, this value reaches a steady state.
SQL Re-Compilations	Number of SQL recompiles per second. Counts the number of times recompiles are triggered. In general, you want the recompiles to be low.



WMI Microsoft SQL Server Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/wmi_microsoft_sql_server.png

Remarks

- This sensor can only be added to a device (computer) running a Microsoft SQL database.
- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per probe 111. Above this number, please consider using multiple **Remote Probes** 3196 for load balancing.
- For a general introduction to the technology behind WMI, please see manual section **Monitoring via WMI** 3092.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the instances of the Microsoft SQL server you want to monitor. PRTG creates one sensor for each instance you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SQL SERVER SETTINGS

MS SQL Server Instance	You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items. Display name and service name are provided as returned by the SQL server.
SQL Server Version	Enter the version of the SQL server. Usually, you can keep the default value.

SQL COUNTER SPECIFIC

SQL Performance Counters	You see a list of different performance counters that the sensor can monitor for the instance(s) that you selected above. Every sensor that PRTG creates for the server instances monitors the performance counter you select here. Choose from: ▪ **General Statistics**: Read general performance counters. This shows the number of user connections, and the number of logins and logouts per second. ▪ **Access Methods**: Read access method counters. This shows the number of full scans, page splits, and table lock escalations (per second). ▪ **Buffer Manager**: Read buffer manager counters. This shows the buffer cache hit ratio in percent, and the number of database pages and stolen pages. ▪ **Memory Manager**: Read memory manager counters. This shows the connection memory, optimizer memory, total server memory, target server memory, and SQL cache memory (in kb). ▪ **Locks**: Read locks counters. This shows the number of lock requests and deadlocks (per second), and the average wait time. ▪ **SQL Statistics**: Read SQL statistics. This shows the number of batch requests, SQL compilations, and SQL re-compilations (per second). Depending on your selection, PRTG creates a sensor with the specified channels.

SQL COUNTER SPECIFIC

To monitor several performance counters for an instance, please add the sensor several times.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SQL SERVER SETTINGS

Service	Shows the service that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Name	Shows the name of the server instance that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
WMI Class Name	Select whether PRTG selects the name of the WMI class used for monitoring automatically. Choose between: ▪ **Automatic**: Choose WMI class automatically. We recommend this setting. ▪ **Manual**: Manually enter a WMI class name. Use this if your server instance returns an error code in automatic mode.
WMI Class	This field is only shown if you enable manual WMI class selection above. This setting is intended for experienced users only. Enter the WMI class name that the sensor uses for monitoring your server instance.
Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section **Data Storage** 3226. You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SQL COUNTER SPECIFIC

SQL Performance Counters	Shows the performance counter that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply. If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply. If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

My WMI sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/1043

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.227 WMI Microsoft SQL Server 2016 Sensor

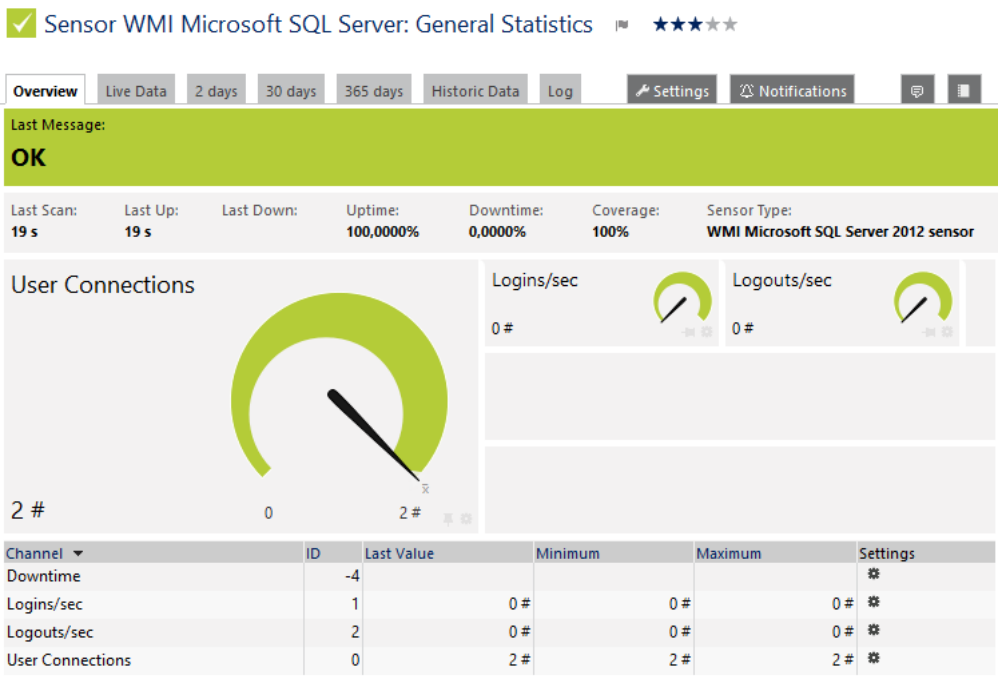
The WMI Microsoft SQL Server sensor monitors the performance of a Microsoft SQL server via Windows Management Instrumentation (WMI). This sensor can monitor **SQL General Statistics**, **Access Methods**, the **Buffer Manager**, the **Memory Manager**, the **Locks Manager**, and **SQL Statistics**. The channels that are actually available for a sensor depend on which performance counters you choose during setup.

CHANNEL OVERVIEW

User Connections	Number of user connections. Because each user connection consumes some memory, configuring overly high numbers of user connections could affect throughput. Set user connections to the maximum expected number of concurrent users.
Logins	Total number of logins started per second.
Logouts	Total number of logout operations started per second.
Full Scans	Number of unrestricted full scans per second. These can be either base-table or full-index scans.
Page Splits	Number of page splits per second that occur as the result of overflowing index pages.
Table Lock Escalations	Number of times locks on a table were escalated.
Buffer Cache Hit Ratio	Percentage of pages found in the buffer cache without having to read from disk. The ratio is the total number of cache hits divided by the total number of cache lookups since an instance of SQL Server was started. After a long period of time, the ratio moves very little. Because reading from the cache is much less expensive than reading from disk, you want this ratio to be high. Generally, you can increase the buffer cache hit ratio by increasing the amount of memory available to SQL Server.
Database Pages	Number of pages in the buffer pool with database content.
Stolen Pages	Number of pages used for miscellaneous server purposes (including procedure cache).
Page Life Expectancy	Number of seconds a page will stay in the buffer pool without references.
Connection Memory (KB)	Total amount of dynamic memory the server is using for maintaining connections.

CHANNEL OVERVIEW

Optimizer Memory (KB)	Total amount of dynamic memory the server is using for query optimization.
Total Server Memory (KB)	Total amount of dynamic memory (in kilobytes) that the server is using currently.
Target Server Memory (KB)	Total amount of dynamic memory the server can consume.
SQL Cache Memory (KB)	Total amount of dynamic memory the server is using for the dynamic SQL cache.
Lock Requests	Number of new locks and lock conversions per second requested from the lock manager.
Deadlocks	Number of lock requests per second that resulted in a deadlock.
Average Wait Time	Average amount of wait time (in milliseconds) for each lock request that resulted in a wait.
Batch Requests	Number of Transact-SQL command batches received per second. This statistic is affected by all constraints (such as I/O, number of users, cache size, complexity of requests, and so on). High batch requests mean good throughput.
SQL Compilations	Number of SQL compilations per second. Indicates the number of times the compile code path is entered. Includes compiles due to recompiles. After SQL Server user activity is stable, this value reaches a steady state.
SQL Re-Compilations	Number of SQL recompiles per second. Counts the number of times recompiles are triggered. In general, you want the recompiles to be low.



WMI Microsoft SQL Server Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/wmi_microsoft_sql_server.png

Remarks

- This sensor can only be added to a device (computer) running a Microsoft SQL database.
- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per probe 111. Above this number, please consider using multiple **Remote Probes** 3196 for load balancing.
- For a general introduction to the technology behind WMI, please see manual section **Monitoring via WMI** 3092.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the instances of the Microsoft SQL server you want to monitor. PRTG creates one sensor for each instance you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SQL SERVER SETTINGS

MS SQL Server Instance	You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items. Display name and service name are provided as returned by the SQL server.
SQL Server Version	Enter the version of the SQL server. Usually, you can keep the default value.

SQL COUNTER SPECIFIC

SQL Performance Counters	You see a list of different performance counters that the sensor can monitor for the instance(s) that you selected above. Every sensor that PRTG creates for the server instances monitors the performance counter you select here. Choose from: ▪ **General Statistics**: Read general performance counters. This shows the number of user connections, and the number of logins and logouts per second. ▪ **Access Methods**: Read access method counters. This shows the number of full scans, page splits, and table lock escalations (per second). ▪ **Buffer Manager**: Read buffer manager counters. This shows the buffer cache hit ratio in percent, and the number of database pages and stolen pages. ▪ **Memory Manager**: Read memory manager counters. This shows the connection memory, optimizer memory, total server memory, target server memory, and SQL cache memory (in kb). ▪ **Locks**: Read locks counters. This shows the number of lock requests and deadlocks (per second), and the average wait time. ▪ **SQL Statistics**: Read SQL statistics. This shows the number of batch requests, SQL compilations, and SQL re-compilations (per second). Depending on your selection, PRTG creates a sensor with the specified channels.

SQL COUNTER SPECIFIC

To monitor several performance counters for an instance, please add the sensor several times.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SQL SERVER SETTINGS

Service	Shows the service that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Name	Shows the name of the server instance that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
WMI Class Name	Select whether PRTG selects the name of the WMI class used for monitoring automatically. Choose between: ▪ **Automatic**: Choose WMI class automatically. We recommend this setting. ▪ **Manual**: Manually enter a WMI class name. Use this if your server instance returns an error code in automatic mode.
WMI Class	This field is only shown if you enable manual WMI class selection above. This setting is intended for experienced users only. Enter the WMI class name that the sensor uses for monitoring your server instance.
Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section **Data Storage** 3226. You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SQL COUNTER SPECIFIC

SQL Performance Counters	Shows the performance counter that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply. If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply. If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

My WMI sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/1043

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

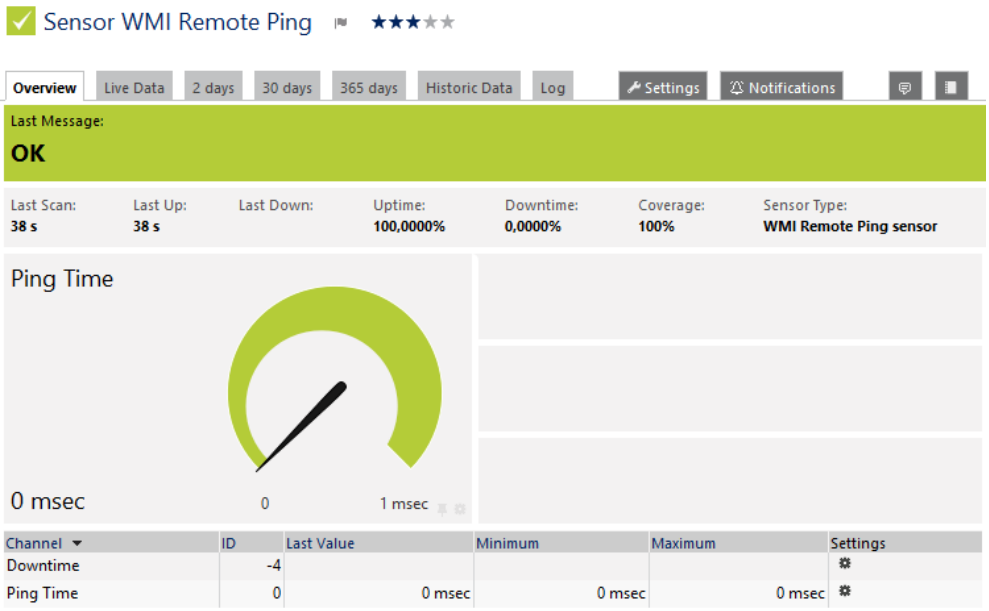
Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.228 WMI Remote Ping Sensor

The WMI Remote Ping sensor remotely connects to a Windows system using Windows Management Instrumentation (WMI), then performs an Internet Control Message Protocol (ICMP) echo request ("Ping") from this device to a specified target.

- The sensor shows the Ping time from the remote device to the target device that is being pinged.



WMI Remote Ping Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/wmi_remote_ping.png

Remarks

- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per probe 111. Above this number, please consider using multiple **Remote Probes** 3196 for load balancing.
- For a general introduction to the technology behind WMI, please see manual section **Monitoring via WMI** 3092.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

WMI REMOTE PING CONFIGURATION

Target	Enter the DNS name or IP address of the target device the Ping is sent to. The sensor remotely connects to its parent device via WMI. Then it performs a Ping request from this remote device to the target device or server. Please enter a string.

WMI REMOTE PING CONFIGURATION

Timeout (Sec.)	Enter a timeout in seconds for the Ping. If the reply takes longer than this value defines, the sensor cancels the request and triggers an error message. Please enter an integer value. The maximum timeout value is 300.
Packet Size (Bytes)	Enter the packet size in bytes for the Ping. You can choose any value between 1 and 10000. Please enter an integer value. We recommend that you use the default value.

DEBUG OPTIONS

Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section Data Storage 3226. You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor.

SENSOR DISPLAY

- **Show channels independently (default)**: Show an own graph for each channel.
- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

My WMI sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/1043

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

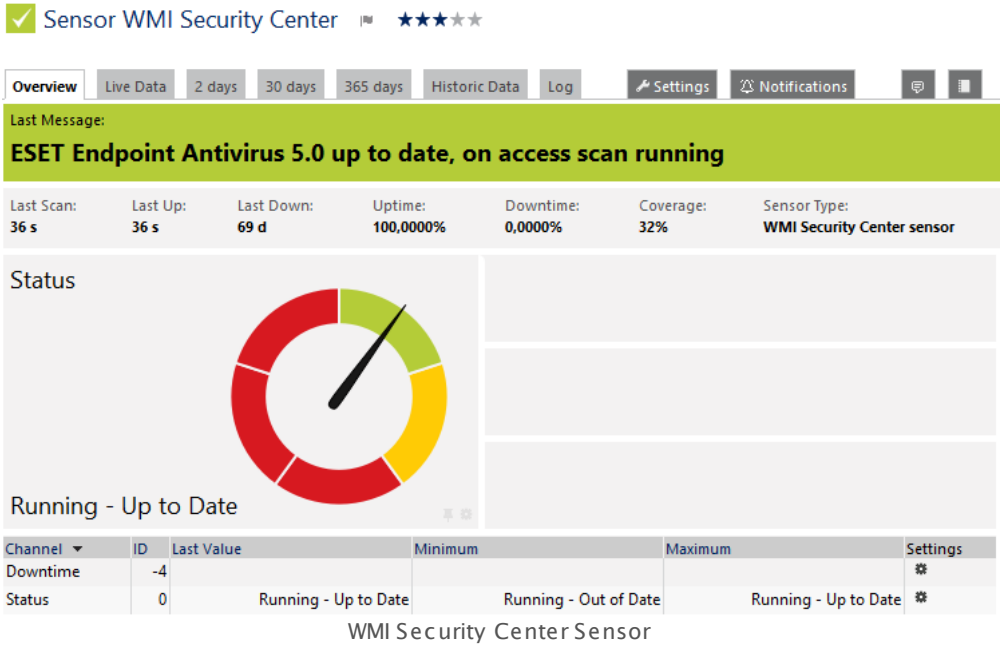
7.8.229 WMI Security Center Sensor

The WMI Security Center sensor monitors the security status of a Windows client computer using Windows Management Instrumentation (WMI). It can monitor all security products that are controlled by Windows Security Center / Windows Action Center.

- It shows the status code of the monitored product and sets the sensor status accordingly. A sensor status showing **Up** indicates that the product is up to date and the access scan is running.

Possible return values for status codes are:

Status Code	Meaning: Status of Monitored Security Product Is ...	Will Result in Sensor Status
0	Unknown	Down
1	Not running, Out of date	Down
2	Running, Out of date	Warning
3	Not running, Up to date	Down
4	Running, Up to date	OK



WMI Security Center Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/wmi_security_center.png

Remarks

- This sensor requires Windows Vista or later on the target computer.
- This sensor type does not run on Windows Server operating systems (Windows Server 2003, 2008, 2012, 2016), because the Windows Security Center / Windows Action Center is only available on client Windows versions.
- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per probe 111. Above this number, please consider using multiple **Remote Probes** 3196 for load balancing.
- For a general introduction to the technology behind WMI, please see manual section **Monitoring via WMI** 3092.
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, please see the manual section **Define Lookups** 3183.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the security center products you want to monitor. PRTG creates one sensor for each product you select in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

WMI SECURITY CENTER SPECIFIC

Security Center Products	You see a list showing the **Name** and **Type** of all security products found in the Windows Security Center on the target device. If there are no products, you see a corresponding message. Add check marks in front of the respective lines to select the desired items. One sensor will be created for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

WMI SECURITY CENTER SPECIFIC

Display Name	Shows the name of the product monitored by this sensor. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

WMI SECURITY CENTER SPECIFIC

Type	Shows the type of the product monitored by this sensor. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

DEBUG OPTIONS

Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result. ▪ **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. For more information on how to find the folder used for storage, see section Data Storage 3226. You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.

SCANNING INTERVAL

- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

	Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

My WMI sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/1043

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.230 WMI Service Sensor

The WMI Service sensor monitors a Windows service using Windows Management Instrumentation (WMI).

It can show the following:

- Execution time of the monitoring request.

Additionally, if you enable **Monitor extended values** in the sensor settings, it can show these parameters:

- CPU usage in percent
- Pagefile usage in bytes
- Number of handles
- Number of threads
- Working set in bytes

The "Running (msec)" channel of this sensor shows the execution time of the monitoring request. It does not refer to the time the Windows service has been running! As of PRTG version 13, the name of this sensor channel is **Sensor Execution Time**.

WMI Service Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/wmi_service.png

Remarks

- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per probe 111. Above this number, please consider using multiple **Remote Probes** 3196 for load balancing.
- For a general introduction to the technology behind WMI, please see manual section **Monitoring via WMI** 3092.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the Windows services you want to monitor. PRTG creates one sensor for each service you select in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

WMI SERVICE MONITOR

Service	You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items. Name and description are provided in the language of the device's Windows installation. Later on, the sensor shows a **Down** status 163 if the service is not running.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

WMI SERVICE MONITOR

If Service is Not Running	Select whether the service will be (re)started if it is stopped or paused. Choose between: ▪ **Start/Restart service**: PRTG tries to start the service if it is not running when scanning the device. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification 2791 whenever PRTG (re)starts the service. ▪ **Do nothing**: PRTG does not start any service on the device automatically. ⓘ If you select the start/restart option and the sensor detects that the monitored service does not run, PRTG will try to restart the service during this scan and postpones the next sensor scan for one interval. With this following scan, the sensor checks if the service runs now. If starting the service was not successful or the service failed again, the sensor will show a **Down** status 163 and not try to start the service again. If the service runs after a (re)start attempt, the sensor will continue monitoring as usual.

WMI SERVICE MONITOR

If Service is Restarted

This setting is only visible if you select **Start/Restart service** above. Define what to do if PRTG restarts the service. Choose between:

- **Ignore changes**: No action is taken on change.
- **Trigger 'change' notification**: The sensor will send an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification 2791 whenever the sensor value changes.

Monitoring

Select whether you want to monitor CPU usage and other useful performance counters. Choose between:

- **Just check if service is running**: PRTG only monitors the channel "Sensor Execution Time".
- **Monitor extended values**: PRTG also monitors other useful performance counters.

Extended monitoring might cause a "Class not found" error on some Windows systems.

Service

Shows the Windows service this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Description

Shows the description of the service. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result**: Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.

  For more information on how to find the folder used for storage, see section **Data Storage** 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

Knowledge Base: How can I monitor a Windows service on Windows 2000?

- https://kb.paessler.com/en/topic/36483

My WMI sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/1043

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

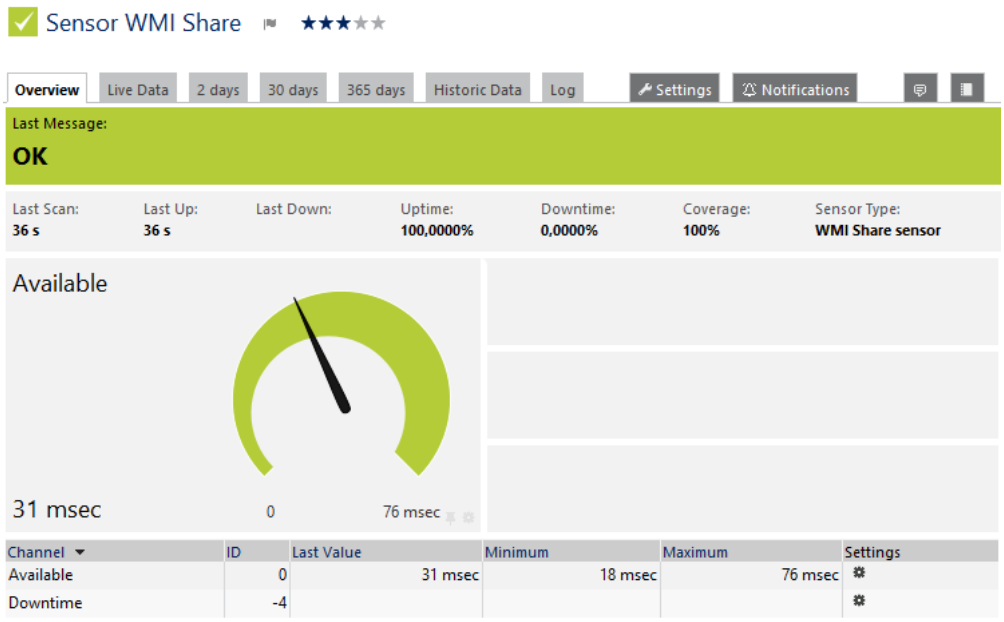
For more general information about settings, please see the **Object Settings** 188 section.

7.8.231 WMI Share Sensor

The WMI Share sensor monitors a shared resource on a Windows system using Windows Management Instrumentation (WMI).

- It shows the availability of the share.

You can define the sensor to show a **Down** status [163] for different share status messages.



WMI Share Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/wmi_share.png

Remarks

- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per probe [111]. Above this number, please consider using multiple **Remote Probes** [3196] for load balancing.
- For a general introduction to the technology behind WMI, please see manual section **Monitoring via WMI** [3092].

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the shares you want to monitor. PRTG creates one sensor for each share you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

WMI SHARED RESOURCE

Share	Select the shares you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items. To provide any shares, the LanmanServer "Server" Windows service must be running on the target computer. If it is not, there are no shares and you see a **No Share available** message here.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.

BASIC SENSOR SETTINGS

Parent Tags	Shows **Tags** [124] that this sensor inherits [124] from its parent device, group, and probe [118]. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** [124], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited [124] from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

WMI SHARED RECOURCE

Shared Recource	
Description	Shows information about the shared resource that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Type	
TypeID	

TRIGGER ERROR STATE ON FOLLOWING CONDITIONS

Select under which conditions the sensor shows a **Down** status [163] from the list below. As long as the share returns OK, the sensor status is **Up**. Add a check mark symbol in front of the according line to choose a **Down** condition. Choose none, one, or several of the following conditions.

Note: While in Down status, a sensor does not record any data in any of its channels.

TRIGGER ERROR STATE ON FOLLOWING CONDITIONS

Error	Set sensor to **Down** status if the share returns an error status. A share in this status is not operational. This condition is selected by default.
Degraded	Set sensor to **Down** status if the share returns a degraded status. A share in this status is still operational. This condition is selected by default.
Unknown	Set sensor to **Down** status if the share returns an unknown status.
Pred Fail	Set sensor to **Down** status if the share returns a "predicted fail" status. This indicates that an element works properly but predicts a failure (for example, a SMART-enabled hard drive). A share in this status is still operational. This condition is selected by default.
Starting	Set sensor to **Down** status if the share returns a starting status. A share in this status is not operational.
Stopping	Set sensor to **Down** status if the share returns a stopping status. A share in this status is not operational.
Service	Set sensor to **Down** status if the share returns a service status. This can apply during disk mirror-resilvering, reloading a user permissions list, or other administrative work on the monitored device. Not all such work is online, but the managed element is neither OK nor in one of the other states. A share in this status is not operational.
Stressed	Set sensor to **Down** status if the share returns a stressed status.
Nonrecover	Set sensor to **Down** status if the share returns a "non recover" status. This condition is selected by default.
NoContact	Set sensor to **Down** status if the share returns a "no contact" status. This condition is selected by default.
LostComm	Set sensor to **Down** status if the share returns "lost communication" status. This condition is selected by default.

DEBUG OPTIONS

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result**: Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section Data Storage 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.
- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings 2782 settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. ⓘ Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

My WMI sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/1043

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

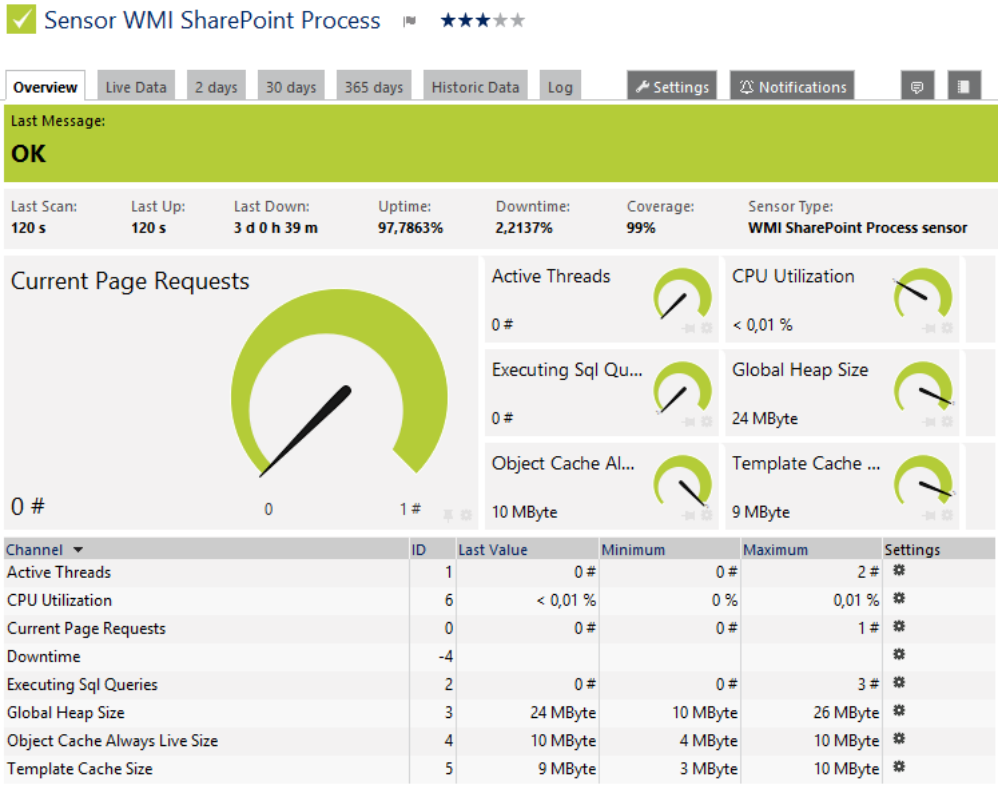
For more general information about settings, please see the **Object Settings** 188 section.

7.8.232 WMI SharePoint Process Sensor

The WMI SharePoint Process sensor monitors a Microsoft SharePoint server using Windows Management Instrumentation (WMI).

It can show the following:

- Number of current page requests
- Number of active threads
- Number of currently executed SQL queries
- Global heap size
- Object cache always live size
- Template cache size
- CPU utilization in percent



WMI SharePoint Process Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/wmi_sharepoint_process.png

Remarks

- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.

- Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per probe 111. Above this number, please consider using multiple **Remote Probes** 3196 for load balancing.
- For a general introduction to the technology behind WMI, please see manual section **Monitoring via WMI** 3092.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the SharePoint processes you want to monitor. PRTG creates one sensor for each process you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

WMI PROCESS MONITOR

SharePoint Processes	You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

WMI PROCESS MONITOR

SharePoint Process	The name of the SharePoint process that is monitored by this sensor. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

DEBUG OPTIONS

Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result.

DEBUG OPTIONS

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section Data Storage 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.
- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings 2782 settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. ⓘ Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

My WMI sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/1043

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

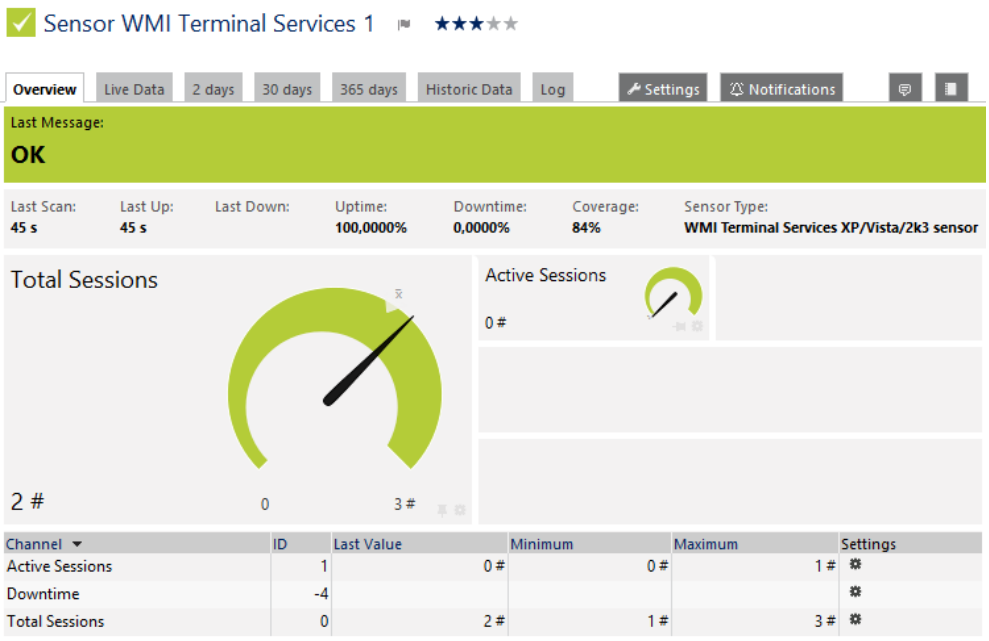
For more general information about settings, please see the **Object Settings** 188 section.

7.8.233 WMI Terminal Services (Windows 2008+) Sensor

The WMI Terminal Services sensor monitors the number of sessions on a Windows Terminal Services (Remote Desktop Services) server using Windows Management Instrumentation (WMI).

It shows the following:

- Number of active sessions: sessions with a currently logged in user, including used published applications
- Number total sessions (including inactive sessions): inactive sessions can be sessions with a disconnected user that has not logged out, or system services using a session



WMI Terminal Services Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/wmi_terminal_services.png

Remarks

- For "Total Sessions", this sensor type returns the number of active and inactive sessions, plus two additional sessions: one for the console, and another for the services. So, the number of total sessions may actually be higher than expected.
- Depending on the OS that you want to monitor, select either the sensor for Windows XP/ Vista/2003 or the one for Windows 2008 and later.
- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per probe 111. Above this number, please consider using multiple **Remote Probes** 3196 for load balancing.

- For a general introduction to the technology behind WMI, please see manual section **Monitoring via WMI** 3092.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DEBUG OPTIONS

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result**: Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section Data Storage 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.
- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings 2782 settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. ⓘ Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

My WMI sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/1043

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

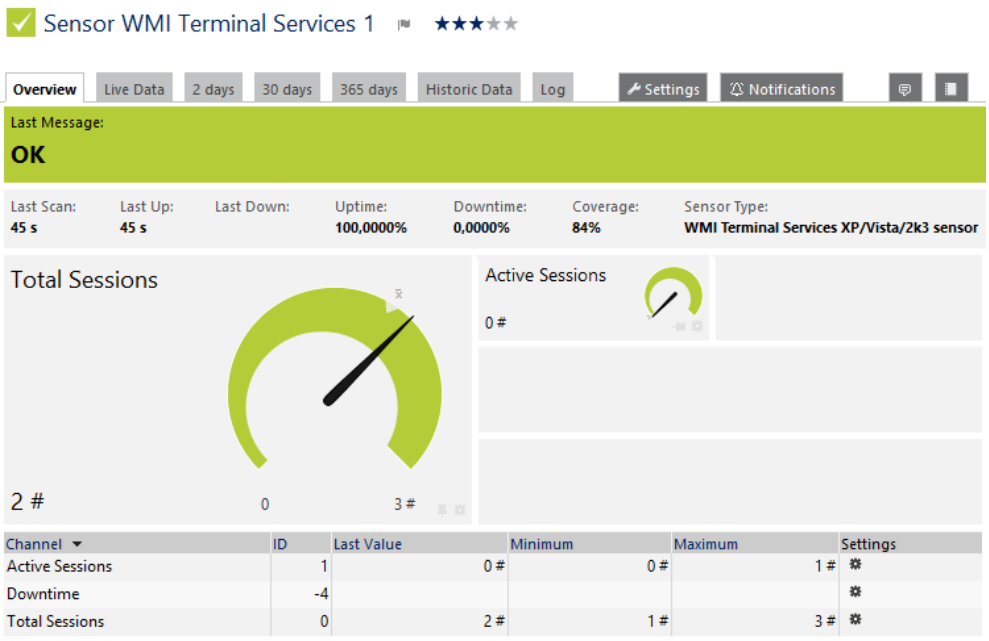
For more general information about settings, please see the **Object Settings** 188 section.

7.8.234 WMI Terminal Services (Windows XP/Vista/2003) Sensor

The WMI Terminal Services sensor monitors the number of sessions on a Windows Terminal Services (Remote Desktop Services) server using Windows Management Instrumentation (WMI).

It shows the following:

- Number of active sessions: sessions with a currently logged in user, including used published applications
- Number total sessions (including inactive sessions): inactive sessions can be sessions with a disconnected user that has not logged out, or system services using a session



WMI Terminal Services Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/wmi_terminal_services.png

Remarks

- For "Total Sessions", this sensor type returns the number of active and inactive sessions, plus two additional sessions: one for the console, and another for the services. So, the number of total sessions may actually be higher than expected.
- Depending on the OS that you want to monitor, select either the sensor for Windows XP/ Vista/2003 or the one for Windows 2008 and later.
- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per probe 111. Above this number, please consider using multiple **Remote Probes** 3196 for load balancing.

- For a general introduction to the technology behind WMI, please see manual section **Monitoring via WMI** 3092.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DEBUG OPTIONS

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result**: Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section Data Storage 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.
- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings 2782 settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. ⓘ Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

My WMI sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/1043

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

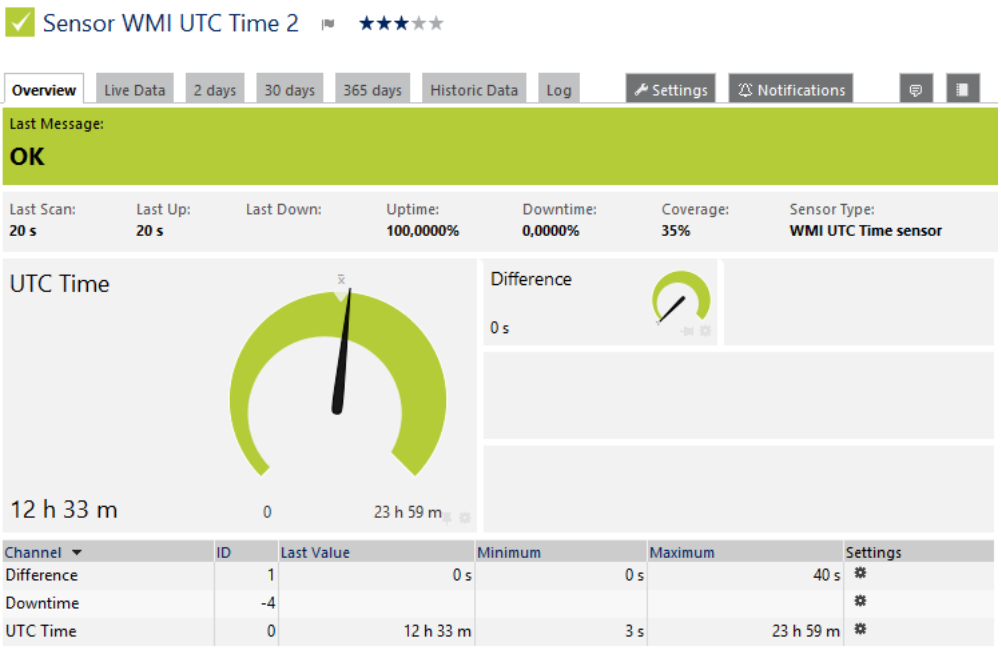
For more general information about settings, please see the **Object Settings** 188 section.

7.8.235 WMI UTC Time Sensor

The WMI UTC Time sensor monitors the UTC (Coordinated Universal Time) time of a target device using Windows Management Instrumentation (WMI).

It shows the following:

- UTC time of the target device
- Time difference between the PRTG system time and the target device in seconds



WMI UTC Time Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/wmi_utc_time.png

Remarks

- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per probe 111. Above this number, please consider using multiple **Remote Probes** 3196 for load balancing.
- For a general introduction to the technology behind WMI, please see manual section **Monitoring via WMI** 3092.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DEBUG OPTIONS

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result**: Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section Data Storage 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.
- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings 2782 settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. ⓘ Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

More

My WMI sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/1043

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

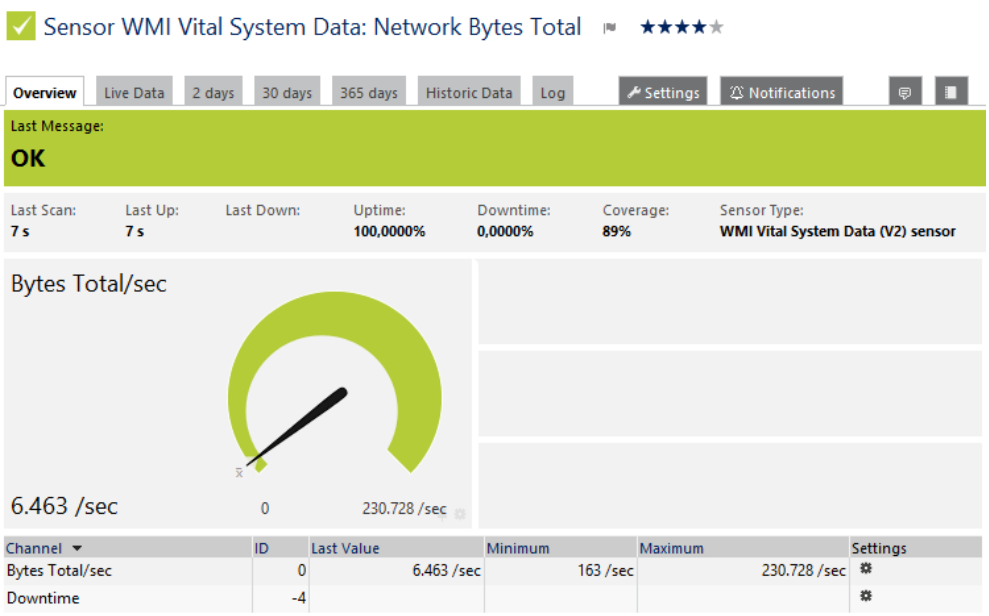
7.8.236 WMI Vital System Data (V2) Sensor

The WMI Vital System Data sensor monitors vital system parameters (CPU, thread, memory, network, pagefile) using Windows Management Instrumentation (WMI).

It can show the following:

- CPU usage: Processor, privileged, and user time
- CPU queue length
- Thread context switches
- Free physical memory
- Total visible memory
- Memory page faults, reads, and writes per second
- Memory pool paged and nonpaged bytes
- Memory committed bytes
- Network sent, received, and total bytes per second
- Network packets outbound errors
- Pagefile usage in percent
- Physical disk time in percent
- Current physical disk queue length
- Physical disk reads and writes per second
- Server bytes received, transmitted, and total
- CLR memory bytes in all heaps
- Thrown CLR exceptions per second

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



WMI Vital System Data (V2) Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/wmi_vital_system_data.png

Remarks

- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per probe 111. Above this number, please consider using multiple **Remote Probes** 3196 for load balancing.
- For a general introduction to the technology behind WMI, please see manual section **Monitoring via WMI** 3092.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the performance counters you want to monitor. PRTG creates one sensor for each counter you select in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

VITAL SYSTEM DATA READINGS ACCESSIBLE USING WMI

Performance Counter	You see a list of available vital system data values the sensor can monitor on the target device. The available options depend on your configuration. PRTG shows all possible performance counters with name and instance description (if available). Add check marks in front of the respective lines to select the desired items. One sensor will be created for each selection. You can also use the check box in the table head select and deselect all items. You can choose between the following counters: ▪ **CPU** ▪ **Thread** ▪ **Memory** ▪ **Network** ▪ **Pagefile**

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	Enter one or more **Tags**, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

READINGS ACCESSIBLE USING WMI

Display Name Instance	These fields show the parameters that are used to query data for this sensor from the target device.Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
WMI Class	
Counter	
Time Stamp	
Time Frequency	
Counter Type	
Sensor Result	Define what PRTG will do with the sensor results. Choose between: ▪ **Discard sensor result**: Do not store the sensor result.

READINGS ACCESSIBLE USING WMI

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section **Data Storage** 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
Graph Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. ⓘ Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

My WMI sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/1043

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

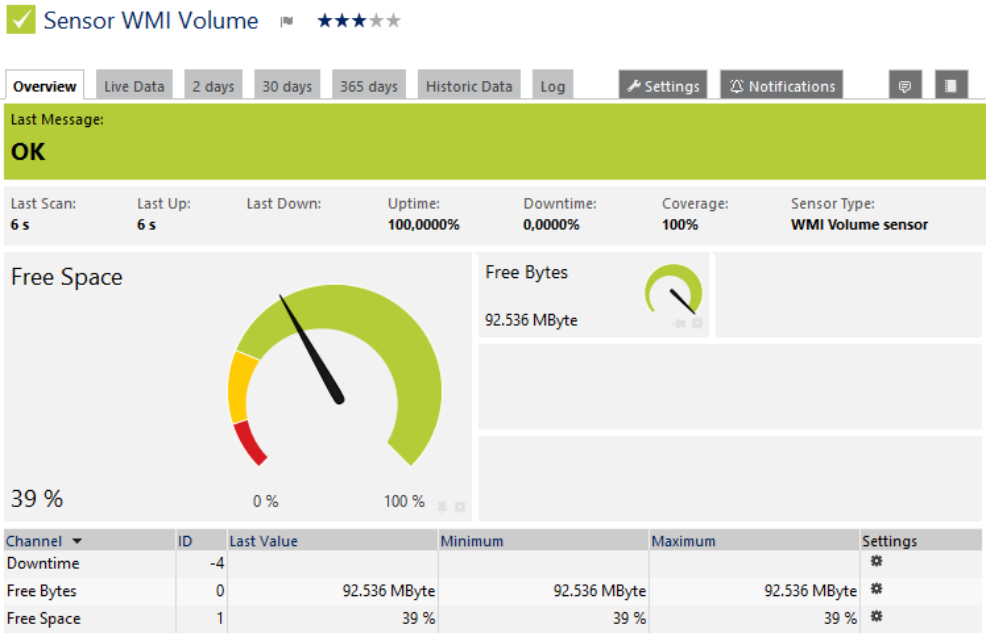
For more general information about settings, please see the **Object Settings** 188 section.

7.8.237 WMI Volume Sensor

The WMI Volume sensor monitors the free disk space on a drive, logical volume, or mount point using Windows Management Instrumentation (WMI). For each drive, logical volume or mount point, PRTG uses one sensor.

- It shows free space in percent and total.

This sensor monitors an area of storage on a hard disk. It can monitor local volumes that are formatted, unformatted, mounted, or offline. A volume is formatted by using a file system, such as File Allocation Table (FAT) or New Technology File System (NFTS), and might have a drive letter assigned to it. One hard disk can have multiple volumes, and volumes can span multiple physical disks. The sensor does not support disk drive management.



WMI Volume Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/wmi_volume.png

Remarks

- This sensor is not supported on Windows XP and earlier.
- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per probe 111. Above this number, please consider using multiple **Remote Probes** 3196 for load balancing.
- For a general introduction to the technology behind WMI, please see manual section **Monitoring via WMI** 3092.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the volumes you want to monitor. PRTG creates one sensor for each volume you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

WMI VOLUME SPECIFIC

Volumes	Select the volumes (drives, logical volumes, mount points) you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	Enter one or more **Tags**, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

WMI VOLUME SPECIFIC

DeviceID	Shows the unique identifier of the volume that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Drive Type	Shows the type of the disk drive that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
ID Selection	Specify the way how sensor identifies the volume. Choose between: ▪ **Use system device ID (recommended)**: This is usually the best option for this sensor type, because the device ID will not change when the volume is renamed. ▪ **Use drive letter**: In a Microsoft cluster environment, the device ID will change when the cluster is switched to another node. In this case, use the drive letter option to avoid issues regarding this.
Drive Letter	This field is only visible if you select the drive letter option above. Enter the letter of the drive you want to monitor followed by a double dot, for example, C:

DEBUG OPTIONS

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result**: Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section Data Storage 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.
- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings 2782 settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests. ▪ **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests. ▪ **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests. ▪ **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests. ⓘ Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

SCANNING INTERVAL

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916. Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: ▪ **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active. ▪ **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.
Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency. Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices	Dependencies** from the main menu bar.
Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

My WMI sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/1043

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.8.238 WSUS Statistics Sensor

The WSUS Statistics sensor monitors various statistics on a Windows Server Update Services (WSUS) server using Windows Management Instrumentation (WMI).

It can show the numbers of the following:

- Approved updates
- Computers having update errors
- Computers needing updates
- Computers not synchronized for 7 days
- Computers registered
- Computers up to date
- Declined updates
- Expired updates
- Not approved critical or security updates
- Not approved updates
- Total updates
- Unapproved needed updates
- Updates needed by computers
- Updates needing files
- Updates up to date
- Updates with client errors
- Updates with server errors
- Updates with stale update approvals
- Number of WSUS infrastructure updates not approved for installation

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

Channel	ID	Last Value	Minimum	Maximum	Settings
Approved updates	0	3,090 #	3,090 #	4,606 #	
Computers having update errors.	1	11 #	7 #	269,412 #	
Computers needing updates.	2	115 #	114 #	245 #	
Computers not synchronised for 7 days	3	8 #	4 #	102 #	
Computers registered	4	185 #	182 #	267 #	
Computers up to date	5	58 #	0 #	59 #	
Declined updates.	6	8,536 #	6,573 #	8,536 #	
Downtime	-4				
Expired updates.	7	0 #	0 #	0 #	
Not approved critical or security updates.	8	0 #	0 #	8 #	
Not approved updates.	9	0 #	0 #	733 #	
Total updates.	10	11,626 #	10,754 #	11,826 #	
Unapproved, needed updates.	11	0 #	0 #	106 #	
Updates needed by computers.	12	710 #	703 #	1,560 #	
Updates needing files.	13	26 #	0 #	703 #	
Updates up to date.	14	0 #	0 #	2,811 #	
Updates with client errors.	15	26 #	8 #	80 #	
Updates with server errors.	16	26 #	0 #	41 #	

WSUS Statistics Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/wsus_statistics.png

Remarks

- Requires 2769 .NET 4.0 or higher on the probe system. If the sensor shows the error PE087, please additionally install .NET 3.5 on the probe system.
- Requires 2769 WSUS 3.0 Administration Console on the probe system.

- Requires 2769 Windows credentials in the parent device settings 360.
- We recommend Windows 2012 R2 on the probe system for best performance of this sensor.
- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.

You cannot add this sensor type to local probes in PRTG on demand. If you want to use this sensor type, please add it to a remote probe device.

Requirement: .NET Framework

This sensor type requires the Microsoft .NET Framework to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the remote probe 3196. If the framework is missing, you cannot create this sensor.

Required .NET version (with latest updates): .NET 4.0 (Client Profile is sufficient), .NET 4.5, or .NET 4.6.

For more information, please see this Knowledge Base article: https://kb.paessler.com/en/topic/60543

Requirement: Windows Credentials

Requires credentials for Windows systems to be defined for the device you want to use the sensor on. In the parent device's 365 **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

If you use local credentials, please make sure that the same Windows user accounts (with the same username and password) exist on both the system running the PRTG probe and the target computer. Otherwise the sensor cannot connect correctly.

Requirement: WSUS 3.0 Administration Console

In order for this sensor to work, Microsoft's WSUS 3.0 Administration Console must be installed on the computer running the PRTG probe: Either on the local system (on every node, if on a cluster probe), or on the system running the remote probe.

Add Sensor

The **Add Sensor** dialog appears when you manually 288 add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** 360 for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree 151, as well as in alarms 190, logs 198, notifications 2829, reports 2862, maps 2885, libraries 2845, and tickets 200.
Parent Tags	Shows **Tags** 124 that this sensor inherits 124 from its parent device, group, and probe 118. This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more **Tags** 124, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited 124 from objects further up in the device tree. These are visible above as **Parent Tags**.
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SETTINGS

WSUS Server Port	Define the port where the WSUS server service runs. The default value is **8530**. Please enter an integer value.
Connection Security	Define if you want to use SSL encryption for the connection to the WSUS server or if you prefer unencrypted connections. Choose between: ▪ **Use SSL** ▪ **Do not use any encryption**

SENSOR SETTINGS

If you want to use SSL encryption, you have to configure your Windows Server Update Services (WSUS) accordingly (see also the **More** 2777 section below).

DEBUG OPTIONS

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result**: Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.
  For more information on how to find the folder used for storage, see section **Data Storage** 3226.

You cannot access stored logs of sensors that run on the local probe of PRTG on demand.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
  This option cannot be used in combination with manual Vertical Axis Scaling (available in the **Sensor Channels Settings** 2782 settings).

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 294 group's settings. To change a setting only for this object, disable inheritance by clicking the check mark in front of the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration 2955 on PRTG on premises installations.
If a Sensor Query Fails	Define the number of scanning intervals that a sensor has time reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down** status 163. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between: ▪ **Set sensor to "down" immediately**: The sensor will show an error immediately after the first failed request. ▪ **Set sensor to "warning" for 1 interval, then set to "down" (recommended)**: After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.

SCANNING INTERVAL

- **Set sensor to "warning" for 2 intervals, then set to "down"**: Show an error status only after three continuously failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down"**: Show an error status only after four continuously failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down"**: Show an error status only after five continuously failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down"**: Show an error status only after six continuously failed requests.

Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

If a channel uses lookup 3183 values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 2916.

Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously)**: No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window**: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies 2822 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the object selector 210 to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value. This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent **Device Settings** 360 or in the superior **Group Settings** 334.

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited**: Use the access rights settings of the parent object.
- **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read**: Users in this group can see the object and review its monitoring results.
- **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details on access rights, please see the section **User Access Rights** 129.

CHANNEL UNIT CONFIGURATION

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Custom channel types can be set on sensor level only.

More

Knowledge Base: Which .NET version does PRTG require?

- https://kb.paessler.com/en/topic/60543

Knowledge Base: Can I encrypt connections to my WSUS server?

- https://kb.paessler.com/en/topic/63611

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, please see the **Sensor Channels Settings** 2782 section.

Notifications

Click the **Notifications** tab to change notification triggers. For detailed information, please see the **Sensor Notifications Settings** 2791 section.

Others

For more general information about settings, please see the **Object Settings** 188 section.

7.9 Additional Sensor Types (Custom Sensors)

Users can create and use their own, self-written custom sensors in PRTG Network Monitor to go far beyond PRTG's standard sensor set. You can create your own sensors using Windows Management Instrumentation Query Language (WQL), visual basic scripting, PowerShell, batch scripting, SQL queries, by compiling an EXE or DLL file (using any Windows software development tool), and by running Python scripts.

You cannot use custom sensors on local probes in PRTG on demand (except SSH sensors). If you want to use custom sensors, please add them to a remote probe device.

Basics

For a general introduction, please see the sections about EXE/Script sensors and the API documentation 3174 which contains details about the necessary return format for these sensors. WMI Custom sensors allow executing WQL requests.

- **EXE/Script Sensor** 747
- **EXE/Script Advanced Sensor** 759
- **Python Script Advanced Sensor** 1385
- **SSH Script Sensor** 2266
- **SSH Script Advanced Sensor** 2278
- **Application Programming Interface (API) Definition** 3174
- **WMI Custom Sensor** 2512

Additionally, some types of SQL sensors execute script files with SQL queries:

- **Microsoft SQL v2 Sensor** 1135
- **MySQL v2 Sensor** 1151
- **Oracle SQL v2 Sensor** 1253
- **PostgreSQL Sensor** 1363

Custom Sensors Included in PRTG

After installing PRTG Network Monitor, you will already find a selection of custom EXE/Script, Python, and WMI WQL script sensors in the PRTG program directory 3226, as well as scripts with SQL queries for specific database sensors 2778. Many of these are sample projects that you can edit and improve for your needs.

Custom Sensors Included in PRTG—Folder: \Custom Sensors\EXE

- Demo Batchfile - Returns 200.bat
- Demo Batchfile - Set sensorstate to error.bat
- Demo Batchfile - Set sensorstate to warning.bat

- Demo Cmd - Returns 200.cmd
- Demo Dll - Returns a random integer.dll
- Demo EXE - Returns a random integer.exe
- Demo EXE - Returns number of files in folder (parameter).exe
- Demo EXE - Returns user of process.exe
- Demo Powershell Script - Available MB via WMI.ps1
- Demo Powershell Script - InterruptsPerSec via WMI.ps1
- Demo Powershell Script - Powershell Version.ps1
- Demo Powershell Script - Returns a fixed integer value.ps1
- Demo Powershell Script - Returns a random integer value.ps1
- Demo Powershell Script - Returns Random Integer and Warnings.ps1
- Demo VBScript - InterruptsPerSec via WMI.vbs
- Demo VBScript - Multiplies two integers(2 parameters).vbs
- Demo VBScript - Returns a fixed float value.vbs
- Demo VBScript - Returns a fixed integer value.vbs
- Demo VBScript - Returns a random value.vbs
- Demo VBScript - Returns number of svchost processes.vbs
- Demo VBScript - Returns user of process.vbs
- Demo VBScript - Returns warning depending on number of svchost processes.vbs
- Demo VBScript - Timezone via WMI.vbs
- Demo VBScript - UTCTime via WMI.vbs
- Load_Test_CPU_1_Mio_Primes.exe
- Load_Test_CPU_10_Mio_Primes.exe
- Load_Test_Disk_Write_Read_1000_files.exe
- Load_Test_Disk_Write_Read_10000_files.exe
- Load_Test_Memory_Allocate_And_Free_400MB.exe

To create a new sensor based on one of these files, create a new **EXE/Script Sensor** 747 and choose the respective file from the **EXE/Script** list in the sensor settings.

Custom Sensors Included in PRTG—Folder: \Custom Sensors\EXEXML

- Demo Batchfile - Returns static values in four channels.bat

To create a new sensor based on one of these files, create a new **EXE/Script Advanced Sensor** 759 and choose the respective file from the **EXE/Script** list in the sensor settings.

Custom Sensors Included in PRTG—Folder: \Custom Sensors\python

- sensor_example.py

This Python example script just returns fixed values in two channels to demonstrate the usage. To create a new sensor based on this file, create a new **Python Script Advanced Sensor** 1385 and choose the file from the **Python Script** list in the sensor settings.

SQL Query Files Included in PRTG—Folder: \Custom Sensors\sql\<dbms>

- Demo Serveruptime.sql

You can find this demo SQL query script in each subfolder for each supported database management system (dbms): **\mssql**, **\mysql**, **\oracle**, **\postgresql**

To create a new sensor that uses one of the scripts in the dbms folders, create the according sensor type (see above for supported sensors 2778) and choose the respective file from the **SQL Query File** list in the sensor settings.

Custom Sensors Included in PRTG—Folder: \Custom Sensors\WMI WQL scripts

- Demo WQL Script - Get Win32LogicalDiscFreeMB.wql
- Demo WQL Script - Get Win32OsBuildnumber.wql
- Demo WQL Script - Get Win32PercentProcessorIdleTime.wql
- Demo WQL Script - Get Win32PercentProcessorTime.wql

To create a new sensor based on one of these files, create a new **WMI Custom Sensor** 2512 and choose the respective file from the **WQL File** list in the sensor settings.

Downloading Pre-Built Custom Sensors

Good resources to find custom sensors that PRTG users and we from Paessler share are the **PRTG Script World** and our Knowledge Base. In the Knowledge Base, search for the tag **custom-script-exe** to find a lot of custom sensors: https://kb.paessler.com/en/tags/custom-script-exe/

More

You can find useful scripts for sensors in the **PRTG Script World**:

- https://www.paessler.com/script-world

For the other sensor types that work out-of-the-box, please see

- **List of Available Sensor Types** 385

Knowledge Base: Guide for PowerShell Based Custom Sensors

- https://kb.paessler.com/en/topic/71356

Knowledge Base: Custom sensors

- https://kb.paessler.com/en/tags/custom-script-exe/

Knowledge Base: How can I share my self-written PRTG script/program with other PRTG users?

- https://kb.paessler.com/en/topic/63737

Knowledge Base: How can I test if parameters are correctly transmitted to my script when using an EXE/Script sensor?

- https://kb.paessler.com/en/topic/11283

Sensor Settings Overview

For information about sensor settings, please see the following sections:

- **Sensor Settings—384 List of Available Sensor Types 385**
- **Additional Sensor Types (Custom Sensors) 2778**
- **Sensor Channels Settings 2782**
- **Sensor Notifications Settings 2791**

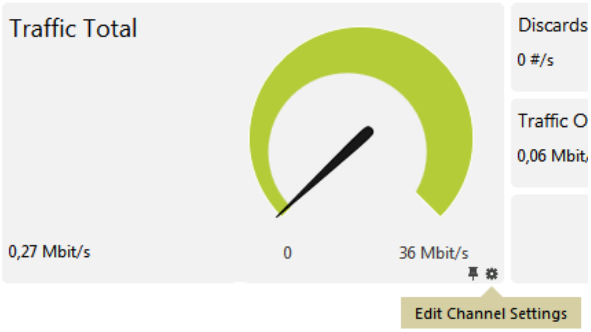
7.10 Sensor Channels Settings

A sensor has one or more channels in which it handles the actual monitoring data. In the channel settings, you can define how to display the data from the sensor's different channels displayed in graphs, gauges, and tables. Additionally, the channel data can determine the sensor status [163]. Use the limit settings to achieve this.

On the sensor's **Overview** tab, click the gear icon of a specific channel gauge to change its settings. Click the pin symbol on the left of the gear icon in a gauge to make this channel the primary channel of the selected sensor.

You can also open the settings of a channel by clicking the respective gear icon in the channels data table.

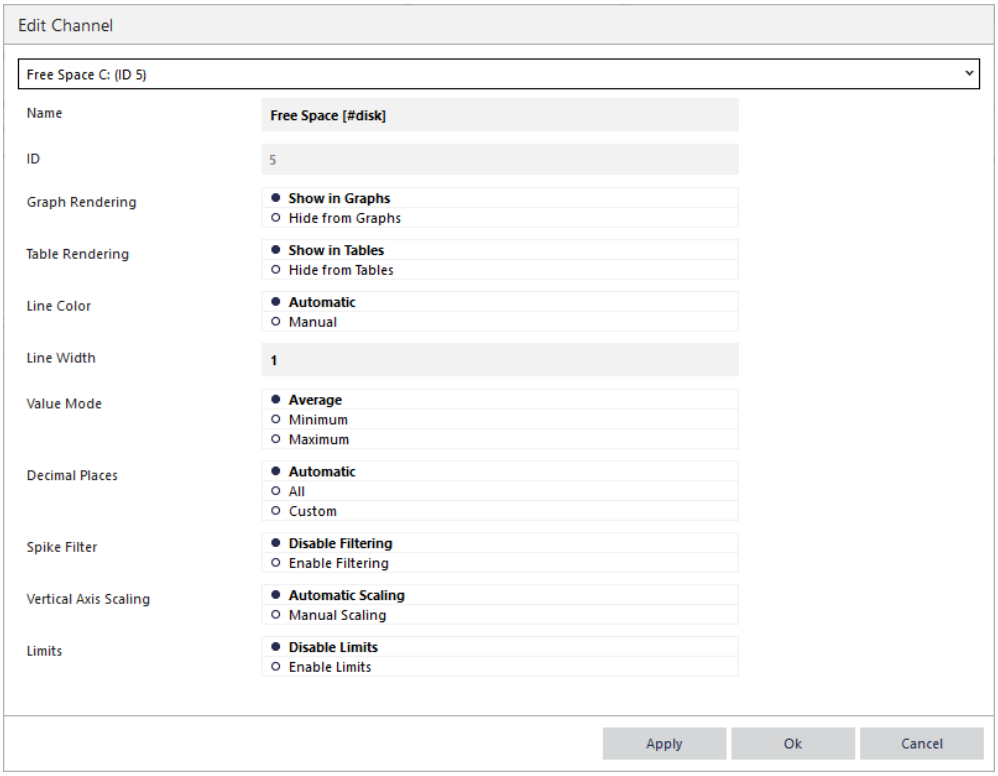
For lookup [3183] channels, we recommend that you stay below 120 lookup values to get expressive gauges. For non-primary lookup channels, the upper limit is around 40 lookup values.



The Gear Icon of an SNMP Traffic Total Channel to Open Channel Settings

The available options are nearly the same for all sensor types. An exception applies to the **Downtime** channel, which is automatically calculated and does not offer all settings. Channels with "absolute" values additionally have an option for defining the **Value Mode**.

You can quickly choose another channel of the selected sensor via the dropdown list at the top of the channel settings dialog.



Channel Settings for a Disk Sensor

Available Channel Settings

EDIT CHANNEL

Name	Enter a meaningful name to identify the channel (not editable for script sensors after sensor creation). The name will appear in graphs and tables. You can automatically add the sensor's ID to the name by using the placeholder **[#id]**.
Unit	This field is only visible for custom sensors. Enter a string that describes the unit of the returned values. This is for display purposes only. Please enter a string.
Scaling Multiplication	This field is only visible for channels with a custom unit. If you want to multiply the received raw data by a certain value, enter the multiplier here. Please enter an integer value. Otherwise, use the default value 1 to not change the received value. ⓘ The following sensor types provide the scaling factor for received values with custom units in their sensor settings.

EDIT CHANNEL

	▪ Sensor Factory Sensor 1440 (you can use multiplication and division in the channel definition) ▪ SNMP APC Hardware Sensor 1532 ▪ SNMP Custom Sensor 1650 ▪ SNMP Dell Hardware Sensor 1731 ▪ SNMP Library Sensor 1916 ▪ WMI Custom Sensor 2514
Scaling Division	This field is only visible for channels with a custom unit. If you want to divide the received raw data by a certain value, enter the divisor here. Please enter an integer value. Otherwise, use the default value 1 to not change the received value. The following sensor types provide the scaling factor for received values with custom units in their sensor settings. ▪ Sensor Factory Sensor 1440 (you can use multiplication and division in the channel definition) ▪ SNMP APC Hardware Sensor 1532 ▪ SNMP Custom Sensor 1650 ▪ SNMP Dell Hardware Sensor 1731 ▪ SNMP Library Sensor 1916 ▪ WMI Custom Sensor 2514
Value Lookup	This field is only visible for custom sensors. Select the lookup 3183 file that you want to use with this channel. Do not use this option for sensors that provide the unit **Value Lookup** in the sensor settings! This channel setting will be overwritten with the next sensor scan. Please define the lookup file that you want to use with this channel on the **Settings** tab of this sensor. Choose the option **Value Lookup** for the setting **Sensor Channel** #x **Unit** (where x is the number of the channel) and choose the desired lookup file under **Sensor Channel** #x **Value Lookup**. See also manual section Define Lookups—Requirement: Channel Unit "Custom" 3183 for affected sensor types.
ID	Shows the ID of the channel. You cannot change the ID. PRTG uses it for unique identification. For example, you need the ID when using Sensor Factory 1438 sensors.

EDIT CHANNEL

	There are a few special channel IDs that are fixed: ▪ -1 is for sum channels of traffic channels (for example, of the **SNMP Traffic Sensor** 2132). ▪ -4 is for the **Downtime** channel (you can use it, for example, for an uptime percentage calculation in a **Sensor Factory Sensor** 1438). ▪ -2 (coverage) and -3 (error) are used internally.
Graph Rendering	Define if you want to show this channel in data graphs 170. Choose between: ▪ **Show in Graphs**: Sensor graphs contain the data of this channel. ▪ **Hide from Graphs**: Sensor graphs do not contain data of this channel. If you choose to hide this channel in graphs, it will also not appear in a **Report** 2862 if you include this graph.
Table Rendering	Define if you want to show this channel in data tables 166. Choose between: ▪ **Show in Tables**: Sensor data tables contain the data of this channel. ▪ **Hide from Tables**: Sensor data tables do not contain the data of this channel. This option hides the channel gauge as well, but the channel will still be available in the data table of the sensor's **Overview** tab. If you choose to hide this channel in data tables, PRTG will also not use it for the calculation of the "sum" (total) channel of the sensor.
Line Color	Define the color of the channel display in graphs. Choose between: ▪ **Automatic**: PRTG sets the color of this channel in graphs automatically. ▪ **Manual**: Individually define the color of this channel. You can enter the desired color code below.
Color (#rrggbb)	This option is only available if you choose manual line color above. Enter a color in hexadecimal RGB notation (as in HTML/CSS), or choose a color from the visual color selector. The field with the hexadecimal color value will change to the selected color automatically.

EDIT CHANNEL

Line Width	Define the width of the channel line in graphs. Enter an integer value in pixels. The maximum line width is 25px, but we recommend that you use values between 1 and 7 only to get optimal results.
Data	This setting is available for most channels. Define how to display data. Choose between: ▪ **Display actual values in** [unit]: Display the values in the unit shown. ▪ **Display in percent of maximum**: Calculate and show percent values based on a maximum value. Provide a maximum below. ⓘ If you choose this option, you cannot display the data of traffic sensors as a positive and negative area graph.
Maximum ([unit])	This field is only visible if you choose the percent of maximum setting above. Enter a value to use as maximum. Please pay attention to the given unit. PRTG calculates all percent values based on this value. Please enter an integer value.
Value Mode	This setting is only available for sensor channels that return absolute values. It is not available for sensors showing difference values, such as traffic channels. Depending on this setting, the channel cannot only show averages, but also minimum or maximum values in the graphs for the respective time spans. Choose between: ▪ **Average**: The channel shows average values. ▪ **Minimum**: The channel shows minimum values. ▪ **Maximum**: The channel shows maximum values. See this Knowledge Base article for more information about the value modes: What is the Value Mode in channel settings?
Decimal Places	Define how many decimal places of the channel's data to display in graphs and tables. Choose between: ▪ **Automatic**: PRTG automatically defines how many decimal places are used for optimal viewing results. ⓘ Values between 10 and -10 are rounded to two decimal places. Values that are very close to an integer are rounded to the integer (for example, 3.001 is rounded to 3). ▪ **All**: Display all available decimal places. ▪ **Custom**: Manually define the number of decimal places. If you choose this option, an additional field will appear. Please enter an integer value.

EDIT CHANNEL

Spike Filter	You can use a spike filter to correct faulty monitoring data. Sometimes, sensors report enormously high or far too low values. This can be because of an error in data transmission, or because of incompatibilities of the physical device you are monitoring. This can make graphs unreadable. A spike filter can compensate for these flaws. If you enable a spike filter, values above and below a certain limit are disregarded in the monitoring data for graphs and tables. Choose between: ▪ **Disable Filtering**: Display all data as it is received. Do not filter out spikes. ▪ **Enable Filtering**: Enable a filter to remove spike values. Additional fields appear below. ⓘ This does not change monitoring data itself but only the presentation of the data. This setting is valid for all data of this channel, including historic data. ⓘ The spike filter option is not available for the channel **Downtime**.
Spike Filter Max. Value [unit]	This field is only visible if you enable the spike filter above. Enter the maximum value to show in the channel data. PRTG disregards all data above this value in graphs and tables. Please enter an integer value or leave the field empty.
Spike Filter Min. Value [unit]	This field is only visible if you enable the spike filter above. Enter the minimum value to show in the channel data. PRTG disregards all data below this value in graphs and tables. Please enter an integer value or leave the field empty.
Vertical Axis Scaling	Define how to display the vertical axis for the channel in graphs. Choose between: ▪ **Automatic Scaling**: PRTG automatically uses the optimum scaling. Usually the scaling ranges from the minimum to the maximum value. PRTG uses one single scale for each unit label only. ▪ **Manual Scaling**: Define the scaling manually. Additional fields appear below. Defining manual axis scaling can make low values better visible in your graph, but it may result in a graph with multiple vertical axes for the same unit label. ⓘ Settings for this option are ignored if you enable the Chart Type **Stack channels on top of each other** or **Show in and out traffic as positive and negative area chart** (available for traffic sensors) on the sensor's **Settings** tab.

EDIT CHANNEL

Vertical Axis Maximum [unit]	This field is only visible if you enable vertical axis scaling above. Enter the maximum value to use on the vertical axis for the channel. Please enter an integer value.
Vertical Axis Minimum [unit]	This field is only visible if you enable vertical axis scaling above. Enter the minimum value to use on the vertical axis for the channel. Please enter an integer value.
Limits	Define if you want to use thresholds for this channel. The channel can affect the status of the sensor 163 it is part of. With limits you can define when the sensor will show a **Warning** or **Down** status, depending on the channel data. For example, you can use this function to set a traffic sensor (which is usually never in a down state) to error when the monitored values reach critical limits. Choose between: ▪ **Disable Limits**: Do not use the channel data to control the sensor status. ▪ **Enable Limits**: Define limits. Additional fields appear below. The sensor of this channel will enter a **Warning** or **Down** status when limits are undercut or overrun. ⓘ The limits option is not available for the channel **Downtime**. ⓘ If a channel uses lookups 3183, we strongly recommend that you control the sensor status only via the lookup definition. If you define limits in addition here, the sensor will use both the channel limits and the status as defined in the lookup file. In this case, channel limits will determine the overall status of the sensor and overwrite the sensor message while the channel gauge still shows the status as defined in the lookups. ⓘ You can show limits in graphs (highlighted in yellow or red) if you select exactly one channel with a limit in a graph.
Upper Error Limit [unit]	This field is only visible if you enable limits above. Specify an upper limit for a **Down** status. If the channel values overrun this value, the sensor will be **Down**. Please enter an integer value or leave the field empty. ⓘ While a sensor shows a **Down** 163 status triggered by a limit, it will still receive data in its channels.
Upper Warning Limit [unit]	This field is only visible if you enable limits above. Specify an upper limit for a **Warning** status. If the channel values overrun this value, the sensor will be **Warning**. Please enter an integer value or leave the field empty.

EDIT CHANNEL

Lower Warning Limit [unit]	This field is only visible if you enable limits above. Specify a lower limit for a **Warning** status. If the channel values undercut this value, the sensor will be **Warning**. Please enter an integer value or leave the field empty.
Lower Error Limit [unit]	This field is only visible if you enable limits above. Specify a lower limit for a **Down** status. If the channel values undercut this value, the sensor will be **Down**. Please enter an integer value or leave the field empty. While a sensor shows a **Down** 163 status triggered by a limit, it will still receive data in its channels.
Error Limit Message	This field is only visible if you enable limits above. Enter an additional message. It will be added to the sensor message when showing a **Down** status. Please enter a string or leave the field empty.
Warning Limit Message	This field is only visible if you enable limits above. Enter an additional message. It will be added to the sensor message when showing a **Warning** status. Please enter a string or leave the field empty.

Click **Ok** to save your settings and to close the settings window. Click **Apply** to save the changed settings while the **Edit Channel** window remains open. This functionality is useful if you want to change the settings of other channels of the current sensor as well. You can select another channel via the dropdown menu above the settings. You can close the settings window without saving by clicking **Cancel**.

If you have changed any settings and click **Cancel** or choose another channel via the dropdown menu without applying the changes, PRTG will ask you to confirm this step. **Discard Changes** will ignore any edits and closes the window or shows the settings of another selected channel. Click **Save** to apply your changes.

More

Knowledge Base: What is the Value Mode in channel settings?

- https://kb.paessler.com/en/topic/60238

Sensor Settings Overview

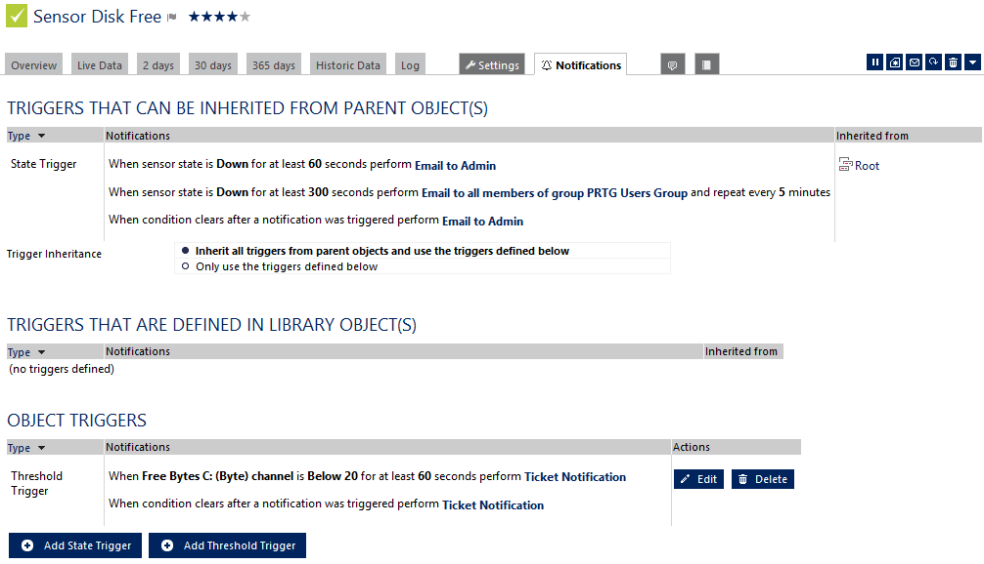
For information about sensor settings, please see the following sections:

- **Sensor Settings**— 384 **List of Available Sensor Types** 385
- **Additional Sensor Types (Custom Sensors)** 2778
- **Sensor Channels Settings** 2782

- Sensor Notifications Settings 2791

7.11 Sensor Notifications Settings

The status or the data of a sensor can trigger notifications. Using this mechanism, you can configure external alerting tailored to your needs.



Example of Notification Trigger Settings

Click here to enlarge: http://media.paessler.com/prtg-screenshots/notification_trigger.png

Although the sensors activate a trigger, you can set notification triggers higher in the hierarchy (for example for groups or devices). Because of this you can define triggers for multiple sensors using the inheritance mechanism 122. Monitoring objects with inherited triggers show these in section **Triggers That Can Be Inherited From Parent Object(s)** on the **Notifications** tab.

PRTG already includes a default notification trigger for the **Root Group** 118. This default trigger provokes the standard notification **Email and push notification to admin** if there is any sensor in down status 163 in your PRTG installation for at least 10 minutes.

You can also define notification triggers in **Libraries** 2845. Sensors that are in a library with defined triggers show these triggers in section **Triggers That Are Defined in Library Object (s)** on the **Notifications** tab.

Note

This section describes one of four steps to set up the notification system in PRTG. A complete notification setup involves:

1. Checking and setting up the **Notification Delivery** settings. This tells PRTG how and where to send messages.
   For detailed information, see **System Administration—Notification Delivery** 2961.

2. Checking and setting up **Notification Contacts** for the users of your PRTG installation. This defines where to send notifications.
   For detailed information, see **Account Settings—Notification Contacts** 2934.
3. Checking and setting up **Notifications**. This defines the kind of message and its content.
   For detailed information, see **Account Settings—Notifications** 2916.
4. Checking and setting up **Notification Triggers** for objects. This provokes the defined notifications.
   For detailed information, see **Sensor Notifications Settings** 2791.

We recommend that you always set up at least two notifications with different delivery methods for a notification trigger, for example, one email notification 2922 and one SMS notification 2924. If delivery via email fails (due to an email server failure or other reasons), PRTG can still notify you via your smartphone. Simply set your latency setting to a state trigger 2793 and a notification via a delivery method other than the one for the first trigger. Or set up a second trigger with another notification for the corresponding object.

For background information, please see the **Notifications** 2829 section.

Available Notification Triggers Settings

On an object's detail page, open the **Notifications** tab to change sensor notification triggers. The available options are the same for all objects. When defining triggers for probes, groups, or devices, they can be inherited down to sensor level.

TRIGGERS THAT CAN BE INHERITED FROM PARENT OBJECT(S)

You see a list of all notification triggers that are defined higher in the hierarchy. The list is empty and shows the message **(no triggers defined)** when you have not set any triggers in probes, groups, or devices above the current object in the **Object Hierarchy** 118. You can see the **Type** of trigger and the **Notifications** that the monitoring object executes once this trigger is activated.

Trigger Inheritance	Define if you want to use the triggers shown above on the current object. Choose between: ▪ **Inherit all triggers from parent objects and use the triggers defined below**: Use the triggers shown above. If the defined condition is met, the corresponding trigger is activated and the notification provoked. Click the notification name to open its settings page 2916. Click the name of the monitoring object in the column **Inherited from** to open its **Overview** tab. ▪ **Only use triggers defined below**: Do not use the triggers shown above. Only use the triggers that you define below in section **Object Triggers** for this object. This setting is valid for all triggers shown above. It is not possible to only select some of the triggers.

In section **Triggers that are defined in library object(s)** you see all notification triggers that are set for **Libraries** 2845 that contain the currently selected sensor.

TRIGGERS THAT ARE DEFINED IN LIBRARY OBJECT(S)

You see a list of all notification triggers that are defined in libraries that include the currently selected sensor. The list is empty and shows the message **(no triggers defined)** when you have not set any triggers in libraries that contain the current sensor. You can see the **Type** of trigger and the **Notifications** that the sensor executes once this trigger is activated.

Click the notification name to open its settings page 2916. Click a library name in the column **Inherited from** to view this library.

You cannot turn off trigger usage for the current sensor from a library here. If you do not want to use any notification triggers from a library for this sensor, open the library and remove this sensor from it or refine the triggers on the **Notifications** 2859 tab.

You can set up one or more of the following triggers, each with different setting options. Which trigger types are visible depends on the kind of object you edit:

- Add State Trigger 2793
- Add Speed Trigger 2795
- Add Volume Trigger 2797
- Add Threshold Trigger 2799
- Add Change Trigger 2800

You can create all notification triggers by forming sentences in "natural language". There are different options available for every type.

Add State Trigger

Define a trigger that is activated when a sensor changes its current status. This is the most common reason to send out notifications. Click the **Add State Trigger** button to add a new trigger, or click the **Edit** button next to an existing notification to change it. Define the settings as described below. Every trigger provokes one or more notification(s) 2916 to be executed.

STATE TRIGGER

When sensor state is [...]	Select the condition that will trigger the notification. The trigger will be activated when a sensor enters the selected status. Choose from the dropdown menu: ▪ **Down**: The trigger is activated if a sensor changes to a **Down** status.

STATE TRIGGER

	▪ **Warning**: The trigger is activated if a sensor changes to a **Warning** status. ▪ **Unusual**: The trigger is activated if a sensor changes to an **Unusual** status. ▪ **Partial Down**: The trigger is activated if a sensor changes to a **Down (Partial)** status (available in a cluster 116 configuration).
...for at least [...] seconds	Define how many seconds PRTG waits before it sends out a notification (latency). This can avoid false alarms if a sensor 'flickers' and, for example, changes to a down status for just a few seconds. If the selected condition (the sensor status) persists after the defined time in seconds, the notification is triggered. Please enter an integer value. Do not define a latency that is shorter than the scanning interval of a sensor that uses this trigger! The notification trigger might not work as expected in this case. .
...perform [...]	Select a notification that PRTG sends out if the selected condition (the sensor status) is true and the latency time defined has elapsed. Choose a notification from the dropdown menu. The menu shows all notifications defined in the Account Settings—Notifications 2916 settings. You can also choose **no notification** to only use other conditions for this trigger.
When sensor state is [...] for at least [...] seconds	Define an escalation latency in seconds. This "escalation" triggers a second notification if the number of seconds you enter here has passed since the sensor status has entered the defined condition. Use this to automatically escalate a notification in case a problem persists for a longer time. Please enter an integer value. PRTG automatically takes the status from the first trigger condition above.
...perform [...]	Select a (second) notification that PRTG sends out if the selected condition (the sensor status) is true and the escalation latency time defined has elapsed. Choose a notification from the dropdown menu. The menu shows all notifications defined in the Account Settings—Notifications 2916 settings. You can also choose **no notification** to only use other conditions for this trigger. Select a notification with another delivery method than above to ensure the delivery in case of technical issues with the first notification.

STATE TRIGGER

...and repeat every [...] minutes	Define an interval in minutes in which PRTG sends the escalation notification (defined above) repeatedly. The second (escalation) notification defined will be resent every x minutes that you enter here. Please enter an integer value. If you enter 0, PRTG will not send repeating escalation notifications.
When condition clears after a notification was triggered perform [...]	Select a notification that PRTG sends out if the selected condition (the sensor status) is not true anymore because the sensor status changed again. Choose a notification from the dropdown menu. The menu shows all notifications defined in the **Account Settings—Notifications** 2916 settings. You can also choose **no notification** to only use other conditions for this trigger. PRTG sends notifications about cleared conditions if the time for the trigger activation elapsed (defined in the first line) and you choose a notification here. If you select **no notification** above, you will get the notification about the cleared condition nevertheless if you define it here. The definition of an "escalation" notification does not influence notifications for cleared conditions.
Save	Click **Save** to confirm your settings.
Cancel	Click **Cancel** to undo your changes.

Add Speed Trigger

Define a trigger that is activated when the currently monitored speed in a sensor changes (for example, a traffic sensor). Click the **Add Speed Trigger** button to add a new trigger, or click the **Edit** button next to an existing notification to change it. Define the settings as described below. Every trigger provokes one or more notification(s) 2916 to be executed.

SPEED TRIGGER

When [...] **channel**	From the dropdown menu, select the channel whose data PRTG considers for speed comparison. Select **Primary** to generally use the primary channel of a sensor (you can define this in the sensor settings 384), or choose a specific channel name from the list (there are different channels for every sensor type). All following settings for this trigger are based on the chosen channel.
...is [...]	Select the condition that will trigger the notification. Choose from the dropdown menu:

SPEED TRIGGER

	▪ **Above**: The trigger is activated if the value of the selected channel exceeds a defined value. ▪ **Below**: The trigger is activated if the value of the selected channel falls below a defined value. ▪ **Equal to**: The trigger is activated if the value of the selected channel is the same as a defined value. ▪ **Not Equal to**: The trigger is activated if the value of the selected channel is different than a defined value.
[value]	Define the value to which PRTG compares the channel data. Please enter an integer value.
[scale]	From the dropdown menu, select the unit in which you entered the **[value]** above. **[scale]** and **[time]** together define the unit for the given value. If the channel data is shown in a different unit, PRTG will automatically convert values internally. Choose from: ▪ **bit** ▪ **kbit** ▪ **Mbit** ▪ **Gbit** ▪ **Tbit** ▪ **Byte** ▪ **KByte** ▪ **MByte** ▪ **GByte** ▪ **TByte**
[time]	Select the time for the scale (so you create a scale per time unit). Choose from the dropdown menu: ▪ **second** ▪ **minute** ▪ **hour** ▪ **day** **[scale]** and **[time]** together define the unit for the given value. If the channel data is shown in a different unit PRTG will automatically convert values internally.

SPEED TRIGGER

..for at least [...] seconds	Define how many seconds PRTG waits before it sends out a notification (latency). This can avoid false alarms if a channel reaches a limit for just a few moments. If the combined channel condition of **[value]**, **[scale]**, and **[time]** persists after the defined time span, the notification will be triggered. Please enter an integer value. Do not define a latency that is shorter than the scanning interval of a sensor that uses this trigger! The notification trigger might not work as expected in this case.
...perform [...]	Select a notification that is triggered if the combined channel condition of **[value]**, **[scale]**, and **[time]** is true and the latency time defined has elapsed. Choose a notification from the dropdown menu. The menu shows all notifications defined in the **Account Settings—Notifications** 2916 settings. You can also choose **no notification** to only use other conditions for this trigger.
When condition clears perform [...]	Select a notification that is triggered if the combined channel condition of **[value]**, **[scale]**, and **[time]** is not true anymore because the channel value has changed again. Choose a notification from the dropdown menu. The menu shows all notifications defined in the **Account Settings—Notifications** 2916 settings. You can also choose **no notification** to only use other conditions for this trigger. PRTG sends notifications about cleared conditions if the time for the trigger activation elapsed (defined in the first line) and you choose a notification here. If you select **no notification** above, you will get the notification about the cleared condition nevertheless if you define it here.
Save	Click **Save** to confirm your settings.
Cancel	Click **Cancel** to undo your changes.

No escalation notification and no repeat are available for this trigger type.

Add Volume Trigger

Define a trigger that is activated when a sensor (for example, a traffic sensor) reaches a certain volume limit in a specified time. Click the **Add Volume Trigger** button to add a new trigger, or click the **Edit** button next to an existing notification to change it. Define the settings as described below. Every trigger provokes one or more notification(s) 2916 to be executed.

VOLUME TRIGGER

When [...] **channel**	From the dropdown menu, select the channel whose data PRTG considers for this comparison. Select **Primary** to generally use the primary channel of a sensor (you can define this in the sensor settings 384), or choose a specific channel name from the list (there are different channels for every sensor type). All following settings for this trigger are based on the chosen channel.
...has reached [value]	Define the value to which PRTG compares the channel data. If the channel data exceeds this value, a notification is triggered. Please enter an integer value.
[scale]	From the dropdown menu, select the unit in which you entered the **[value]** above. **[scale]** and **[time]** together define the unit for the given value. If the channel data is shown in a different unit, PRTG will automatically convert values internally. Choose between: ▪ **Byte** ▪ **KByte** ▪ **MByte** ▪ **GByte** ▪ **TByte**
per [time]	Select the time for the scale (so you create a scale per time designation). Choose from the dropdown menu: ▪ **Hour** ▪ **Day** ▪ **Week** ▪ **Month** **[scale]** and **[time]** together define the unit for the given value. If the channel data is shown in a different unit, PRTG will automatically convert values internally.
...perform [...]	Select a notification that is triggered if the **[value]** in the combined unit of **[scale]** and **[time]** is exceeded. Choose a notification from the dropdown menu. The menu shows all notifications defined in the **Account Settings—Notifications** 2916 settings. You can also choose **no notification** to only use other conditions for this trigger.
Save	Click **Save** to confirm your settings.
Cancel	Click **Cancel** to undo your changes.

No escalation notification, no repeat, and no notification when condition clears are available for this trigger type.

Add Threshold Trigger

Define a trigger that is activated when a sensor reaches specific values. Click the **Add Threshold Trigger** button to add a new trigger, or click the **Edit** button next to an existing notification to change it. Define the settings as described below. Every trigger provokes one or more notification(s) 2916 to be executed.

THRESHOLD TRIGGER

When [...] **channel**	From the dropdown menu, select the channel whose data PRTG considers for this comparison. Select **Primary** to generally use the primary channel of a sensor (you can define this in the sensor settings 384), or choose a specific channel name from the list (there are different channels for every sensor type). All following settings for this trigger are based on the chosen channel.
...is [...]	Select the condition that will trigger the notification. Choose from the dropdown menu: ▪ **Above**: The trigger is activated if the value of the selected channel exceeds a defined value. ▪ **Below**: The trigger is activated if the value of the selected channel falls below a defined value. ▪ **Equal to**: The trigger is activated if the value of the selected channel is the same as a defined value. ▪ **Not Equal to**: The trigger is activated if the value of the selected channel is different than a defined value.
[value]	Define the value PRTG will compare the channel data to. Enter values in the smallest possible (base) unit, for example, in bytes, milliseconds, or percent. Please enter an integer value.
..for at least [...] seconds	Define how many seconds PRTG waits before it sends out a notification (latency). This can avoid false alarms in case a channel reaches a limit for just a few moments. If the defined channel condition persists after the defined time span, the notification is triggered. Please enter an integer value. Do not define a latency that is shorter than the scanning interval of a sensor that uses this trigger! The notification trigger might not work as expected in this case.

...perform [...]	Select a notification that is triggered if the defined channel condition is true and the latency time defined has elapsed. Choose a notification from the dropdown menu. The menu shows all notifications defined in the Account Settings—Notifications 2916 settings. You can also choose **no notification** to only use other conditions for this trigger.
When condition clears perform [...]	Select a notification that is triggered if the defined channel condition is not true any more because the channel value has changed again. Choose a notification from the dropdown menu. The menu shows all notifications defined in the Account Settings—Notifications 2916 settings. You can also choose **no notification** to only use other conditions for this trigger. PRTG sends notifications about cleared conditions if the time for the trigger activation elapsed (defined in the first line) and you choose a notification here. If you select **no notification** above, you will get the notification about the cleared condition nevertheless if you define it here.
Save	Click **Save** button to confirm your settings.
Cancel	Click **Cancel** to undo your changes.

No escalation notification and no repeat are available for this trigger type.

Add Change Trigger

Define a trigger that is activated by an 'on change' trigger. Some sensors offer the option to send such a trigger whenever sensor values have changed. Click the **Add Change Trigger** button to add a new trigger, or click the **Edit** button next to an existing notification to change it. Then define settings as described below. Every trigger will provoke one or more notification (s) 2916 to be executed.

CHANGE TRIGGER

When sensor changes perform [...]	Select a notification that is triggered whenever a compatible sensor sends a 'change notification'. You can enable this option in the settings 384 of some sensors. The notification trigger is activated immediately whenever a sensor sends an 'on change' trigger. Choose a notification from the dropdown menu. The menu shows all notifications defined in the Account Settings—Notifications 2916 settings.

There are no other options available for this trigger type.

Sensor Settings Overview

For information about sensor settings, please see the following sections:

- Sensor Settings—384 List of Available Sensor Types 385
- Additional Sensor Types (Custom Sensors) 2778
- Sensor Channels Settings 2782
- Sensor Notifications Settings 2791

Object Settings Overview

For more general information about object settings, please see section Object Settings 188.

Part 8

Ajax Web Interface—Advanced Procedures

8 Ajax Web Interface—Advanced Procedures

The Ajax-based web interface is your access to PRTG. Use it to configure devices and sensors, to set up notifications, as well as to review monitoring results, and to create reports. This web interface is highly interactive and uses Asynchronous Java Script and XML (AJAX) to deliver a powerful and easy-to-use user experience. While you are logged in 138, the PRTG web interface continuously refreshes the data on the screen (via Ajax calls) so it always shows the current monitoring results (you can set 2975 refresh interval and method individually).

Because the web interface works as a Single Page Application (SPA), you rarely see a full page refresh to avoid a performance impact due to redundant processing. Only single page elements are refreshed when necessary. The AJAX web interface shows all object setting dialogs as pop-up layers, so you never lose the current context. This speeds up the user experience appreciably and makes the configuration of objects in PRTG comprehensible. The responsive design of the web interface ensures that it always adjusts to the size of your screen so that you see more information at a glance.

The following sections introduce more advanced procedures in the Ajax Graphical User Interface (GUI).

Ajax Web Interface—Advanced Procedures—Topics

- Toplists 2806
- Arrange Objects 2811
- Clone Object 2812
- Multi-Edit 2814
- Create Device Template 2818
- Show Dependencies 2822
- Geo Maps 2824
- Notifications 2829
- Libraries 2845
- Reports 2862
- Maps 2885
- Setup 2907

Other Ajax Web Interface Sections

- Ajax Web Interface—Basic Procedures 136
- Ajax Web Interface—Device and Sensor Setup 248

Related Topics

- Enterprise Console 3028

- PRTG Apps for Mobile Network Monitoring 3082

8.1 Toplists

Packet Sniffer and xFlow (NetFlow, jFlow, sFlow, IPFIX) sensor types can not only measure the total bandwidth usage, they can also break down the traffic by IP address, port, protocol, and other parameters. The results are shown in so-called **Toplists**. This way PRTG is able to tell which IP address, connection, or protocol uses the most bandwidth.

PRTG looks at all network packets (or streams) and collects the bandwidth information for all IPs, ports, and protocols. At the end of the toplist period, PRTG only stores the top entries of each list in its database.

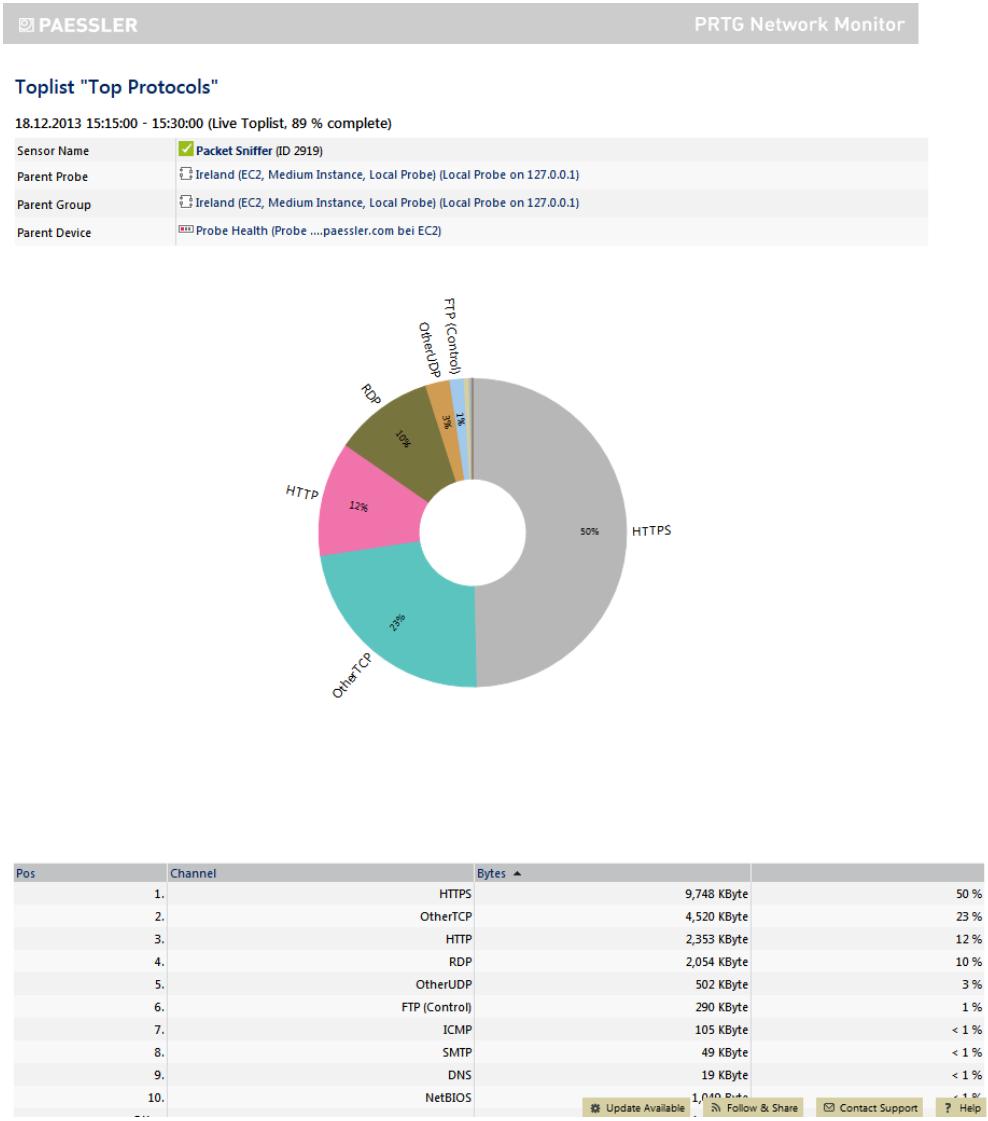
Only Top Entries are Stored

Storing all available analysis data in a database during the analysis process would create a huge amount of data, which would be very slow to transfer between probe and core and also retrieving data would be too slow. By storing only the top 100 entries for short periods of time it is possible to reduce the amount of data to a minimum while still being able to identify devices with huge bandwidth usage.

Toplists Overview

Toplists are available for xFlow, IPFIX, and Packet Sniffer sensors 386 only. Toplist graphs are displayed right on the sensor overview page. By default, there are three different toplists predefined for each sensor:

- **Top Connections**: Shows bandwidth usage by connection.
- **Top Protocols**: Shows bandwidth usage by protocol.
- **Top Talkers**: Shows bandwidth usage by IP address.



Toplist Top Protocols for a Packet Sniffer Sensor

- Click one of these items to view a distribution chart and a list of source and destination IP and port, protocols, kind of traffic in different channels, for example. What kind of information is available depends on the list selected.
- Click an entry in the Toplist periods list on the left side to view data for a certain time span. By default, a time span of 15 minutes is set. You can also manually define start and end time of the Toplist period you want to view. Use the date time picker to enter the date and time. Additionally, several table list options [207] are available.
- To print a Toplist, click the **Print This Toplist** button to view a printer-friendly version. Use the print option of your browser to send it to your printer.
- With **Sensor Overview** you can return to the current sensor's **Overview** tab. For a quick selection of other Toplists of the current sensor, click one of the Toplist icons at the top of the page.
- You can add or delete new Toplists, or edit existing ones on the sensor's **Overview** tab,

Add

Click the **Add Toplist** tile in the sensor overview to create a new Toplist. The available options are the same as for editing 2808 a list.

Edit

Click the small gear icon of a Toplist tile in the sensor overview to modify it.

TOPLIST

Name	Enter a meaningful name to identify the toplist.
Type	▪ **Top Talkers (Which IPs use the most bandwidth?)**: Shows bandwidth usage by IP address. ▪ **Top Connections (Which connections use most bandwidth?)**: Shows bandwidth usage by connection. ▪ **Top Protocols (Which protocols use the most bandwidth?)**: Shows bandwidth usage by protocol. ▪ **Custom (Create your own Toplist)**: Create your own list by selecting criteria below.
Toplist Fields	This setting is only available if you select a custom type above. Select the fields you want to add to the Toplist by adding a check mark in front of the respective field name. The available options depend on the type of sensor used. They are different for Packet Sniffer, NetFlow v5, v9 (and IPFIX), and sFlow. ⓘ For performance reasons, only select the fields you really want to monitor. Please see **Performance Considerations** 2810 section below.
Period (Minutes)	Define the interval for the Toplist in minutes. Please enter an integer value. Toplists always cover a certain time span. Once a time span has passed, the top results are stored and a new Toplist is started. ⓘ To avoid load problems on your probe system, please do not set this interval too long. Default setting is **15** minutes. Please see **Performance Considerations** 2810 section below.
Top Count	Define the length of your Toplist. Only this number of entries will be stored for each period. Please enter an integer value. ⓘ To avoid load problems on your probe system, please set this value as low as possible. Default setting is **100** to store the top 100 entries for each period. Please see **Performance Considerations** 2810 section below.

TOPLIST	
Reverse DNS	Define if you want to do a reverse Domain Name Service (DNS) lookup for IP addresses stored in the Toplist. Choose between: ▪ **Do a reverse DNS lookup for IPs**: Determine the domain name associated with an IP address and show it in the Toplist. ▪ **Do no reverse DNS lookup (faster)**: Show IP addresses only. Choose this option to increase performance.
Probe/Core Data Transfer	Define how the probe sends the Toplist data set to the core server. Choose between: ▪ **According to sensor interval (default)**: Send data in the interval defined in the settings of the sensor for which you create this Toplist. This can create a lot of bandwidth and CPU load with many sniffer sensors, complex traffic, or long Toplists. ▪ **Wait until Toplist period ends (less CPU and bandwidth usage)**: Send data once a Toplist period has finished. This will create less bandwidth usage and CPU load, but you cannot see the current Toplist in the web interface, only Toplists with finished periods. For more information, please see **Performance Considerations** 2810 section below.
Memory Limit (MB)	Define the maximal amount of memory in MB that the probe will use for collecting the different connection information. Every Toplist adds its amount to the probe's memory consumption. Increase this value if the number of captured connections is not sufficient. Please enter an integer value.

Click **Save** to save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Delete

Click the small trashcan icon of a Toplist tile in the sensor overview to delete it. Confirm with **Delete** to delete the list.

Details

Click on the windows symbol to show details of a Toplist.

Performance Considerations

If you create Toplists for data lines with considerable usage (for example, steady bandwidth over 10 Mbit/s) or if the traffic is very diverse (for example, many IPs or ports with only little traffic each) please consider the following aspects:

- The probe gathers all information needed for the Toplist in RAM memory during each period. Only the top 100 entries are transferred to the core. Depending on the Toplist type and traffic patterns, the required memory can grow into many megabytes.
- Choose periods that are as short as possible (especially important when traffic has a high level of diversity) to minimize memory usage.
- Memory requirements can grow almost exponentially with each field used in the Toplist definition (depending on traffic pattern). Avoid complex Toplists for high and diverse traffic. For example, **Top Connections** (5 fields) needs a lot more memory than **Top Talkers** (1 field).
- If you experience high bandwidth usage between core and probe, try to choose the **Wait until Toplist period ends** option in the Toplist settings 2808.
- If you experience Data incomplete, memory limit was exceeded messages, try to increase the memory limit in the Toplist settings but keep an eye on the memory usage of the probe process.
- To increase the performance of a Toplist, disable the reverse DNS lookup.

Notes

- When working with Toplists, be aware that privacy issues can come up for certain configurations of this feature. Using Toplists you can track all single connections of an individual PC to the outside world and you, as the administrator, must make sure it is legal for you to configure PRTG like this.
- Keep in mind that Toplists can be viewed through the web interface. You may not want to show lists of domains used in your network to others, so restrict access rights 129 to sensor types having Toplists.
- Note that diagrams, for example, for top connections are not meant to be used for detailed analysis. Rather they should indicate if there is an uncommon bigger change in this Toplist.

More

- **Monitoring Bandwidth via Flows** 3099
- **Monitoring Bandwidth via Packet Sniffing** 3097

8.2 Arrange Objects

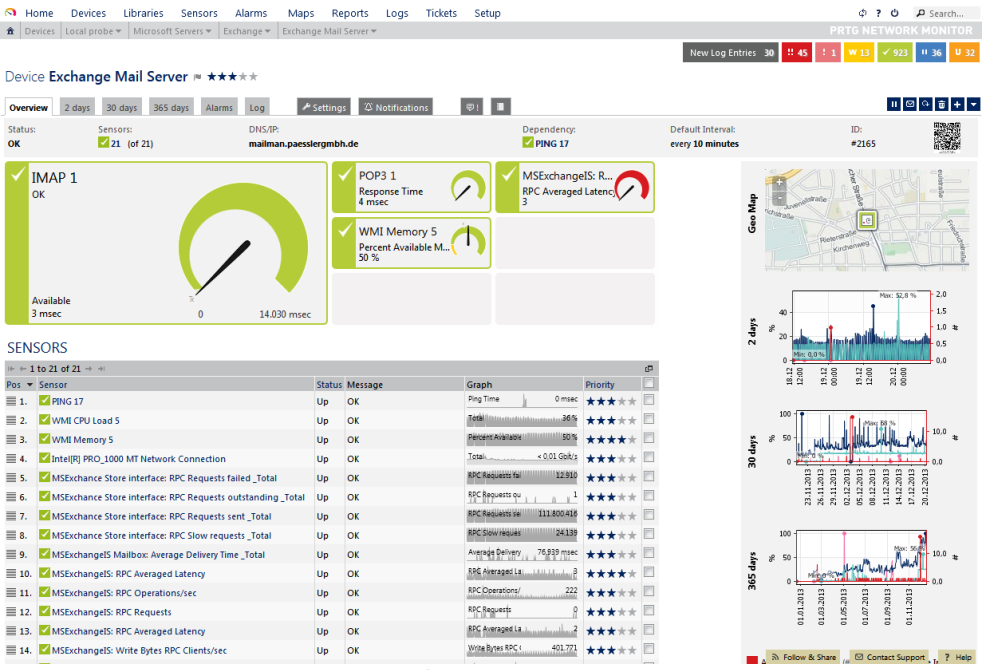
There are several options to move objects within the device tree, or to move objects from one probe or group to another.

Manage Tab in Device Tree

While viewing the device tree (or parts of it), click the **Management** tab to switch to a tree view where you can move monitoring objects using drag&drop in your browser window. For more information, see section Manage Device Tree 292.

Device Details View: Arrange Sensors

When you view the **Overview** tab of a device, you see a list of all sensors on this device.



Arrange Sensors on a Device

Click the column headers **Pos, Sensor, Status,** or **Priority** to re-sort the sensor list. To change a sensor's position, click the small grip at the beginning of the row, drag it to the position you like, and drop it. Changes take effect immediately.

Context Menu: Move

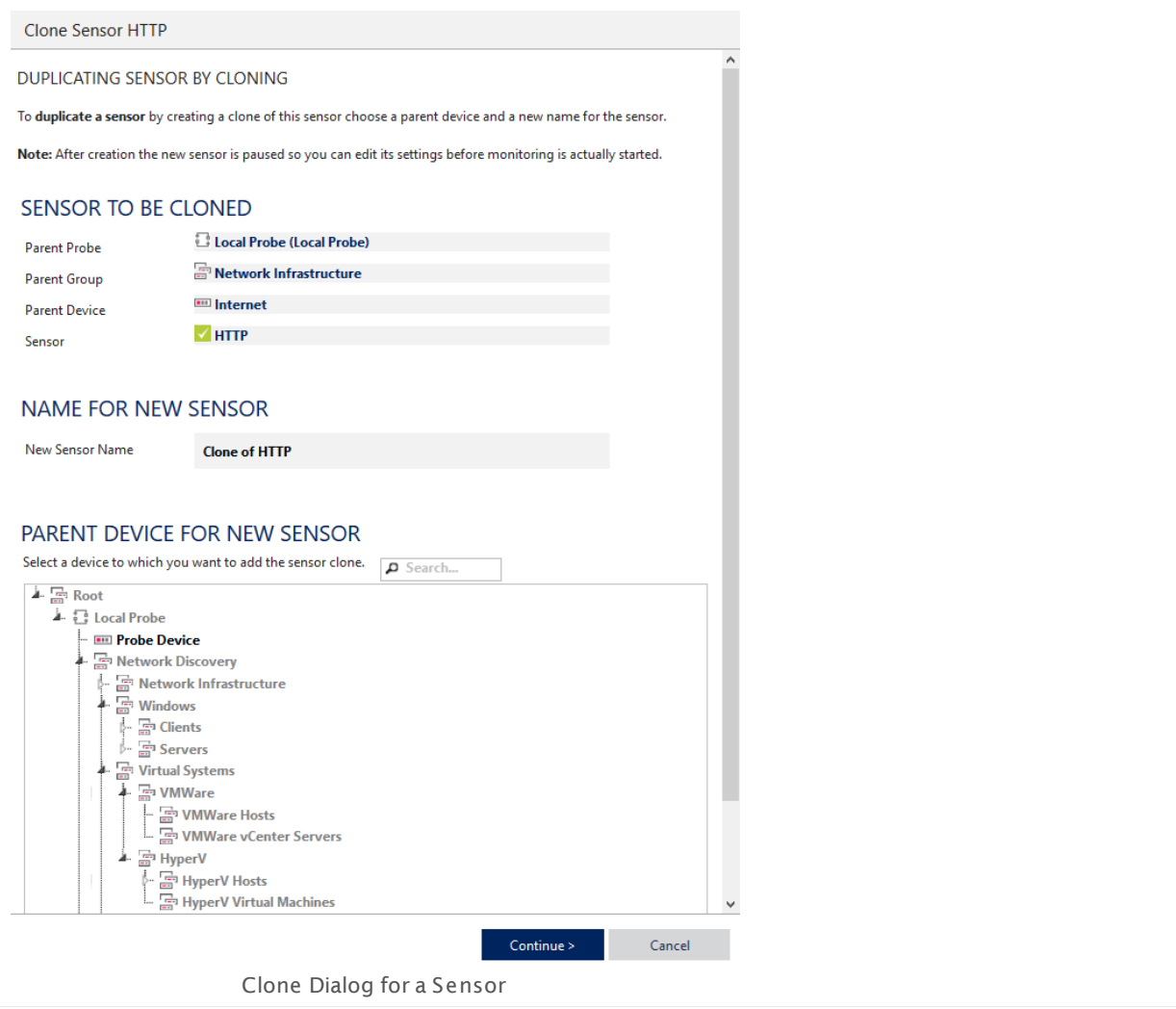
You can also right-click any object in the device tree to show the context menu 215. Select the **Move** entry to move sensors, devices, or groups up and down, or to move groups or devices into other groups or on other probes.

8.3 Clone Object

If you want to duplicate an object with the same settings, you can clone it. Cloning is available for groups, devices, and sensors. Unlike the results when using the **Create Device Template** 2818 option, a cloned device contains all objects of the original device, regardless of whether they bring about working sensors or not. This often depends on the settings of the cloned device.

The new object takes over all settings of the original object. This means, for example, that an **Auto-Discovery** 249 will start automatically on a cloned device (as soon as you resume it) if this option is set on the original device. This may result in sensors appearing twice. To prevent doubled sensors, set **Sensor Management** to **Manual (no auto-discovery)** in the device settings 362 before resuming the clone.

To start, right-click an object in your device tree, and from the context menu 215, select **Clone...** to open an assistant.



Clone Dialog for a Sensor

You cannot clone 'fixed' objects, such as the root group or a probe device.

If you want to clone a sensor, a faster way is to use the **Manage Device Tree** 292 function.

The user account 2975 that clones an object must have at least read access 129 to this object and all objects underneath in the hierarchy 118. The user group of this account must have the permission to create all sensor types 2983 which run on the device or group that is going to be cloned.

Clone Object Settings

OBJECT TO BE CLONED

Object	Several fields show information about the object that you are cloning. The available information varies depending on whether you clone a group, device, or sensor.

NAME OF NEW OBJECT

New Object Name	Enter a meaningful name for the new object to identify it later in, for example, the device tree or lists. By default, PRTG uses the old name with a preceding Clone of.
New IP Address/DNS Name	This field is only available when you clone a device. Enter the IP address or DNS name for the new device.

PARENT GROUP/DEVICE FOR NEW OBJECT

Use the object selector 210 to choose the object that you want to add the object clone to. If you clone a group or device, select a group. If you clone a sensor, select the device you want to add it to.

Click the **Continue** button to save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

The overview 166 page of the new object that you have cloned will open. By default, all sensors are initially paused 214 so you can change settings before monitoring starts. Please check the settings 188 and resume 214 monitoring.

Related Topics

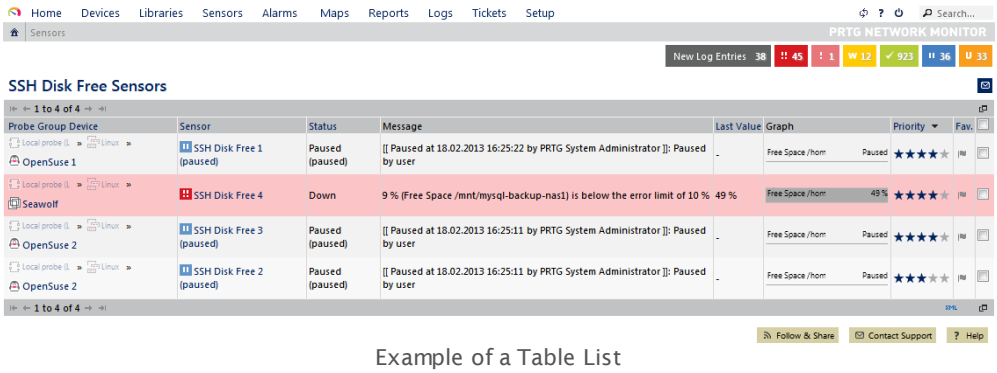
- **Create Device Template** 2818
- **Manage Device Tree** 292

8.4 Multi-Edit

Device and sensor table lists, as well as some other lists, offer multi-edit functionality. With this, you can bulk edit the properties of many objects at a time. Multi-edit is also available in the **Management** tab if you select multiple objects by holding down the Ctrl key (see Manage Device Tree 293).

You cannot change every setting type with multi-edit. PRTG only displays settings that all selected objects have in common.

You cannot multi-edit the standard user groups 2982 "PRTG Administrators" and "PRTG Users Group".

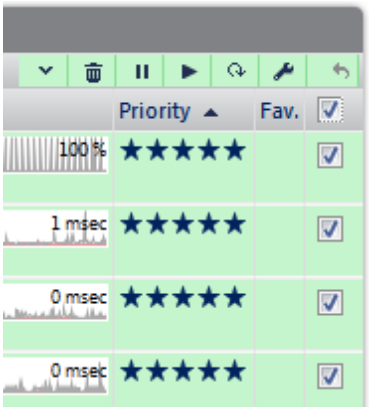


Example of a Table List

Start Multi-Edit in Lists

Start with viewing a table list. For example, choose **Sensors | By Type | ...** or **Devices | Device List | ...** from the main menu bar 231. Table lists are also available in the **Overview** tab of **Libraries** 2845, **Maps** 2885, **Reports** 2862, **Notifications** 2829, and **Schedules** 2938.

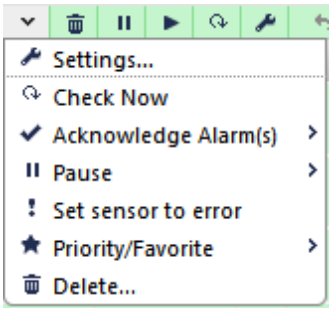
In a table list, start multi-edit by selecting objects using the check boxes on the right. You can also select all objects of the current page at once by clicking the check box in the table header. Use the **Item Count** option to view more items per page. As soon as you select one or more objects, the multi-edit menu appears at the top of the table. Chosen objects are shaded in green.



Multi Edit Menu

Depending on the object type, different functions are available. For example, for sensor lists, some frequently used functions are available as quick buttons, such as **Delete**, **Pause**, **Resume**, **Check Now**, and **Settings**. Click one of the buttons to apply the respective function to all selected objects.

Other options are available in the dropdown menu. Hover over the arrow symbol to show it.



Example of Multi Edit Drop Down Menu

The options in this menu vary depending on the kind of objects selected. Choose an entry to apply the according function to all selected objects.

Once you have selected the objects you want to change settings for, click the wrench symbol to enter the edit settings mode. For available settings, please see below.

Start Multi-Edit in Management Tab

In the device tree, start by clicking the **Management** tab.

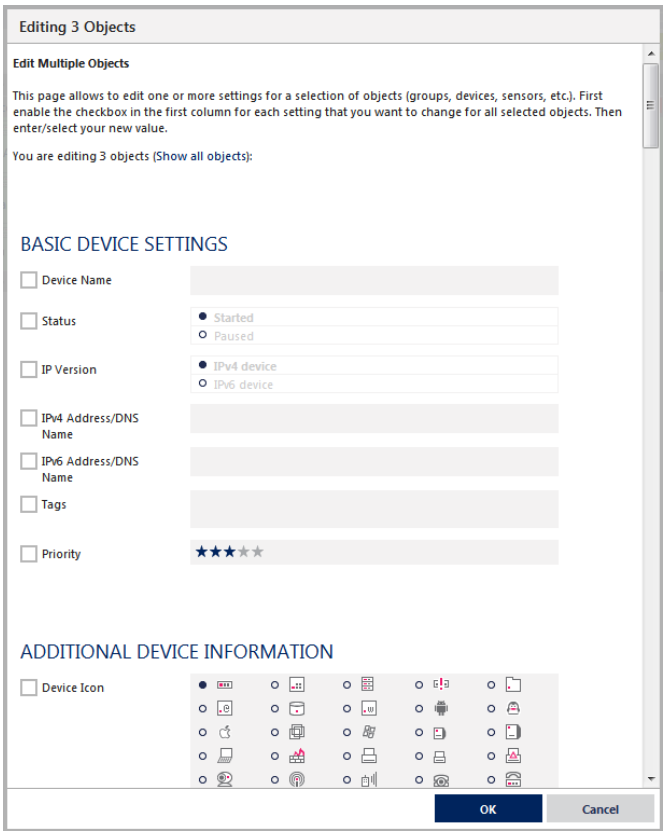
You can use Multi-Edit for object settings:

- Hold down the Ctrl key and select multiple groups, devices, or sensors (one of a kind).
- In the appearing dialog, select the settings you want to edit, change the according values, and click **Save**. The changes will be applied to all selected objects.

For available settings, please see below.

Edit Settings—Settings

The **Edit Multiple Objects** dialog box shows most of the settings that the selected sensors respective devices have in common. For example, you can edit the name, tags, priority, scanning interval, and access rights.



Example of Device Settings in Multi-Edit Mode

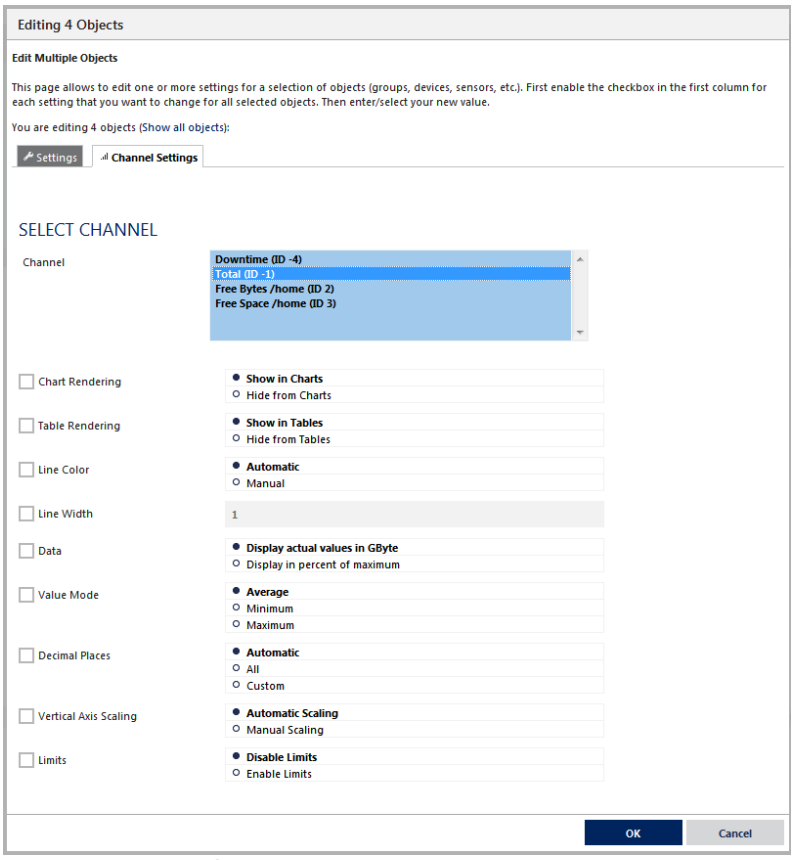
The available options depend on the selected objects and vary according to your selection. When editing multiple sensors, it may be useful to only choose one certain sensor type from the list, so that there are as many settings as possible available for multi-edit.

To change a property, add a check mark in front of the respective line and then change the settings. The new setting(s) will be applied to all objects you selected for multi-edit. All properties that are not activated with a check mark remain unchanged.

Click **OK** to store your settings. If you close the dialog box via the **X** or **Cancel** button, all changes to the settings will be lost!

Edit Settings—Channel Settings

The **Channel Settings** tab in the **Edit Multiple Objects** dialog box is only available when editing sensors. You can edit settings of all channels that the selected sensors have in common. Select a channel name from the **Channel** list. You can then edit display settings, colors, scaling, and limits, for example.



Example of Sensor Channel Settings in Multi-Edit Mode

The available options depend on the selected sensors and vary according to your selection. It may be useful to only choose one certain sensor type from the list, so that there are as many channel settings as possible available for multi-edit.

To change a property, add a check mark in front of the respective line and then change the channel settings. The new setting(s) will be applied to all sensors you selected for multi-edit. All properties that are not activated with a check mark remain unchanged.

Click **OK** to store your settings. If you close the dialog box via the **X** or **Cancel** button, all changes to the settings will be lost!

Related Topics

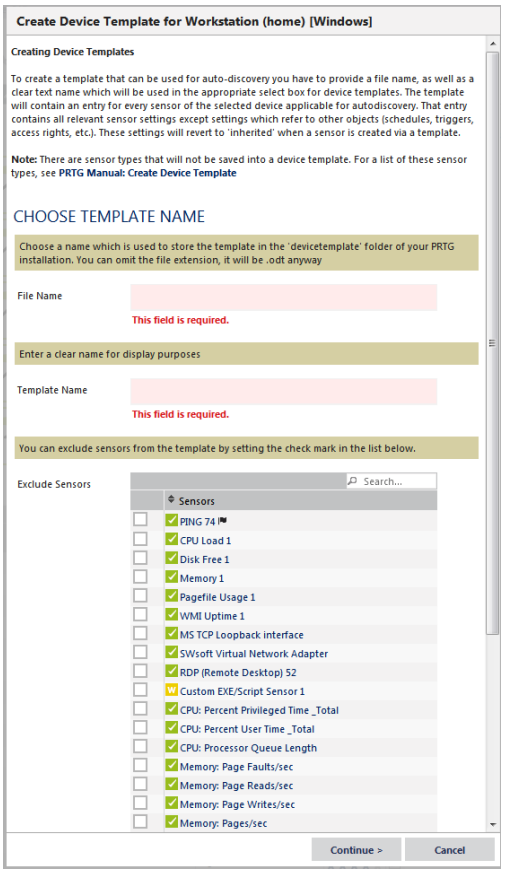
- Working with Table Lists 207
- Manage Device Tree 292

8.5 Create Device Template

If you want to add a certain device several times, you can create a device template from an existing device in your device tree. When creating a device template, PRTG will save information for nearly all sensors on this device to a template file that you can later use in combination with **Auto-Discovery** 249 (restrictions 2820 apply for a few sensor types).

From the sensors, all relevant settings are saved, except settings that refer to other objects, such as schedules 127, notification triggers 2829, and access rights 129. PRTG will automatically revert them to **Inherit**.

To start, right-click a device in your device tree. From the context menu 215, select **Create Device Template...**. An assistant appears.



Create Device Template Assistant

Device Template Settings

CHOOSE TEMPLATE NAME

File Name	Enter a name under which PRTG will store the file. Template files have the extension .odt in the \PRTG Network Monitor \devicetemplates sub-directory of your PRTG core installation 3226 (of the Master node, if in a cluster 116). If a file with this name already exists in this directory, you will see an according error message. The device templates folder is not accessible on PRTG on demand.
Template Name	Enter a meaningful display name for the template as it will appear in the web interface.
Exclude Sensors	Select sensors that you do not want to include into the device template. Mark the corresponding checkboxes of the sensors that you do not want to include into the device template. Sensors that cannot be saved into templates 2820 will not appear in this list. Sensor types that dynamically scan for available monitoring items when you add the sensor to a device will not appear in this list. PRTG includes these sensors automatically into the template if they support template functionality. You cannot exclude them from the device template that you create.

Click the **Continue** button to save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

If your template file was saved successfully, you will see an according message and can review the sensors that were added. Click **OK** to finish. The device template is now stored in the program path of your PRTG core installation. Your device template file contains all sensors, including their settings, of the original device.

During your next auto-discovery, choose the **Automatic sensor creation using specific device template(s)** option and select the name of your newly created device template from the list. PRTG will then try to discover the stored sensor types on the new (or existing) device. If the physical device answers to a sensor request, the sensor is added to the PRTG device. For detailed information, please see **Auto-Discovery** 249 section.

Settings That Are Not Saved

There are a few settings that you cannot save into a device template, so PRTG will set them to default, for example, the Dependency Type setting **Master object for parent** (in **Schedules and Dependencies** section) and Result Handling settings **Write result do disk** (because this is intended for debugging purposes only). Also, settings in the **Access Rights** section are not saved to avoid security flaws.

In general, you cannot save all **Sensor Settings** 384 and **Sensor Channels Settings** 2782 (for example, channel limits) of sensor types that dynamically scan for available monitoring items when you add the sensor. This affects, for example, **traffic sensors** where you can choose interfaces that you want to monitor in the add sensor dialog 288.

Furthermore, due to internal restrictions, the following sensor types will not be saved into a device template:

- **Amazon CloudWatch sensors**
- **Business Process**
- **Core/Probe/Cluster Health**
- **DHCP**
- **Docker Container Status**
- **Dropbox**
- **Enterprise Virtual Array**
- **Google Analytics**
- **Google Drive**
- **IPFIX**
- **IPFIX (Custom)**
- **IPMI System Health**
- **jFlow V5**
- **jFlow V5 (Custom)**
- **Microsoft OneDrive**
- **NetApp cDOT Aggregate (SOAP)**
- **NetApp cDOT I/O (SOAP)**
- **NetApp cDOT Physical Disk (SOAP)**
- **NetApp cDOT System Health (SOAP)**
- **NetFlow V5**
- **NetFlow V5 (Custom)**
- **NetFlow V9**
- **NetFlow V9 (Custom)**

- **Packet Sniffer**
- **Packet Sniffer (Custom)**
- **Passive Application Performance**
- **QoS (Quality of Service)**
- **QoS (Quality of Service) Roundtrip**
- **Sensor Factory**
- **sFlow**
- **sFlow (Custom)**
- **SNMP Trap Receiver**
- **Syslog Receiver**
- **WMI Security Center**

No Update of Device Templates

Once a device template is created, it is not possible to add additional sensors to it via the PRTG web interface. If you want to create a template with an extended set of sensors, please create a new one.

When saving a new device template, all internal IDs of the sensors in this template are updated. Because of this, when you apply a new template to an existing device, PRTG will newly create all sensors that this template contains on this device, even if these sensors were previously created using another device template!

You cannot directly delete device templates.

You cannot edit existing template files on PRTG on demand.

Related Topics

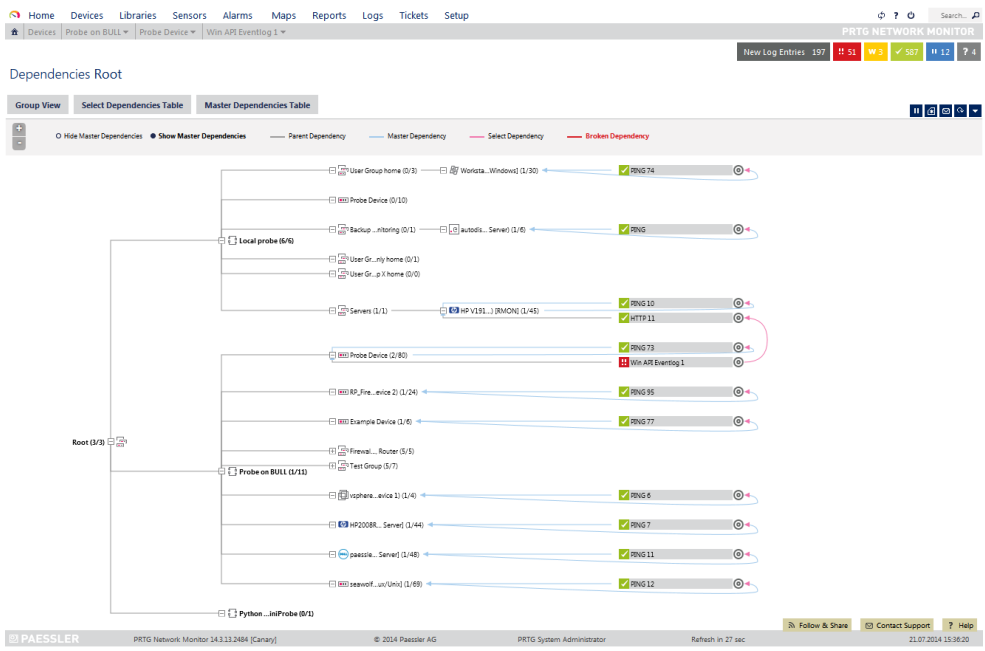
- Clone Object 2812
- Manage Device Tree 292

8.6 Show Dependencies

This function shows an overview of the dependencies configured for the objects in your setup. For a general introduction please see the Dependencies 126 section.

In the main menu bar 231, hover over **Devices** | **Dependencies** to show other menu items. Follow the menu path (it is specific to your setup) to view dependencies of the objects in a specific probe or group only.

- **Selected Dependencies** shows a table of manually set dependencies (section Select object in any object's settings).
- **Master Dependencies** shows a table of master dependencies.
- **Dependencies Graph** shows a visualization of device, group, and sensor dependencies. See below 2822.



Dependencies Graph View

Dependencies Graph

Click **Dependencies Graph** to see the device tree in the dependencies graph view with lines of different color connecting objects. Hover over **Dependencies Graph** to show other menu items for the dependency graph (probes and groups). Click a probe or group menu item to show its dependencies directly. The lines in the dependencies graph symbolize dependencies between the monitoring objects in the device tree. Additionally, a color code 2823 is used for the dependencies.

To show the Dependencies Graph, you need to access the PRTG web interface as a **PRTG System Administrator** user.

- Above the graph header bar, you can switch the dependencies view to tables of the currently selected object with the buttons **Select Dependencies Table** and **Master Dependencies Table**. The button **Group View** will show the **Overview** tab 155 of the currently selected object.
- Mark the radio button in the header bar to **Show Master Dependencies**. By default, **Hide Master Dependencies** is selected and only parent, selected, and broken dependencies are shown.
  These buttons are not available in Internet Explorer for technical reasons. Please use Google Chrome 57 or later (recommended) or Mozilla Firefox 52 or later.
- Click the + or — buttons on the left in the header bar to zoom in or out of the graph.
- Click probe and group nodes to show the respective dependencies.
- Click device or sensor nodes to open the corresponding overview tab.
- Click the + or — boxes to expand or collapse probe and group nodes.
- Numbers in parentheses indicate how many child nodes of an object are shown.
- The **Highlight Connection** buttons to the right of sensors show the corresponding dependency line and parent and dependent objects in bold.

Color Code of Dependencies Graph

The line's colors show the kind and source of a dependency. This represents the **Dependency Type** as defined in the **Schedule, Dependencies, and Maintenance Window** settings of a probe, group, device, or sensor 248.

You can find the color legend also in the graph header bar.

- **Gray**
  Gray lines show a dependency by inheritance (Use parent). The source of the dependency is the parent object on the left end of the line, for example, Root is the parent of Local Probe.
- **Pink**
  Pink lines show a dependency that was set manually (Select object). The source of the dependency points to the dependant with a pink arrow at the line's end.
- **Blue**
  Blue lines show a master dependency for a device (Master object for parent). The sensor that is set as the master points to the dependent device with a blue arrow head at the line's end. The arrow head from the dependent device to its master object is pink.
- **Red**
  Red lines indicate broken dependencies, for example, if the master is not available.

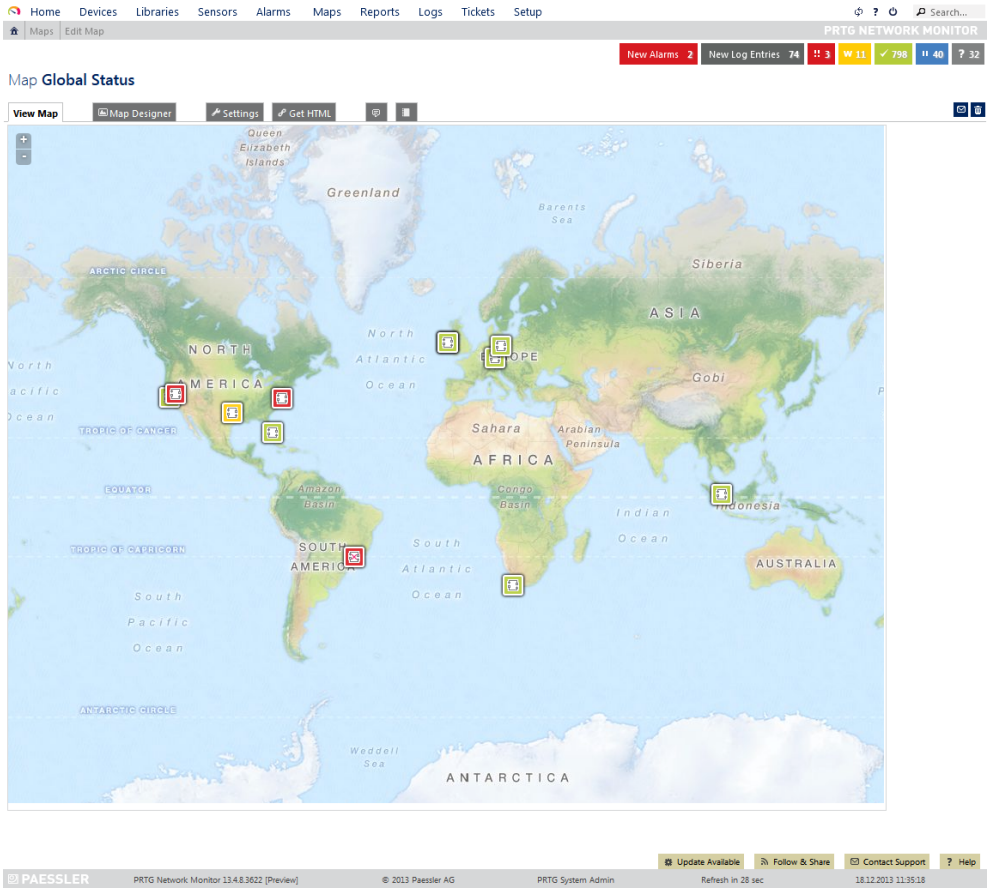
8.7 Geo Maps

With the PRTG Geo Maps feature you can visualize geographical information about your monitored objects. You can display the location of probes, groups, and devices in a graphical map on the details page of an object, or on PRTG **Maps** 2885. This feature is especially useful when you monitor networks that are spread over several different locations. Devices located in a few cities of a country or various continents can all easily be visualized.

You can enter **Location** information for each probe, group, and device. PRTG uses the first line of this information to query a geographical map that shows your objects. Your location specification is resolved to global geographical coordinates by the PRTG core server with the help of an external map service provider.

PRTG connects to the specified maps provider to get map tiles. The map tiles provide the (geo) graphical "background". Then PRTG marks the defined locations with the corresponding object icons and their status 2826 on the map. You can select your favorite map tiles provider in **System Administration—User Interface** 2945 (setting **Geo Maps**).

You can display geographical maps on the device tree. PRTG adjusts the zoom of a map automatically so that it can show all locations of a selected object. You can also add geographical maps to PRTG **Maps** 2885. To do so, open the PRTG **Map Designer** 2893 (either in an existing map or create a new one) and click **Geo Maps** in the properties menu on the right.



The Global Status of a Network in a Geo Map

Using Geo Maps

To use geographical maps within the PRTG web interface 136 or **Enterprise Console** 3028, please ensure the following:

1. In the system administration in the PRTG web interface, select the maps provider and type you want to view. There, you will also find an option to disable geo maps integration if you do not want to use it. See section **System Administration—User Interface** 2945 (setting **Geo Maps**) for detailed information.

2. In the settings of a monitoring object 188 (probe, group, device), add a city name, address, or coordinates in the first line of the **Location** field. When you view the details of this object, PRTG will show a geographical map. PRTG uses the **Location** information also when you view objects in the **Enterprise Console** 3028 or add **Geo Maps** objects to PRTG **Maps** 2885.

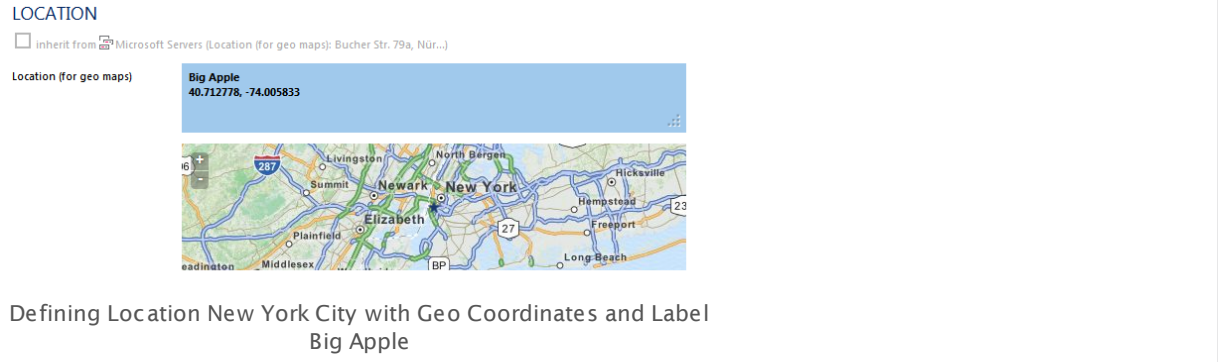
3. Make sure your PRTG core server has access to the internet to obtain map tiles. If a proxy is mandatory in your network, configure proxy settings accordingly. For details, please see **System Administration—Core & Probes** 2967. For details about tile server domains, please see this Knowledge Base article: Which domains and ports does the GeoMaps feature use?

Labeling Locations

You can define your own labels for locations of objects. To do so, enter the desired label in the first line of the **Location** settings and provide the geo coordinates of the location in the second line. This object will appear with the defined label in PRTG geo maps.

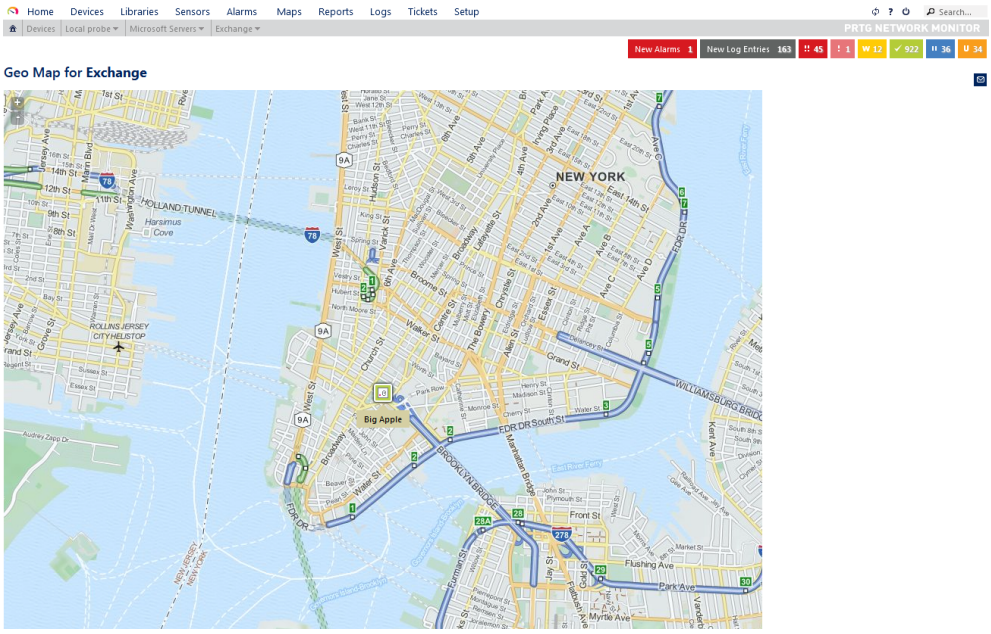
For example, add the following to the location field:

```
Big Apple
40.712778,-74.005833
```



Defining Location New York City with Geo Coordinates and Label Big Apple

The location New York City appears the with the label Big Apple:



Location New York City with Label Big Apple

It is also possible to define the same label for different locations. For example, imagine your company's headquarter is spread over several different locations. For each object representing a dedicated headquarter in the PRTG device tree, enter its coordinates in the second line of the respective **Location** settings and the label "Headquarter" in the first line. All corresponding objects will be displayed as "Headquarter".

This way, you can easily find your desired objects on the map.

Map Icon Colors

On the geographical maps the different location icons show the overall status 163 at this location by using a color code. Following, you can see all possible location states in order of their hierarchy:

Flag	Flag Color	Location Status	Meaning
	Red	**Down**	At least one sensor at this location shows a red **Down** status. Hover the circle with the letter symbol in the legend to view the total number of alarms at this location.
	Bright-Red	**Down (Acknowledged)**	At least one sensor at this location is **Down** and a PRTG user acknowledged this status with the **Acknowledge Alarm** function. The **Down** states of all sensors at this location must be acknowledged—if at least one sensor is unacknowledged down, this location will be displayed as **Down**.
	Yellow	**Warning**	At least one sensor at this location shows a yellow **Warning** status. There is no sensor in a **Down** or **Down (Acknowledged)** status at this location.
	Orange	**Unusual**	At least one sensor at this location shows an orange **Unusual** status. There is no sensor in a **Down**, **Down (Acknowledged)**, or **Warning** status at this location.
	Green	**Up**	All sensors at this location are in a green **Up** status. There is no sensor in a **Down**, **Down (Acknowledged)**, **Warning**, **Paused**, or **Unusual** status at this location.
	Blue	**Paused**	All sensors at this location show a blue **Paused** status. There is no sensor in a **Down**, **Down (Acknowledged)**, **Warning**, **Unusual**, or **Up** status at this location.
	Black (Grey)	**Unknown**	All sensors at this location have an **Unknown** status. There is no sensor in a **Down**, **Down (Acknowledged)**, **Warning**, **Unusual**, **Paused**, or **Up** status at this location.

For detailed information about sensor states, please see the section **Sensor States** 163.

Geo Tracking of Your Mobile Device

It is possible to show the location of an Android device and track its movements on PRTG Geo Maps. PRTG can draw the route a device has taken directly into geo maps. For this feature, you need the PRTG Mobile Probe for Android.

For details, see this Knowledge Base article: How can I track geo data of my Mobile Probe device?

More

Knowledge Base: Which provider should I use for PRTG's "Geo Maps" feature?

- https://kb.paessler.com/en/topic/34603

Knowledge Base: Which domains and ports does the GeoMaps feature use?

- https://kb.paessler.com/en/topic/35823

Knowledge Base: Why does my street not appear on the Geo Map shown in PRTG?

- https://kb.paessler.com/en/topic/35653

Knowledge Base: How do I get a Google Maps API key for use in PRTG?

- https://kb.paessler.com/en/topic/32363

Knowledge Base: Which limitations apply when using the Google Maps API in PRTG?

- https://kb.paessler.com/en/topic/7913

Knowledge Base: How can I change the way markers look like in PRTG's geo maps?

- https://kb.paessler.com/en/topic/43153

Knowledge Base: How can I track geo data of my Mobile Probe device?

- https://kb.paessler.com/en/topic/59647

Knowledge Base: My geo maps are displayed without background. What can I do?

- https://kb.paessler.com/en/topic/63608

8.8 Notifications

PRTG uses notifications to send you alerts whenever PRTG discovers a defined status, such as slow or failing sensors, or when sensor channels breach threshold values. You can define an unlimited number of notifications allowing to use one, or more, of several communication channels like email 2922, text messaging 2924, push notifications 2923 to Android and iOS devices, and many more 2921. PRTG sends notifications to the desired user's **Notification Contacts** 2934 that you can define for each user account of your PRTG installation.

See also our video tutorials for notifications:

- Video Tutorial: Use Cases for Notifications
- Video Tutorial: How to Set Up and Use Notifications in PRTG

Overview

PRTG sends a notification when a defined event evokes it. The following events can trigger notifications:

- **Sensor status changes**
  For example, when a sensor changes status to **Down** or **Warning**, if responses are slow, or sensors show an **Unusual** status.
- **Sensor value threshold breaches**
  For example, when a sensor shows a request time higher than 1,000 ms for more than 30 minutes, or when free disk space is below 10%.
- **Speed threshold breaches**
  For example, when a traffic sensor shows more than 1 Mbit/s for more than 5 minutes.
- **Volume threshold breaches**
  For example, when a traffic sensor shows more than 1 Gbyte transferred in 24 hours.
- **Sensor value changes**
  For some sensors you can trigger a notification whenever the value changes, for example, when monitoring files on a hard disk drive.

A notification can be one of these actions:

- Send Email 2922
- Send Push Notification 2923
- Send SMS/Pager Message 2924
- Add Entry to Event Log 2926
- Send Syslog Message 2927
- Send SNMP Trap 2928
- Execute HTTP Action 2929
- Execute Program 2930
- Send Amazon Simple Notification Service (SNS) Message 2930
- Assign Ticket 2931

For details, see section **Account Settings—Notifications** 2921.

Usually there are three successive attempts to deliver a notification. If all of these attempts fail, the notification is lost. To never miss a notification, we recommend that you always add two different ways to get a notification. For example, use the latency setting of a state trigger 2793 to choose a notification with another delivery method than in the first trigger condition, or set up a second trigger with another notification for the corresponding object.

Notifications can contain valuable sensor information, such as:

- Last error message
- Last good/failed request
- Total downtime
- Total uptime
- Recent sensor history
- A direct link to the web interface

For available placeholders, see this Knowledge Base article: What placeholders can I use with PRTG?

Notifications Setup

Overall, you have to go through four steps to use notifications with PRTG. Please go through all of them for a first setup:

1. Check and set up the **Notification Delivery** settings. This tells PRTG how to send messages.
   For detailed information, see **System Administration—Notification Delivery** 2961.

This only applies to PRTG on premises instances, not to PRTG on demand.

2. Check and set up Notification Contacts for the users of your PRTG installation. This defines where to send notifications.
   For detailed information, see **Account Settings—Notification Contacts** 2934.

3. Check and set up several **Notifications**. This defines the kind of message and its content.
   For detailed information, see **Account Settings—Notifications** 2916.

4. Check and set up **Notification Triggers** for objects. These provoke the defined notifications.
   For detailed information, see **Sensor Notifications Settings** 2791.

We recommend that you always set up at least two notifications with different delivery methods for a notification trigger, for example, one email notification 2922 and one SMS notification 2924. If delivery via email fails (due to a email server outage or for other reasons), PRTG can still notify you via your smartphone in this case as a fallback. You can achieve this, for example, by using the latency setting in a state trigger 2793 and selecting a notification with another delivery method than for the first trigger condition.

Please see the sections **Setting Up Notifications Based on Sensor Limits: Example** 2832 and **Setting up Notifications Based on Libraries: Example** 2840 for a step-by-step guide that describes a potential notifications setup.

There are also custom notification scripts available in the PRTG Script World.

More

Video Tutorial: Use Cases for Notifications

- https://www.paessler.com/support/video_tutorials/notification-and-trigger

Video Tutorial: How to Set Up and Use Notifications in PRTG

- https://www.paessler.com/support/videos/prtg-basics/notifications

Knowledge Base: What placeholders can I use with PRTG?

- https://kb.paessler.com/en/topic/373

Knowledge Base: Notifications based on priorities

- https://kb.paessler.com/en/topic/31243

8.8.1 Setting up Notifications Based on Sensor Limits: Example

This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

This section shows you exemplarily how to set up a notification for exceeded disk free limits. We provide the approach for this specific use case step by step so you can adapt it to define limits and corresponding notifications for other sensor types.

You have to take several steps to set up notifications based on limits:

- Step 1: 2832 Provide necessary information about the delivery of notifications (SMTP and SMS).
- Step 2: 2833 Specify recipients for notifications for each user account of your PRTG installation.
- Step 3: 2833 Create notifications, specifying the type of notification and its content.
- Step 4: 2834 Define thresholds that change a sensor's status (this is not necessary for every kind of notification).
- Step 5: 2837 Add suitable triggers to objects which evoke notifications if something is going wrong in your network.
- Step 6: 2837 Test if the created notification is triggered and delivered correctly.

When you set up your own notifications, you do not necessarily need to go through all the steps we describe here. In this section, our main goal is to give you a general idea of the notifications concept.

Step 1: Setting up the Notification Delivery

Before creating your actual notifications, you first have to define how those notifications are delivered to your email account, mobile phone, or pager. To do so, choose **Setup | System Administration | Notification Delivery** from the PRTG main menu bar. Specify the mechanism of SMTP delivery, sender email and name, as well as the HELO ident. For SMS delivery, select your service provider and provide the corresponding credentials.

You can find details about notification delivery in section **System Administration—Notification Delivery** 2961.

This only applies to PRTG on premises instances, not to PRTG on demand.

Step 2: Setting up Notification Contacts

Create notification contacts to define where you want receive notifications. Recipients can be email addresses, phone numbers (PRTG on premises only), or push devices (Android or iOS devices, or Windows Phone, with the corresponding PRTG smartphone app 3082). You can define as many recipients for each user account in your PRTG installation as you want. By default, the recipient "Primary Email Address" is available—this is the email address you provide in your account settings 2909. This is sufficient for a first setup of notifications. Later on, when you see how it works, you can define more contacts. When you add a notification to a device, you just have to select a user or user group as recipient then and PRTG uses the according contacts you define here.

For details, see section **Account Settings—Notification Contacts** 2934.

Step 3: Setting up the Notification's Content

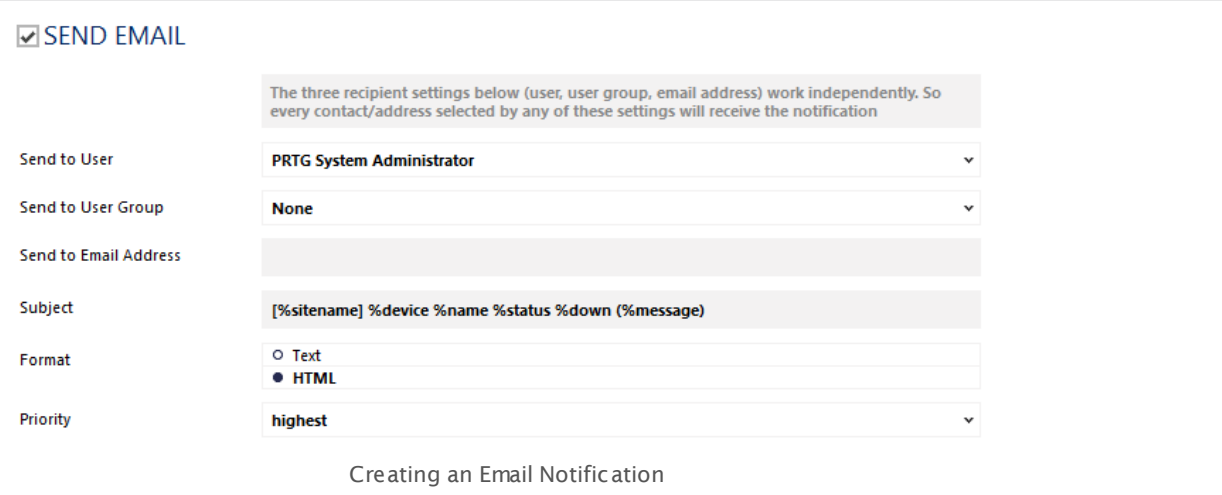
To get an informative message when a disk is running out of capacity, create a corresponding notification. Choose **Setup | Account Settings | Notifications** from PRTG's main menu bar and click on the button **Add New Notification**. Give the notification an explanatory name; in our case you could use Disk Free Limit Notification. However, if you want to trigger this notification on a global level (for example, for a probe or group) such that it would not only apply to breached disk free limits, a general name would be more suitable (like the predefined notification "Email to Admin"). If you leave the default text of the newly created notification, it already contains all necessary information, for example:

- which sensor is affected,
- since when the sensor is affected,
- last value of this sensor.

See section **More** 2838 for the other options you have here.

After providing this basic information, select the delivery method. In our case, we choose **Send Email** for this notification by marking the corresponding checkbox. Specify who will receive the notification (select a specific user, for example, and PRTG sends the notification to all contacts of this user you specified in step 2 2833), its subject, the format, and its priority. By default, the email notification contains several information parameters about the evoking sensor: its name, status, time, message, location in the device tree, etc.

You can choose any other notification method, of course. Please see **Account Settings—Notifications** 2921.



Creating an Email Notification

Once you set up the notification completely, click **Save**. PRTG opens the notifications overview page again. You can now use this notification for every trigger on every object in your device tree.

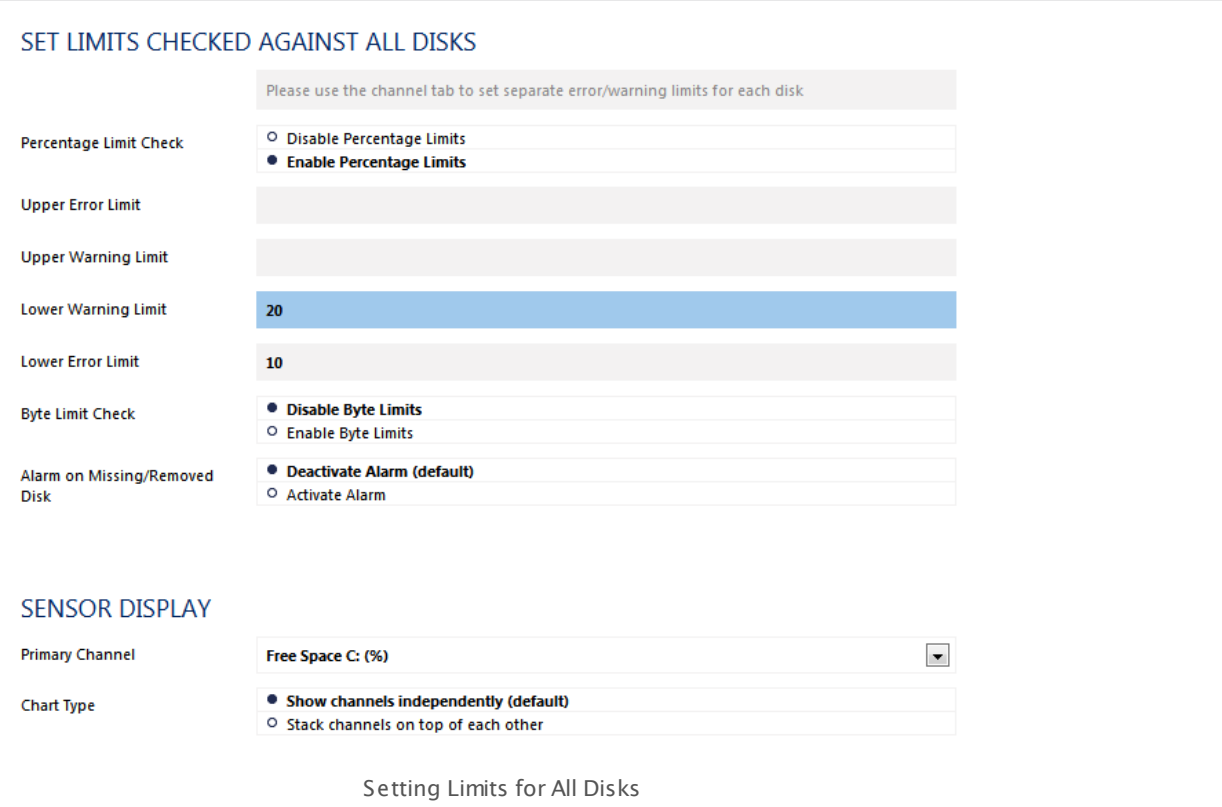
Step 4: Define Limits

Before creating triggers that evoke notifications, first specify the limits which you want to apply to your disks. For example, if you want to get a notification when a disk has exceeded 80% of its capacity, force the sensor into a **Warning** status at this utilization. You have several options to set limits for disk free sensors:

- Set limits checked against all disks in the settings of multi-drive sensors: **WMI Free Disk Space** 2573, **SNMP Linux Disk Free** 1924, **SSH Disk Free** 2170
- Enable limits in **Sensor Channels Settings** 2782 of single sensors.
- You can achieve both with **Multi-Edit** 2814.

Step 4.1: Define Limits in Sensor Settings (Multi-Disk Free Sensors Only)

You can set limits for sensors monitoring multiple disks directly via the **Settings** tab on a sensor's details page. **Multi-Edit** 2816 for existing sensors is also possible. Open the settings of the selected sensor(s) and go to section **Set limits checked against ALL disks**. There, for example, enable **Percentage Limit Check**. In the field **Lower Warning Limit**, enter the percentage suitable to your needs. In our example, this would be **20**. Alternatively, you can use bytes to define a limit. However, we recommend using percentage values for more flexibility. This limit applies to all channels of this sensor that represent disks.



Setting Limits for All Disks

This sensor setting is only available for multi-drive sensors. You can omit Step 4.1 for all sensors that are not from the type "disk free".

Step 4.2: Define Limits for Sensor Channels

To set specific limits for single disks, use the sensor's **Channel** settings. You can open channel settings via the gear icon in the respective channel gauge or in the channels table. **Enable Limits** at the bottom of the channel settings dialog and specify your desired limits in the **Lower Warning Limit** field. This limit only applies to the respective channel.

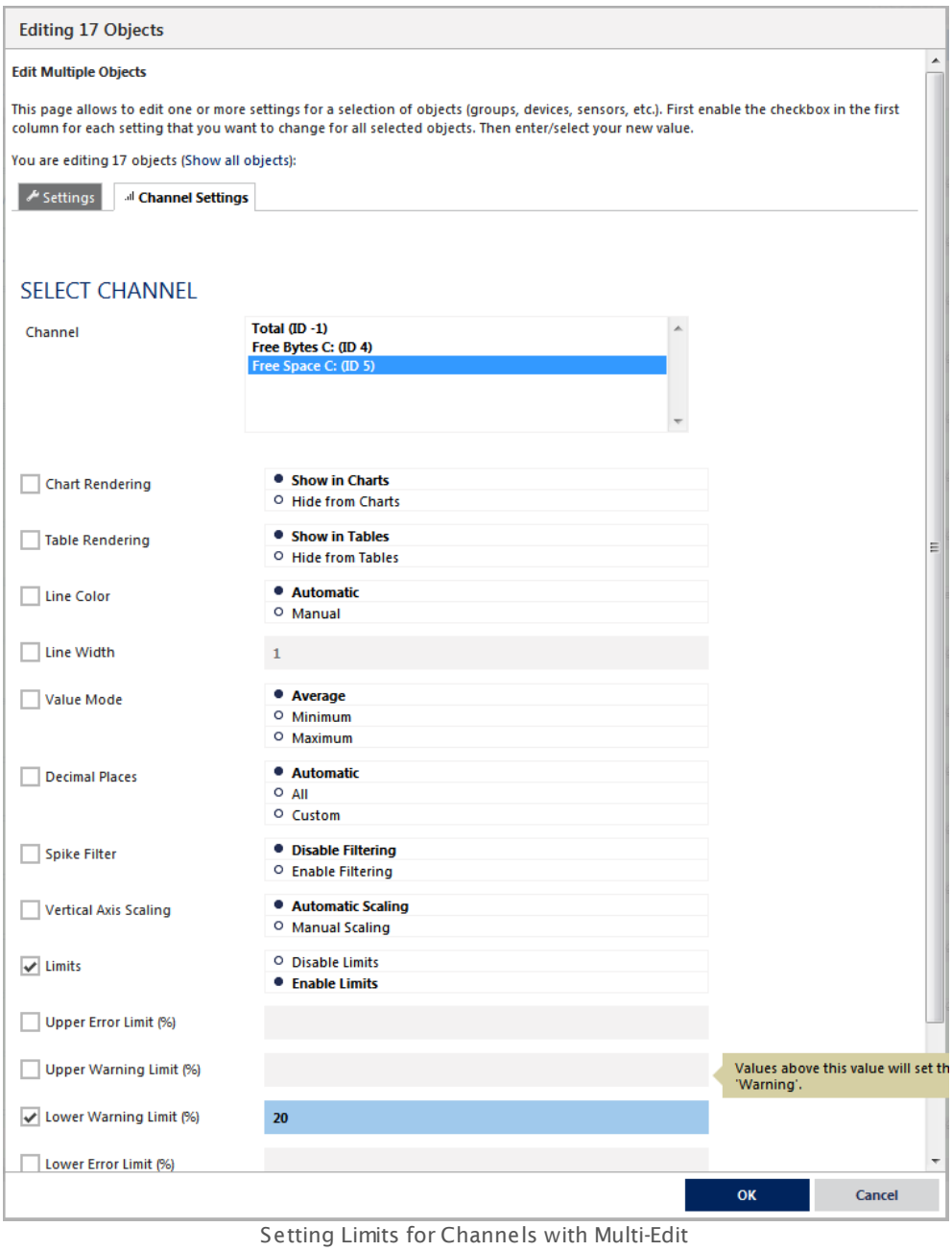
If you define channel limits when using the sensor's limit setting in the sensor's **Settings** tab at the same time, the first limit that applies will be considered. This way, you can individually define harder limits for single disks in a multi-disk sensor. All defined limits are valid side-by-side.

You have to take the approach via channel settings for sensor types that monitor only one (logical) disk, for example, the **SNMP Disk Free Sensor** 1757. For these sensor types, you can use **Multi-Edit** 2817 if you want to apply the same limits for each of these sensors automatically.

- To see all sensors of this type at a glance, just filter for it: From PRTG's main menu bar, choose **Sensors | By Type | SNMP Disk Free**.
- Mark the checkboxes of the sensors you want to add a limit for.
- Click the wrench symbol in the multi-edit bar.
- Open the **Channel Settings** tab.

- Select the channel you want to add a limit for; in this case it would be most likely the channel **Free Space**.
- Then **Enable Limits** at the bottom of the dialog and enter the number in the correct field as described above.

When you are done, save these settings—the new limit applies to all channels with this name of the multi-edited sensors.



Setting Limits for Channels with Multi-Edit

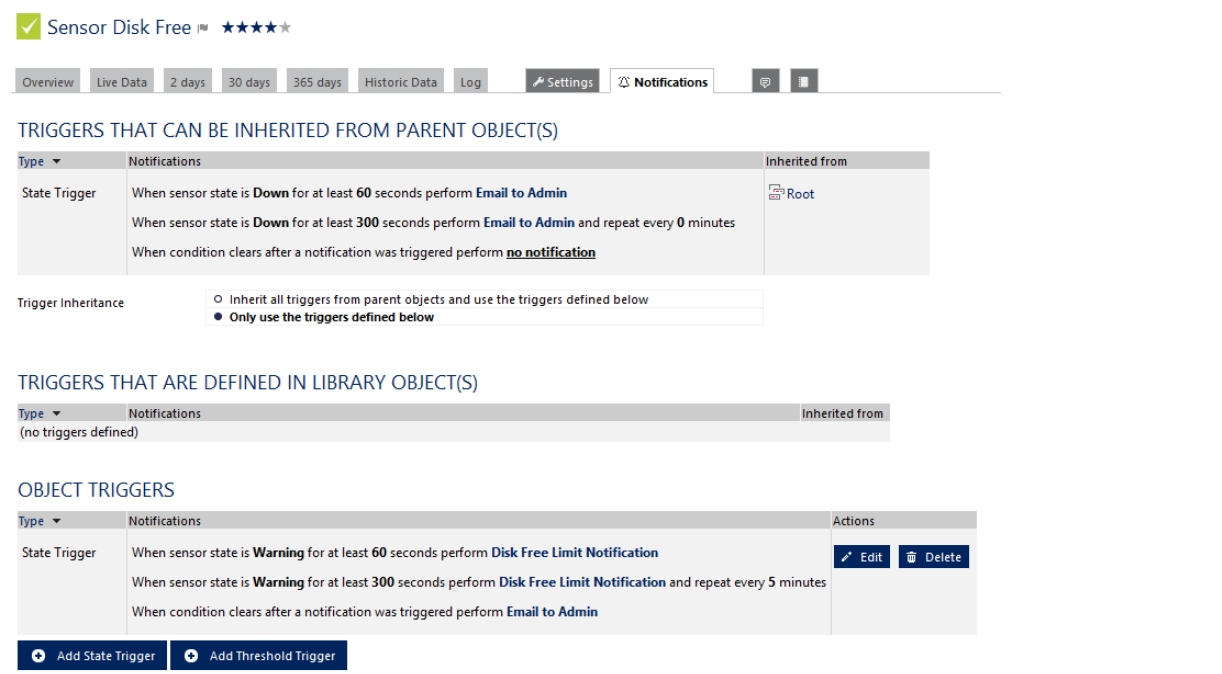
Step 5: Setting up the Notification Trigger

You specified limits to define when a sensor will go into a **Warning** (or **Error**) status. Now you can create the according triggers. The trigger we use in this example is the **State Trigger**.

For details about other possible notification triggers, see section **More** 2838.

- You can set up a **State Trigger** on any level in your device tree. For example, open a group containing the device(s) representing your disks.
- Open the **Notifications** tab.
- Click **Add State Trigger**.
- Set the trigger to "When sensor is Warning" and choose the notification you created before ("Disk Free Limit Notification" or a more general one) from the drop down list.
- Adjust the other notification settings to your needs and save this new object trigger.

Now you receive a notification immediately when the capacity of one of your disks falls below the defined limit, in this case 20% free disk space.



Setting a Trigger for Disk Free Limit Notification

Step 6: Testing the Notification

Finally, test the notification that you created. You can trigger this notification for test purposes immediately:

- From the main menu bar 231, choose **Setup | Account Settings | Notifications**.
- For the respective notification, click on the corresponding **Test** button.

Then, check if the notification was triggered and delivered correctly, depending on the delivery method you defined before. If you do not get a notification (or a defined action is not executed) at all, check the notification logs: From the main menu bar, choose **Logs | System Events | Notifications**. Look for the triggered notification in the table list (verifying that the notification delivery is set up correctly in general) and consider the corresponding message. See section **Logs** 198 for more information.

More

This section provides information about additional options you have when working with notifications.

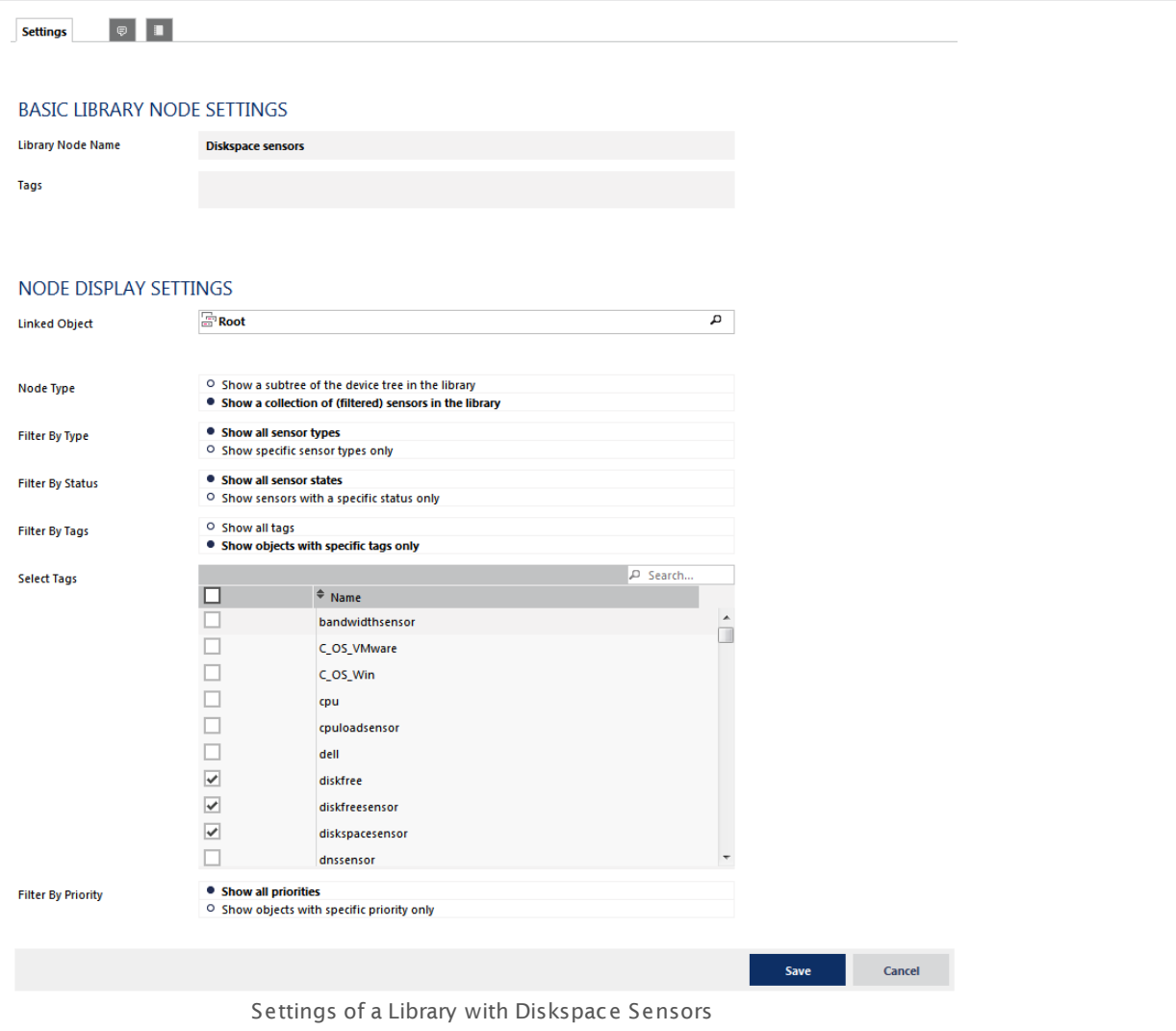
- **Notification Settings:**
  You can create schedules to activate notifications only at specific times, for example, only on weekdays. In section **Notification Summarization** you can choose between various options to avoid message floodings. Furthermore, define which user groups will have access to edit this notification. For details about notification settings, refer to section **Account Settings—Notifications** 2916.

- **Content of Emails:**
  You can individually adjust the subject, header, and footer of emails to your needs. See section **Account Settings—Notifications** 2921 for details about editing the subject. The article How can I include my own logo into HTML emails? in the Knowledge Base explains how to edit the header and footer of emails.

- **Other Triggers:**
  An alternative to the state trigger would be to add a **Threshold Trigger**; then you would not need to set up limits explicitly, though, this trigger type would only be suitable for disk free sensors when using the trigger for single sensors, one by one. Free disk sensors have free space in percent as primary by default, other sensors have primary channels with the units bytes or seconds. However, threshold triggers only apply to the primary or total channel. General notification triggering by threshold might not work as expected for sensors of the "percentage" type. You can find all available triggers in section **Notifications** 2829.

- Add a **Threshold Trigger** to a sensor directly:
  Go on a sensor's detail page and select the **Notifications** tab. Click on **Add Threshold Trigger**, select the desired channel, and provide the condition when this notification will be sent. In this example for free disk space, the setting would be "When Free Bytes C: (%) channel is Below 20 for at least 60 seconds perform Disk Free Limit Notification".

- **Notifications with Libraries:**
  If your disk devices are spread over many groups, we recommend that you use a PRTG library 2845 for your disks. Choose **Libraries | All diskspace sensors** from the main menu bar, go on the **Notifications** tab, and add a state trigger as described above.
  Not all disk free sensor types might appear. You can add them to this library in the settings of the library node. There you can filter by type or tag 2855 and add missing sensors this way. You can also filter by priority and other sensor properties.



Settings of a Library with Diskspace Sensors

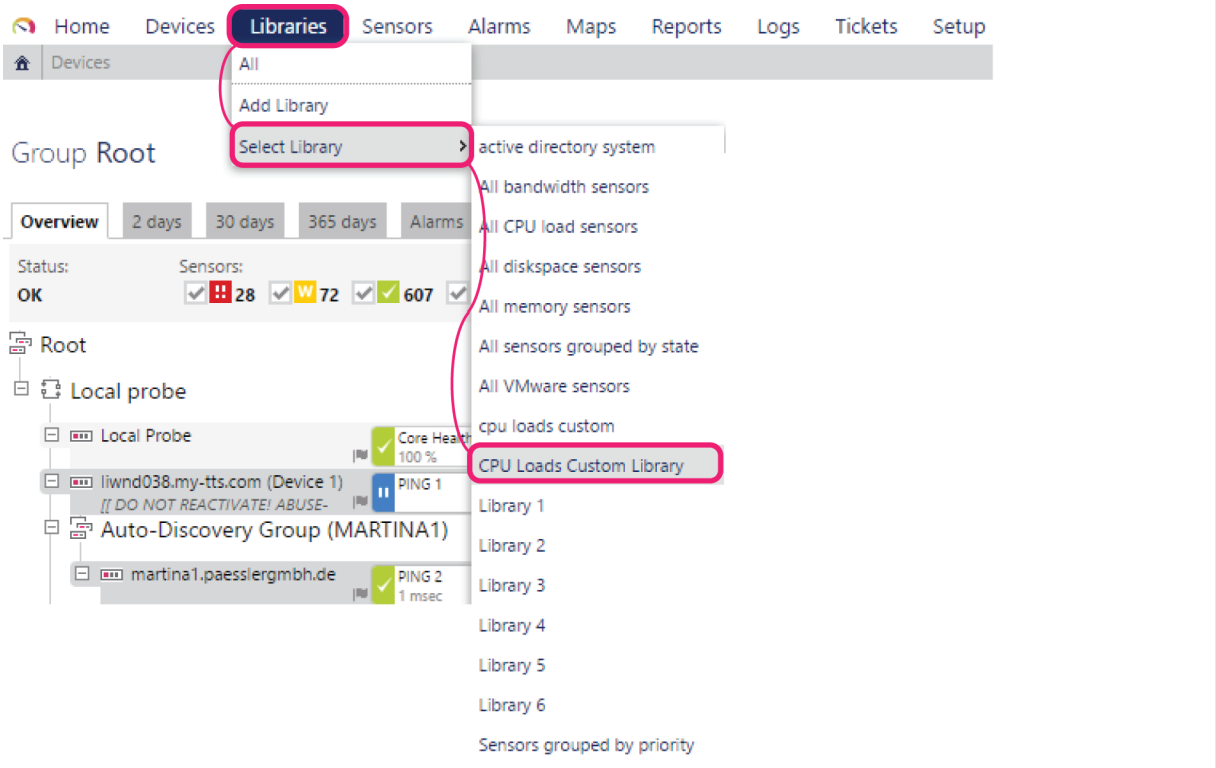
8.8.2 Setting up Notifications Based on Libraries: Example

What's so special about notifications set to whole libraries instead of single sensors? How do I set up libraries, and how do I get the most out of my library notifications?

This section describes how you can reorganize your devices or sensors by their function, and thereby create a new customizable view. This way you can monitor entire sections of your network with a single set of notifications [2829].

You can personalize these views and their notifications for your own use. Furthermore, you can grant and restrict permission to this view to other PRTG users or PRTG user groups, to give them direct access to some of the information in PRTG. By using libraries, you can make your notification management faster, easier, more powerful, and more refined.

Step 1: Setting up a New Library



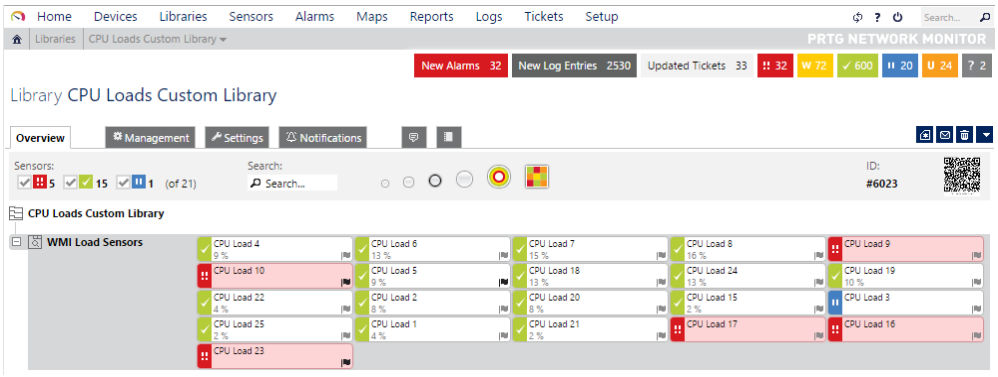
Creating a new library

Click here to enlarge: https://media-s3.paessler.com/prtg-screenshots/Setting-up-notifications-based-on-libraries_3.png

Create a new library:

- Select **Libraries** from the main menu bar and click **Add Library**.
- Give the library a meaningful name. Possibly add some **Tags** [124] for easier organization.
- Optionally, assign access rights to your predefined user groups.

- Click **Continue** to create the new library.
- The **Management** tab of the library opens.



Library overview tab

Click here to enlarge: https://media-s3.paessler.com/prtg-screenshots/Setting-up-notifications-based-on-libraries_4.png

Add objects to your library:

- Click the **Add Library Node** button.
- The **Add Library** dialog opens.
- Define the **Node Display Settings**:
  - Choose a node from which the sensors will be taken (predefined: **Root**).
  - Select **Show a collection of filtered sensors in the library (max. 1000)** to filter (the subtree) further.

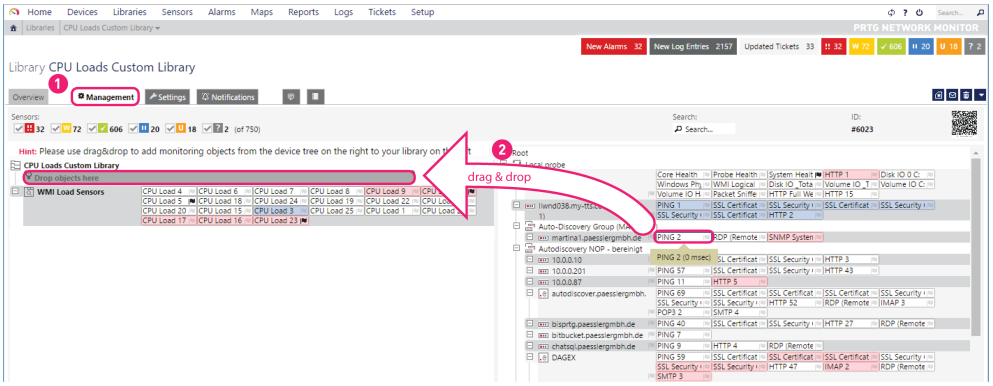
Choose from following filter criteria:

- **Show specific sensor types only:** Add checkmarks to sensor types you want to include.
- **Show specific sensor types only:** Add checkmarks to sensor types you want to include.
- **Show sensors with a specific sensor status only:** Choose from up, warning, down, or unusual.
- **Show objects with specific tags only:** Enter tags to include certain sensors.
- **Show objects with a specific priority only**: Priority "1" through "5" is possible.

The libraries are dynamic not static. When you add or remove sensors to your device tree that are of a type already specified here, the library will automatically update the displayed sensors. The same is true for the other three categories.

- Confirm via **Continue**.
- The new library node appears.

You can rearrange the nodes in any sequence you require. To manually add objects from the device tree, proceed as follows: Select the **Management** tab, click and hold an object from the right-hand device tree, then drag over to left-hand gray area. This will transfer the entire content of the object to a new library node.



Manually adding objects to libraries

Click here to enlarge: https://media-s3.paessler.com/prtg-screenshots/Setting-up-notifications-based-on-libraries_2.png

Step 2: Specify Notification Triggers

You can use library notifications very much the same way as notifications for sensors or devices.

- In your library, click the **Notifications** tab.
- Choose one of the various notification trigger types and configure it:
- **Add State Trigger** to send notifications about sensor states 163 over a specified time period.
- **Add Speed Trigger** to send notifications when having too little or too much traffic over a specified time period.
- **Add Volume Trigger** to send notifications when a predefined amount of data in the specified interval is accumulated.
- **Add Threshold Trigger** to send notifications if a sensor channel value goes beyond or below a certain limit.
- **Add Change Trigger** to send change messages sent by your sensor (only certain sensors provoke change triggers).

Example: Library Notification

You monitor hundreds of servers and want to keep an eye on CPU utilization. Using the channel limits within the sensors would cause an overwhelming amount of alerts, because CPUs can easily spike to 100% load for one scanning interval, without necessarily indicating a problem.

Using libraries, it only takes you a couple of minutes to create a notification setup that will notify you when a CPU runs at more than 90% load for more than 5 minutes.

We recommend the following steps:

1. Create a custom library.

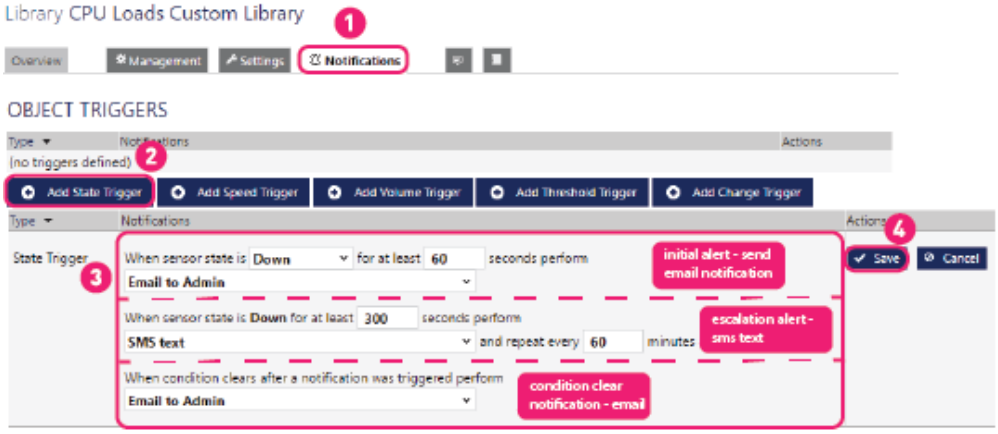
2. Add CPU sensors (via tag or type).

3. Add a threshold-based notification.

4. Enjoy complete piece of mind!

Add a state trigger to your library:

- Select **Notifications** tab (1).
- Click **Add State Trigger** (2).
- Enter the desired notification specifications in the definition box (3), including:
  - initial parameters (triggering state, triggering state duration, notification type triggered),
  - escalation parameters (triggering state is always the same, ongoing duration that triggers escalation, the type of the escalation notification triggered, and how often it is repeated),
  - if the trigger parameters no longer apply, enter the type of notification to be triggered.
- Click **Save** and you're done (4).



Example: setting notifications to libraries

Click here to enlarge: https://media-s3.paessler.com/prtg-screenshots/Setting-up-notifications-based-on-libraries.png

- An overview of all currently defined triggers appears.

On top of that, you may want PRTG to keep sending you **Tickets**, when a lower load threshold is periodically exceeded. This low priority notification will remind you to keep an eye on a certain part of your network. Proceed likewise via the **Add Threshold Trigger** button.

Note: You are completely free to set multiple triggers of the same type, so you can define increasingly serious notifications, as well progressing through different notification actions (like email and SMS text). For system-critical network components we recommend that you always define two different notification triggers (for example: email and escalation SMS text message).

The next steps will be to review the notifications settings, summarization, and notification actions in the main menu **Setup | Account Settings | Notifications**.

Step 3: Test, Troubleshooting, and Customization

To make sure the notification system works as desired, you can trigger test notifications out of PRTG.

- Click the **Test** button next to a notification under **Setup | Account Settings | Notifications**.
- Check if the test email and/or SMS text has arrived.

In test notification messages, placeholders will not be resolved.

Troubleshooting: if you suspect a notification might not arrive, proceed as follows:

- Choose **Setup | Account Settings | Notifications** from the main menu bar.
- Go to the notification action you have assigned in the library and click **Edit**.
- Review the notification setting so that:
  - The notifications are in the **Active** status.
  - The notifications have a schedule 2938 that does not conflict with the library you just set up or currently pauses the notification.
  - The summarization method collects alarms for a certain period. Also consider the **Timespan for Summarizing Messages** value.
  - The user email addresses (phone numbers) specified for each user account are correct.
- Check the **Notification Delivery Settings** 2961 under **Setup | System Administration | Notification Delivery**.

This only applies to PRTG on premises instances, not to PRTG on demand.

- Review the logs 198 for system events of the type "Notification" and the respective notification's name.
- Repeat these steps for all your notifications.

Sensors can perform simulated errors. Go to the library's **Overview** tab, right-click a sensor, and select **Simulate Error Status** from the context menu. You will see that the sensor status quickly changes and sends the following message: Simulated error (code: PE034). This also triggers the notification.

You can have the overall status of your library displayed as custom object on a map. See this Knowledge Base article: How can I use a status icon of a device in Maps which only considers specific sensors?

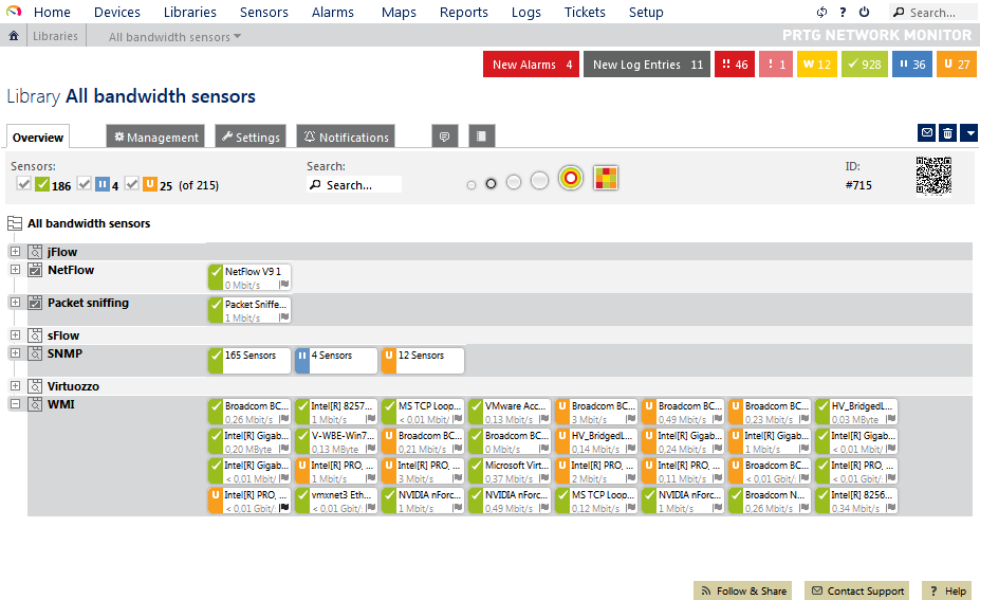
More

Knowledge Base: How can I use a status icon of a device in Maps which only considers specific sensors?

- https://kb.paessler.com/en/topic/59942

8.9 Libraries

With the **Libraries** feature in PRTG you can create special views of your device tree with up-to-the-minute monitoring status information, arranged the way you want it.



Example of a Library

In this section:

- Introduction 2845
- Start Libraries 2846
- Libraries List 2846
- Working with Libraries 2847

See also this video tutorial: PRTG Network Monitor – Libraries

Introduction

Libraries are a powerful feature that enables you to create additional views of your device tree. These views are updated with the same scanning interval as your device tree, showing the same monitoring data, but arranged the way you want. This is useful if you want to display data in different ways, like depending on target groups or a specific use case.

For example, you can create a library that contains an overview of all your bandwidth monitoring sensors, regardless of the device they are running on.

The library features include:

- Create libraries containing nodes with monitoring objects from all over your configuration.
- Show data from different PRTG probes in one library.

- Show different branches of your device tree right next to each other.
- Arrange sensors in a tree-like view regardless of the device they are running on.
- Filter your entire tree (or parts of it) for sensor type, state, or tag, showing only matching sensors.

You can create libraries easily, using drag&drop.

PRTG comes with several pre-configured standard libraries, which you can use right away. You can also change or delete them, if you like. The following libraries are automatically created when you install PRTG for the first time (visible for the PRTG Administrator user). Some of them will initially be empty, but as you add more sensors, they will be filled automatically according to the filter settings defined for the nodes of the libraries:

- All bandwidth sensors
- All CPU load sensors
- All disk space sensors
- All memory sensors
- All VMware sensors
- Sensors grouped by priority
- Sensors grouped by state

Sensors that are added to libraries are not counted against the maximum number of sensors of your license.

Start Libraries

Click **Libraries** in the main menu 235 to view or add custom views of your network's status and monitoring data. Hover over **Start Libraries** to show other menu items. Choose between:

LIBRARIES	
All	Open the Libraries overview list where you can view or add custom device tree views of your network status and monitoring data.
Add Library	Open an assistant to directly create 2848 a new library.
Select Library	Open an existing library. Hover over **Select Library** to show other menu items. Follow the menu path (it is specific to your setup) to select a library and open it.

Libraries List

In the **All** view, you see a list of all existing libraries. Using the links next to a library name, you can perform the following actions.

- **Edit**: Open this library and change the settings 2855 of the library and its nodes.
- **Clone**: Create a clone 2812 of this library.
- **Delete**: Delete this library.
- **Used by**: Show which other monitoring objects use this library.
- Click the **Add Library** button to add a new library.

Please also see **Working with Table Lists** 207. Additionally, the multi-edit functionality is available. This enables you to change properties of several objects simultaneously via bulk changes. For more details, see the **Multi-Edit Lists** 2814 section.

Working with Libraries

For detailed information on how to create and edit libraries please see the following sections.

- **Libraries Step By Step** 2848
- **Management** 2852
- **Libraries and Node Settings** 2855
- **Context Menus** 2861

More

Video Tutorial: PRTG Network Monitor – Libraries

- https://www.paessler.com/support/videos/prtg-basics/libraries

8.9.1 Libraries Step By Step

In order to create a new library, follow the steps in this section. In the web interface, click on the **Libraries** entry in the main menu to show the libraries main screen.

This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

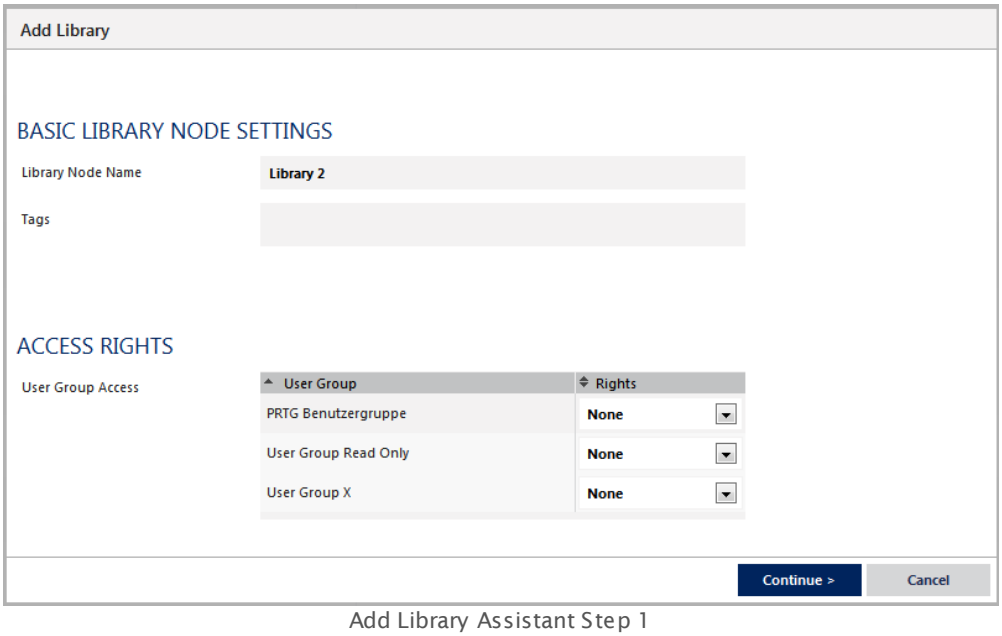
In this section:

- Step 1: Add Library 2848
- Step 2: Add Library Nodes 2849
- Step 3: Set Library Node Display Settings 2850
- Step 4: View 2850

Step 1: Add Library

- Click the **Add Library** button. An assistant is shown.
- Enter a **Library Name**.
- Define **Tags** and **Access Rights** if you like.
- Click **Continue**.

For detailed information, see **Libraries Settings** 2855 section.

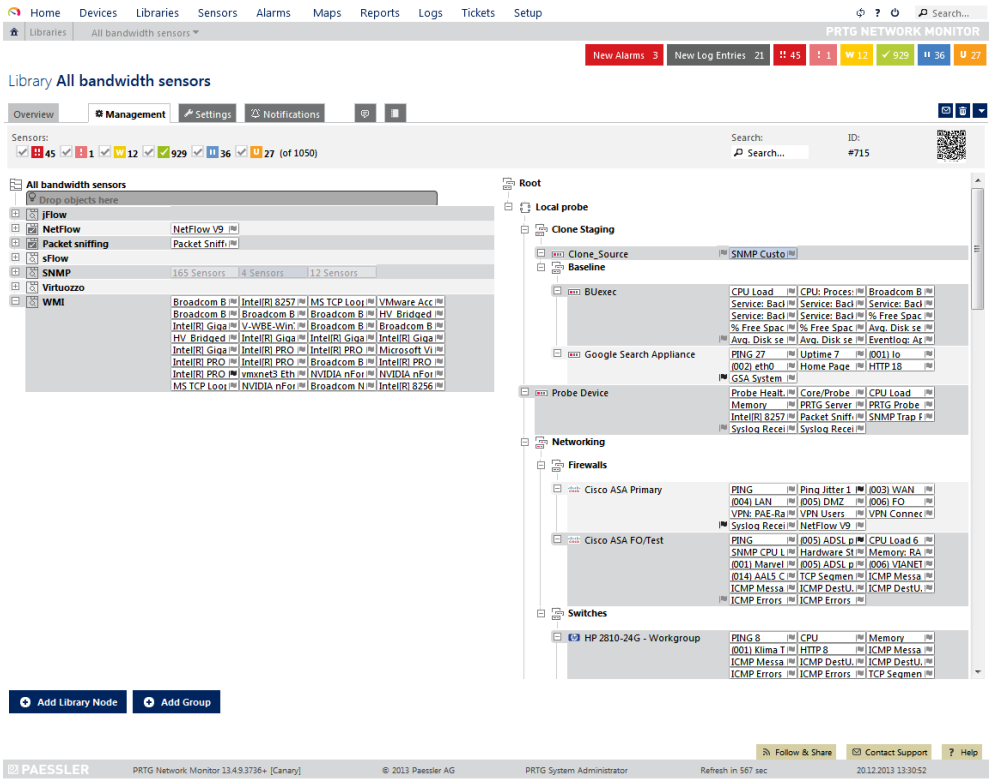


Add Library Assistant Step 1

Step 2: Add Library Nodes

Click the **Management** tab. You will see a split screen:

- On the left side, your library is shown (empty in the beginning).
- On the right side, you see a less colorful view of your device tree, as known from the device tree's Management [292] tab.



Bandwidth Library in Management Mode

From the device tree on the right side, drag objects and drop them on the library on the left side. Each dropped object will be added immediately as a new Library Node. Repeat this procedure as often as you wish until you have added all desired items to the library.

When adding single sensors to the library, there can only be one sensor in one library node.

Library nodes can contain up to 1,000 sensors.

You can also create nested library nodes by adding a new node underneath an existing one or to a group.

Drag and drop nodes within the library to change their position. If you want to change the monitoring object that is associated with a library node, you can change the **Linked Object** in the node's settings.

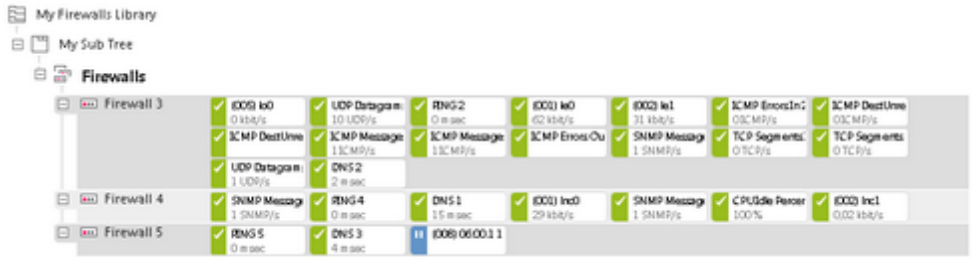
Step 3: Set Library Node Display Settings

You are still in the library **Management** tab.

Right-click the name of a Library Node and from the context menu, select **Edit | Settings...** to change the **Node Display Settings**. In this dialog, you can change the name of the library and its tags, as well as the linked object, node type, and filters.

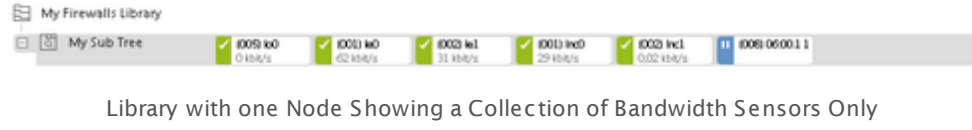
These settings are available for each library node. You can choose to either show the **Linked Object** as a sub-tree of your device tree, or to view a collection of all sensors underneath the **Linked Object**.

When selecting the sub-tree view, the library node will just look like a branch in your device tree, as shown in the screen shot below for the library node names "My Sub Tree".



Library with one Node Showing a Branch of the Device Tree

When selecting a sensor collection view, only the sensors underneath the **Linked Object** are shown, omitting probes, groups, and devices. You can additionally filter by certain sensor **Type**, **Status**, and **Tags**. Only matching sensors will be shown. The screenshot below shows the same **Linked Object** as above, but in sensor collection view, additionally filtered for sensors with a **bandwidthsensor** tag.



Library with one Node Showing a Collection of Bandwidth Sensors Only

For detailed information, see **Libraries and Node Settings** 2855 (Overview—Library Node Display Settings) section.

Step 4: View

Click the **Overview** tab to see the final appearance of your library. You have the following options:

- Hover over an object to view a popup window with recent monitoring and status data.

- Use the sensor status selection bar to select which sensors you want to see for the library: Simply remove check marks for sensor states you want to hide.
  This function is the same you know from the device tree's sensor status bar 155. The setting is reset the next time you open the library.

- Use the **Device Tree View** selection in the page header bar 155 to change the size of the library display.
  This function is the same you know from the device tree 157.

- Use the **Search** box in the page header bar 155 to search the library for a string in object names. Matching objects will be shown full-colored, all others will be grayed out while the filter is active. Click the small **x** symbol in the search field to reset the filter.
  This function is the same you know from the device tree 155.

It depends on the library's access rights and the currently logged in user account if it will be visible to other PRTG users. Also, clicking objects in the library (for example, sensors) will lead to more detailed information about the object or to an error message indicating insufficient access rights—depending on user account and access rights.

In libraries, you can right-click objects to access their **Context Menus** 2861. If you want you can also set up notifications to entire libraries, see our example chapter here 2840

More

Video Tutorial: Libraries in PRTG

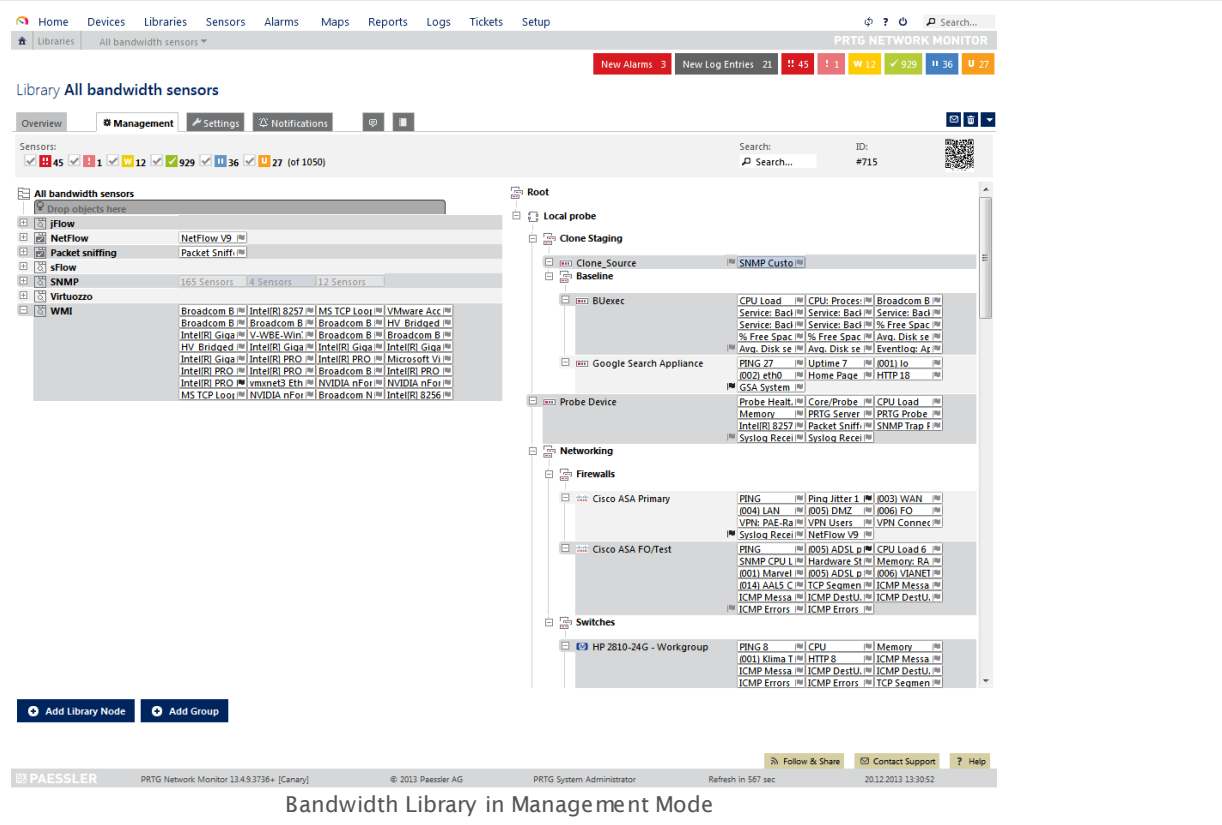
- https://www.paessler.com/support/videos/prtg-basics/libraries

8.9.2 Management

This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

Click the **Management** tab. You will see a split screen:

- On the left side, your library is shown (empty in the beginning).
- On the right side, you see a less colorful view of your device tree, as known from the device tree's **Management** 292 tab.



Bandwidth Library in Management Mode

Add and Change Library Nodes

From the device tree on the right side, drag objects and drop them on the library on the left side. Each dropped object will be added immediately as a new Library Node. Repeat this procedure as often as you wish until you have added all desired items to the library.

When adding single sensors to the library, there can only be one sensor in one library node.

Library nodes can contain up to 1,000 sensors.

You can also create nested library nodes by adding a new node underneath an existing one or to a group.

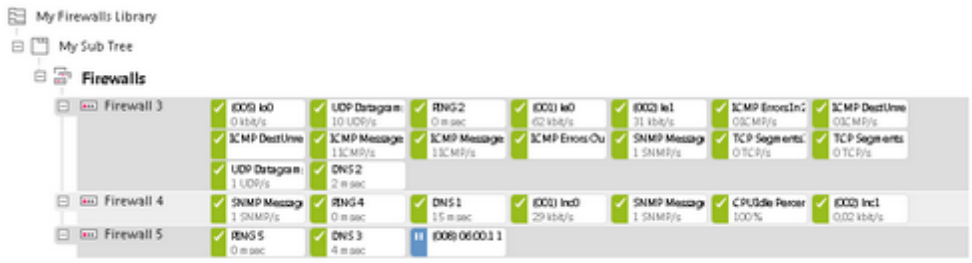
Drag and drop nodes within the library to change their position. If you want to change the monitoring object that is associated with a library node, you can change the **Linked Object** in the node's settings.

Set Library Node Display Settings

Right-click the name of a Library Node and from the context menu, select **Edit | Settings...** to change the **Node Display Settings**. In this dialog, you can change the name of the library and its tags, as well as the linked object, node type, and filters.

These settings are available for each library node. You can choose to either show the **Linked Object** as a sub-tree of your device tree, or to view a collection of all sensors underneath the **Linked Object**.

When selecting the sub-tree view, the library node will just look like a branch in your device tree, as shown in the screen shot below for the library node names "My Sub Tree".



Library with one Node Showing a Branch of the Device Tree

When selecting a sensor collection view, only the sensors underneath the **Linked Object** are shown, omitting probes, groups, and devices. You can additionally filter by certain sensor **Type**, **Status**, and **Tags**. Only matching sensors will be shown. The screenshot below shows the same **Linked Object** as above, but in sensor collection view, additionally filtered for sensors with a **bandwidthsensor** tag.

Library with one Node Showing a Collection of Bandwidth Sensors Only

For detailed information, see Libraries and Node Settings 2855 (Overview—Library Node Display Settings) section.

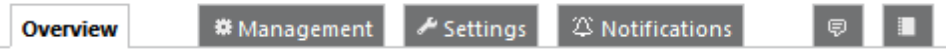
Context Menus

On right-click, there are different context menus available—in the **Management** as well as in the **Overview** tab.

For detailed information, please see **Context Menus** 2863 section.

8.9.3 Libraries and Node Settings

Using the libraries tabs you can access all functionalities and settings for a library.



Library Tabs

Overview

Click the **Overview** tab any time to show the current state of your library.

Library Node Display Settings

While in the **Overview** tab, click the name of a library node to change its settings. Or, while in the **Management** tab, right-click a library node's name and select **Edit | Settings...** from the context menu. In both cases, the following settings are shown.

You can only change the settings of a node if it already contains monitoring objects like groups, devices, or sensors.

BASIC LIBRARY NODE SETTINGS

Library Node Name	Enter a meaningful name for the library node.
Tags	Enter one or more tags, separated by space or comma. For example, you can use tags later to search for the library. Tags are not case sensitive.

NODE DISPLAY SETTINGS

Linked Object	Click the reading-class symbol to change the object that is linked to this library node. The **Object Selector** 210 will appear.
Node Type	Select what you want to view for this library node. Choose between: ▪ **Show a subtree of the device tree in the library**: View all objects underneath the linked object as a device tree. ▪ **Show a collection of filtered sensors in the library (max. 1000)**: View all sensors underneath the linked object (only sensors are shown). You can combine several filters with each other (see below).

NODE DISPLAY SETTINGS

The node can show up to 1,000 sensors, surplus sensors are discarded.

Filter By Type

This option is only visible if collection of sensors is enabled above. Select if you want to filter the sensor list by a certain type. Choose between:

- **Show all sensor types**: Do not filter for a sensor type.
- **Show specific sensor types only**: Filter the sensor list of the linked object for certain sensor types.

This filter is applied in real-time. If the configuration underneath the linked object changes, the library node will show matching sensors accordingly.

Select Sensor Types

This option is only visible if filtering by type is enabled above. A list of all sensor types is shown, currently available sensor types are shown in bold letters for your convenience.

Set a check mark in front of each sensor type you want to include in the library node view. You can also select and deselect all items by using the check box in the table head.

This filter is applied in real-time. If the configuration underneath the linked object changes, the library node will show matching sensors accordingly.

You cannot filter for sensor types that are defined in PRTG Mini Probes.

Filter By Status

This option is only visible if collection of sensors is enabled above. Choose between:

- **Show all sensor states**: Do not filter for a sensor status.
- **Show sensors with a specific status only**: Filter the sensor list of the linked object for sensors in certain states.

Select Sensor States

This option is only visible if filtering by sensor state is enabled above. A list of sensor states is shown. Set a check mark in front of each status you want to include in the library node view. Choose from:

- **Unknown**
- **Up**
- **Warning**

NODE DISPLAY SETTINGS

- **Down**
- **Paused**
- **Unusual**
- **Down (Acknowledged)**
- **Down (Partial)**

You can also select and deselect all items by using the check box in the table head.

This filter is applied in real-time. If the configuration underneath the linked object changes, the library node will show matching sensors accordingly.

Filter By Tags

This option is only visible if collection of sensors is enabled above. Choose between:

- **Show all sensor tags**: Do not filter for a tag.
- **Show objects with specific tags only**: Filter the sensor list of the linked object for sensors with a certain tag 124.

The tag of a sensor can also be inherited 122 by a parent object.

Select Tags

This option is only visible if collection of sensors is enabled above. Enter one or more tags 124 of sensors that you want to include in the library node view. You can also use plus (must have) and minus (must not have) signs to categorize tags, for example, +snmp;-wmi (must have the tag snmp and must not have the tag wmi).

This filter is applied in real-time. If the configuration underneath the linked object changes, the library node will show matching sensors accordingly.

Filter By Priority

This option is only visible if collection of sensors is enabled above. Choose between:

- **Show all priorities**: Do not filter for the priority setting 211 of a sensor.
- **Show objects with specific priority only**: Filter the sensor list of the linked object for sensors with specific priority.

The priority setting of a group, device, or sensor is ignored here; only the priority setting of the sensor itself is regarded.

NODE DISPLAY SETTINGS

Select Priority	This option is only visible if collection of sensors is enabled above. Define which priority setting sensors must have to appear in this collection. Set a check mark in front of each priority you want to include in the library node view. Choose from: ▪ ***** **(highest)** ▪ **** ▪ *** ▪ ** ▪ * **(lowest)** This filter is applied in real-time. If the configuration underneath the linked object changes, the library node will show matching sensors accordingly.

Click **Save** to save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

After applying filters it might take several seconds for the changes to become visible. This is due to internal filter processes running in the background.

Management

Click the **Management** tab to edit the contents of your library, for example, to add items to the library using drag&drop.

For more details, see section **Management** 2852.

Settings

Click the **Settings** tab to open a library's general settings.

BASIC LIBRARY SETTINGS

Library Name	Enter a meaningful name for the library.
Tags	Enter one or more tags 124, separated by space or comma. For example, you can use tags later to search for the library. Tags entered here are inherited 122 to all library nodes underneath. Tags are not case sensitive.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the access rights settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ **Read**: Users in this group can see the object and review its monitoring results. ▪ **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 2982 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option. For more details on access rights, please see the section **User Access Rights** 129.

When giving access rights to a user group, all members of this user group will be able to see the objects in the library just as seen by the user who originally created the library.

Click **Save** to save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Notifications

You can define notification triggers for any kind of object libraries. This is even possible for dynamic libraries which can change with every scanning interval, for example, when you filter a library for the sensor status or priority.

For details about how to use notifications, please see section **Notifications** 2829.

Comments

On the **Comments** tab you can enter free text for each object. You can use this function for documentation purposes or to leave information for other users.

Click **Save** to save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

History

In the **History** tab all changes in the settings of an object are logged with a timestamp, the name of the PRTG user who made the change, and a message. The history log retains the last 100 entries.

Delete

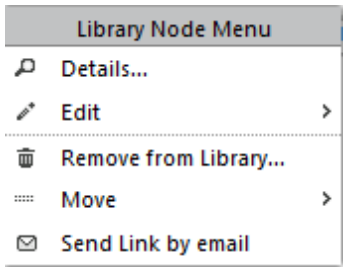
You can delete the entire library any time by clicking on the trash symbol on the right.

8.9.4 Context Menus

On right-click, there are different context menus available.

Library Node Menu

While in the **Overview** or the **Management** tab, right-click any library node to show its context menu.



Library Node Menu

- Select either **Details...** or **Edit | Settings...** to get to the Libraries and Node Settings 2855.
  While on the **Overview** tab, these settings are also accessible via left-click on the node's name.

- **Edit | Rename...** will give you an option to rename the library node quickly.
- **Remove from Library...** will remove this library node from the current library.
  This will not delete any objects in your device tree.

- The **Move | ...** options will move the library node up and down within the library.
- Click on the **Send Link by email** entry to open a new email using your system's standard email client. It will contain a direct link to the page you're currently viewing.

Monitoring Objects Menus

In libraries are the same Context Menus 215 available you already know from the device tree. With one exception: While accessing these menus within libraries, the **Move** and **Delete** options are disabled to avoid accidental changes to your device tree.

8.10 Reports

You can use reports to analyze historic monitoring results over a specified time such as one or more days, one month, or an entire year, and for your system configuration. You can create reports for all or only for certain sensors.

Introduction

PRTG includes a powerful reporting engine for the ad-hoc as well as scheduled report generation in HTML, PDF, CSV, and XML format. This means that you can run reports on demand or on a regular basis (for example, once a day or once a month). Furthermore, you can create reports for a single sensor or for a whole range of sensors. It is also possible to create HTML reports of your system configuration 2865.

The content and layout of the report is controlled by the report template of your choice and is the same for all sensors in a report. The report time that is shown in data tables and data graph legends depends on the system time of your PRTG core server, not on the timezone settings 2980 of the current user account.

Report Sample

The sample report above shows the report data for devices on a local probe. You can see graphs for the preceding week, plus data tables with numeric results.

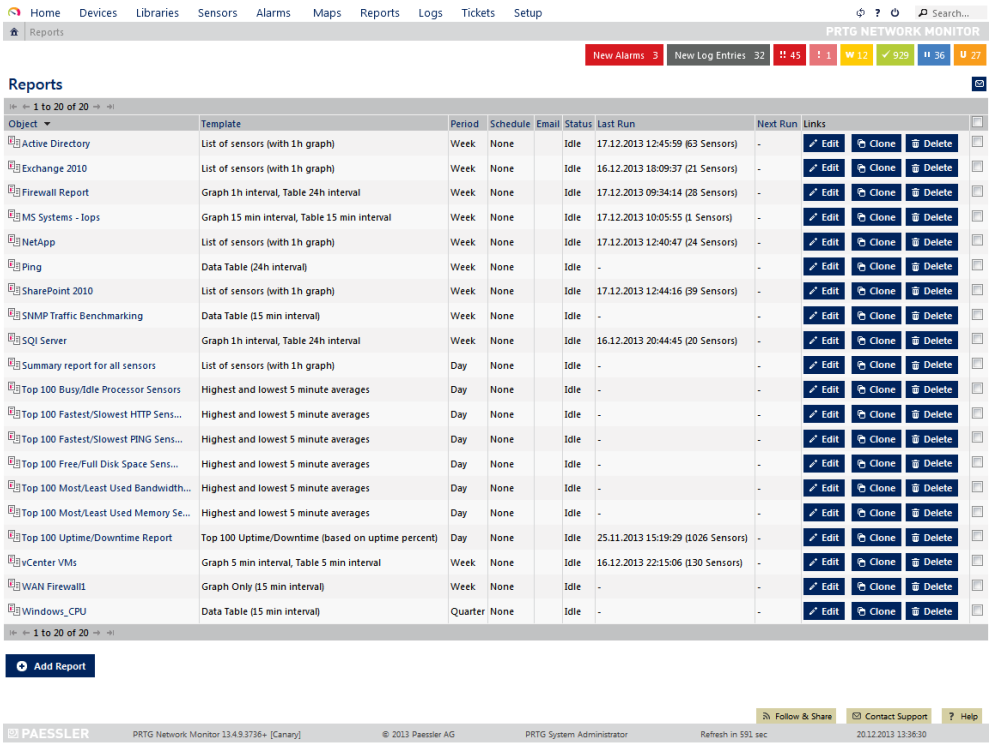
Start Reports

Click the **Reports** entry in the main menu 240 to view or add reports of your monitoring data. Hove over **Reports** to show other menu items. Choose between:

REPORTS

All	Open the Reports overview page where you can view or add reports of your monitoring data.
Add Report	Open an assistant to directly add 2866 a new report.
Select Report ›	Open an existing report. Point to **Select Report** to show other menu items. Follow the menu path (it is specific to your setup) to select a report.
Configuration Reports ›	Create reports for maps, reports, users & user groups, and system configuration to document changes to the configuration. Point to **Reports | Configuration Reports** to see the available configuration reports 2865.

Reports Overview



List of Reports

In the **All** view, you see a list of all existing reports for monitoring data. Every line shows information about one report:

- **Object**: Shows the name of the report.

- **Template**: Shows the name of the template that this report uses.
- **Security Context**: Shows the user account that PRTG uses to run the report.
- **Period**: Shows the time span that the report covers.
- **Schedule**: Shows if you set a schedule to regularly execute the report automatically.
- **Email**: If you set a schedule and an email address in the report settings, this shows the email address to which PRTG sends the report automatically.
- **Status**: Shows the current status of the report.
- **Next Run**: If you set a schedule in the report settings, this shows when PRTG runs the report the next time.
- **Last Run**: If you set a schedule in the report settings, this shows when PRTG ran the report the last time.
- **Number of Sensors in Last Run**: Shows about how many sensors the report includes data.

Using the buttons at the end of a row, you can **Edit**, **Clone**, and **Delete** a report.

Please also see **Working with Table Lists** 207. Additionally, the multi-edit functionality is available. This enables you to change properties of several objects simultaneously via bulk changes. For more details, see the **Multi-Edit Lists** 2814 section.

Click the **Add Report** button to add a new report, or click the name of an existing report to view and edit its settings. You can also run a pre-configured report easily by clicking its name and then using the options in the **Run Now** tab.

For both options, please see the **Reports Step By Step** 2866 section.

You can only run configuration reports 2862 via the main menu.

Working With Reports

For detailed information on how to create, edit, and schedule reports, please see the following sections:

- **Reports Step By Step** 2866
- **View and Run Reports** 2870
- **Report Settings** 2873

Automatic Averaging

For performance reasons, PRTG automatically averages monitoring data when calculating data for large time spans. Data is then averaged regardless of the selected average interval.

TIME SPAN IN REPORT	MINIMUM LEVEL OF DETAIL (AVERAGE INTERVAL)
Up to 40 days	Any
40 to 500 days	60 minutes/1 hour or larger

Reports for time spans of more than 500 days are not possible. If you enter a longer time span, it will automatically be shortened to 365 days.

Configuration Reports

Configuration reports are a special type of reports and show the current PRTG configuration. They are available for **Maps**, **Reports**, **Users & User Groups**, and **System Configuration**. PRTG generates configuration reports and displays them in a new browser window as an HTML page in the common PRTG report style (like, for example, Historic Data Reports 175 of sensors). You can use configuration reports, for example, to file and document changes to the configuration of your PRTG installation.

Configuration reports contain the same information as you can see on the overview pages of Maps 2885, Reports 2862, as well as on the system administration tabs User Accounts 2975 and User Groups 2982. The configuration report **System Configuration** includes the current system administration settings of the tabs User Interface 2943, Monitoring 2955, Notification Delivery 2961, Core & Probes 2967, and Cluster 2992.

Configuration reports are interactive so you can click available links to go to the corresponding webpage in the PRTG web interface.

Related Topics

- Review Monitoring Data 166
- Historic Data Reports 175

8.10.1 Reports Step By Step

To create a new report or to run an existing one, follow the steps in this section. In the PRTG web interface, click on the **Reports** entry in the main menu to show the reports main screen.

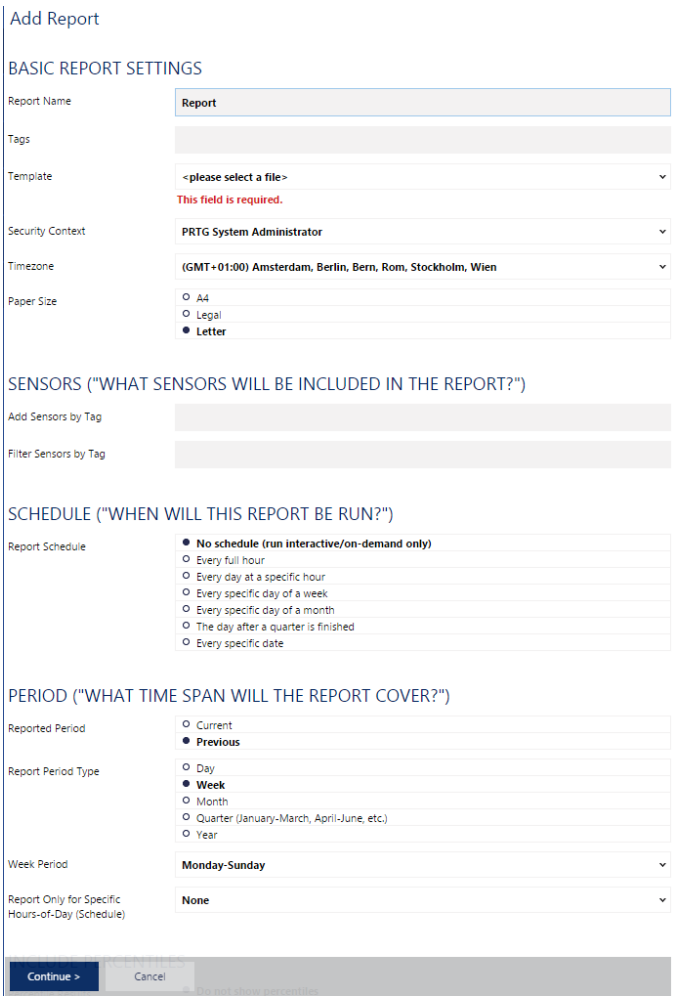
This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

Quick Start: Run an Existing Report

PRTG is delivered with several pre-configured reports. To use one of them, click a report's name in the reports main screen and select the **Settings** tab. The next steps are the same as for completely new reports. Although some settings are already given, we recommend that you check them. For example, check the sensors that are included in the report. For some reports that come with PRTG, there are no sensors added yet. Continue with **Step 3: Define Additional Options** 2867 in this section.

Step 1: Add Report

Click the **Add Report** button to add a new report. An assistant appears where you can define various settings. First, enter a meaningful **Report Name**.



Add Report Assistant

Click here to enlarge: http://media.paessler.com/prtg-screenshots/add_report.png

Step 2: Select a Template

In the **Template** option, select one of the report templates from the list. This defines the overall look of your report and how detailed (regarding the intervals) monitoring data is included. For a detailed description of the available template options, please see the **Report Settings** 2873 section. If you are not sure yet, try a template that appears most suitable to you. You can still change all settings later.

Step 3: Define Additional Options

Select a **Security Context** (best choose **PRTG System Administrator**, if available), your **Timezone**, and the **Paper Size** for PDF generation.

For detailed information, see section **Report Settings** 2873.

Step 4: Select Nodes and Sensors

Choose the sensors you want to include in the report. When running a cluster 116, define the **Cluster Node** the monitoring data is taken from first. Select a specific node from the list. If you select **All nodes**, PRTG creates a report with data from all of your cluster nodes, but only the primary channel of every sensor appears in the report.

Every report shows monitoring results based on sensor data. There are two ways to include sensors in a report: You can either add sensors manually or by tag. In the **Add Sensors by Tag** field, enter one or more tags that match the sensor range you want a report for.

For example, enter the tag bandwidthsensor to include all sensors that measure bandwidth (or select it from the list of tags which PRTG suggests). PRTG provides this tag by default when you add any bandwidth sensor, so the tag typically gathers all bandwidth sensors, unless you configured your system differently. You can enter several tags. Hit the enter key, or insert comma or space after each tag and enter the next one. Use the **Filter Sensors by Tag** field to explicitly filter sensors with certain tags from the bulk of tags or manually selected sensors defined above.

Tagging is a great option to group sensors or other objects. For more information, see the **Tags** 124 section. You can also leave the tag fields empty and only choose specific sensors manually later.

Step 5: Decide on a Schedule and Additional Settings

In the **Report Schedule** section, choose if you want to run the report on a regular basis or on demand only. Also define which time **Period** will be covered by the report, if you want to show percentiles, if you want to generate CSV and XML data files for reports with data tables, and add report comments or special access rights.

For detailed information, please see the **Report Settings** 2873 section.

Scheduled reports are not executed on failover nodes 3212 by default.

Click the **Continue** button to save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Step 6: Check and Adjust the Sensors Included

After saving the settings, switch to the **Sensors Selected by Tag** tab to see a list of all sensors that you added with the tag(s) you defined in step 4. To change tags, go back to the **Settings** tab. You can additionally add sensors manually. To do so, switch to the **Select Sensors Manually** tab. The final report shows sensors from both manual and by tag selection.

See section **Report Settings** 2882 for detailed information.

Step 7: Run Report

Switch to the **Run Now** tab, select a period, and in the **Processing Options** select **View Report as HTML**. Click the **Run Report** button. PRTG generates the report in a new browser window or tab immediately. Depending on the number of selected sensors and the used template, it may take a few minutes until you see the report. If you do not want to wait, close the newly opened browser window or tab and select a PDF option in the **Processing Options**. Click the **Run Report** button again. The report is then generated in the background and you get a **ToDo ticket** or email once it is finished.

For large PDF reports, PRTG automatically splits the output into separate files to avoid huge PDF files. You can change the number of sensors that PRTG includes into each PDF file by editing the report templates manually. For details, see this Knowledge Base article: Can I change the number of PDFs created by a report?

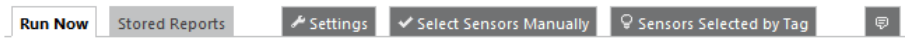
More

Knowledge Base: Can I change the number of PDFs created by a report?

- https://kb.paessler.com/en/topic/11863

8.10.2 View and Run Reports

In the web interface, click the **Reports** entry in the main menu to show the reports main screen. Click a report's name to select it. Using the reports tabs you can access all functionalities and settings for this report. Click the **Go to all reports** button at the bottom of the page to return to the list of **Reports**.



Report Tabs

This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

Run Now

On the **Run Now** tab you can execute a report immediately with the settings configured.

RUN REPORT "[Name]"

Report for	Define the time span covered by the report. Choose between: ▪ **Current Period**: Use monitoring data of the current period. The actual time span depends on the report period type defined in the report's settings. It can be today, this week, this month, or this year. ▪ **Previous Period**: Use monitoring data of the last period. The actual time span depends on the report period type defined in the report's settings. It can be yesterday, last week, last month, or last year. ▪ **Select a Period**: Use monitoring data of a period other than current or previous. Select below. ▪ **Select Date Range Manually**: Define a custom time span for the monitoring data that will be used. Set start and end date below.
Date Range	This selection is only visible if you enable the period option above. From the list, select a data range for which PRTG will generate the report. The shown time spans depend on the available monitoring data and on the report period type defined in the report's settings. It can be days, weeks, months, or years.
Start Date	This selection is only visible if you enable the date range option above. Define the begin of the time span for which PRTG will generate the report. Use the date time picker to enter the date and time. Make sure you define a valid period.

RUN REPORT "[Name]"

End Date	This selection is only visible if you enable the date range option above. Define the end of the time span for which PRTG will generate the report. Use the date time picker to enter the date and time. Make sure you define a valid period.
Quick Range	This selection is only visible if you enable the date range option above. Choose between different pre-defined ranges by simply clicking the desired range. Each click changes the **Start** and **End Date** fields above accordingly.

PROCESSING OPTIONS

File Format and Delivery

Define how you want to view the report. Choose between:

- **View Report as HTML**: Directly view the report in your web browser. PRTG loads it in a new browser window or tab.
- **Create and store PDF and data files (available for templates with data tables)**: Create a PDF file and, depending on the **Data Files** settings 2873 of the report, CSV and XML files of the report and store them. Once finished, you will find it in the **Stored Reports** tab and a ToDo ticket 201 will be created. By default, PRTG sends out a notification email to the administrator in this case.
- **Create PDF and data files (available for templates with data tables), store them, and send by email**: Create a PDF file and CSV and XML files of the report, store the files, and send them via email once finished.

CSV and XML data files are only generated for report templates that include data tables.

To create PDF files, ensure the print spooler service is running on the system with your PRTG server.

Certain special characters, for example, 4-byte unicode characters, may not be displayed correctly in PDF reports. As workaround, generate an HTML report and save it as PDF.

For large PDF reports, PRTG automatically splits the output into separate files to avoid huge PDF files. You can change the number of sensors that PRTG includes into each PDF file by editing the report templates manually. For details, see this Knowledge Base article: Can I change the number of PDFs created by a report?

PROCESSING OPTIONS

Target Email Address	This setting is only available if you define above to send the report by email. Enter a valid email address to which PRTG will send the report. You can change the configuration for outgoing emails in the System Administration—Notification Delivery 2961 settings.
Compression	This setting is only available if you define above to send the report by email. Define if you want to compress the attached report files before sending. Choose between: ▪ **Send files uncompressed**: PRTG will not compress the report files before they are sent by email but send the files in their original size. ▪ **Send all in one ZIP file**: PRTG will compress the report files to a ZIP file before they are sent by email.

Click the **Run Report** button to start report generation. Depending on the number of selected sensors, this may take a while. If you experience a long waiting time when generating HTML reports for immediate view, please consider using one of the PDF options. You can then view the report as soon as it has finished.

Any sensor graph in your report will only show the channels that are enabled via the **Show in Graphs** option in the Sensor Graph Settings 2782 of the corresponding sensor.

Reports cannot show uptime or downtime data for the Sensor Factory Sensor 1438.

Stored Reports

In the **Stored Reports** tab you can view all PDF reports and data files created in the past. Click a name to open the report. Reports are stored until they are deleted according to the data purging settings of your PRTG configuration. You can set data purging limits for reports in the System Administration—Core & Probes 2972 settings.

Other Tabs

For all other tabs, please see the Report Settings 2873 section.

More

Knowledge Base: Can I change the number of PDFs created by a report?

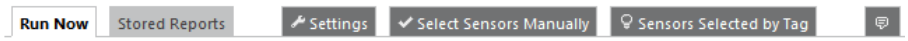
- https://kb.paessler.com/en/topic/11863

Knowledge Base: Why is there missing data in historical data reports?

- https://kb.paessler.com/en/topic/61382

8.10.3 Report Settings

In the web interface, click the **Reports** entry in the main menu to show the reports main screen. Click a report's name to select it. Using the reports tabs you can access all functionalities and settings for this report. Click the **Go to all reports** button at the bottom of the page to return to the list of **Reports**.



Report Tabs

This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

Run Now

On the **Run Now** tab you can execute a report immediately with the settings that you configured before.

See section View and Run Reports 2870 for details.

Stored Reports

On the **Stored Reports** tab you can view reports created in the past.

See section View and Run Reports 2872 for details.

Settings

Click the **Settings** tab to open the settings of a report.

BASIC REPORT SETTINGS

Report Name	Enter a meaningful name to identify this report. The name of the report is used in reports lists 240 and as headline of generated reports.
Tags	Enter one or more tags, separated by space or comma. For example, you can use tags later to search for the report. Tags are not case sensitive.

BASIC REPORT SETTINGS

Template

Select a template for the report. The template defines the overall look of your report and in which detail (interval) the report shows monitoring data. PRTG includes several report templates out of the box. You can choose from templates in the following categories:

- **Data Table Only**: Create a report with data tables only. Choose from several intervals. Reports with this template also generate data files (CSV and XML) if set in the **Data Files** section of the report.
- **Graph Only**: Create a report with graphs only. Choose from several intervals. Reports with this template cannot generate data files (neither CSV nor XML).
- **Graph with Data Table**: Create a report with graphs and data table. Choose from several intervals. Reports with this template also generate data files (CSV and XML) if set in the **Data Files** section of the report.
- **List of Sensors**: Create a report in a compact sensor list style. This is available with and without graphs. Reports with this template cannot generate data files (neither CSV nor XML)
- **Top 10 Uptime/Downtime**: Create a report with up to 10 objects with the highest uptime and downtime each. You can choose between data in percent and hours. Reports with this template cannot generate data files (neither CSV nor XML)
- **Top 100 Highest and Lowest**: Create a report with up to 100 objects with the highest and lowest average values. Choose from different intervals. Reports with this template cannot generate data files (neither CSV nor XML)
- **Top 100 Uptime/Downtime**: Create a report with up to 100 objects with the highest uptime and downtime each. You can choose between data in percent and hours. Reports with this template cannot generate data files (neither CSV nor XML)

Monitoring data within an interval is averaged. See also the comment on data averaging in the **Reports** 2864 (Automatic Averaging) section.

For information on how to modify templates, see this Knowledge Base article: How do I modify PRTG's report templates?

Security Context

Define the user account 2975 that you want to use for access to your monitoring data. The report only contains objects which the selected user 129 is allowed to view.

Choose a PRTG user from the list. The available users depend on your configuration. By default, this is the user that created the report. PRTG System Administrator users can change this setting.

BASIC REPORT SETTINGS

Timezone	Define the time zone to use for all date-specific settings in this report (see below 2878). Choose a time zone from the list.
Paper Size	Define the paper size in which PDF reports are created. Choose between: ▪ **None**: Do not specify a paper format. The size is set automatically. ▪ **A4**: Use German DIN A4 format. ▪ **A3**: Use DIN A3 format. ▪ **A2**: Use DIN A2 format. ▪ **Legal**: Use North American legal paper format. ▪ **Letter**: Use North American letter paper format. ▪ **Ledger**: Use North American ledger paper format.
Orientation	Define the page orientation for the data in PDF reports. Choose between: ▪ **Portrait**: Use portrait mode for the page orientation. ▪ **Landscape**: Use landscape mode for the page orientation. The landscape format is designed to properly show data tables of sensors with many channels. Other parts of the report will remain in portrait mode and do not re-size to the landscape format.

SENSORS ("WHAT SENSORS WILL BE INCLUDED IN THE REPORT?")

Cluster Node	This field is only visible when you run PRTG in **Clustering** 116 mode. Define the cluster node from which the report will take monitoring data. Choose a cluster node from the list. The available options are specific to your configuration. By default, the current master node is set. Select **All nodes** to create a report with data from all of your cluster nodes. A report for all nodes includes data of the primary sensor channels only, not for other sensor channels. Be careful with big reports for all nodes because the report generation may slow down significantly.

SENSORS ("WHAT SENSORS WILL BE INCLUDED IN THE REPORT?")

If you select a failover node, report and data files will not show data from the local probe or from a remote probe and might be empty or show "0" values.

You can generate CSV and XML data files only for a single failover node. If you choose the option **All nodes**, the report will not create data files!

Add Sensors Manually

If you want to manually choose the sensors included in this report, please save settings and switch to the **Select Sensors Manually** 2882 tab.

Add Sensors by Tag

Define the sensors included in this report by tag 124. Enter one or more tags. The report covers all sensors that have at least one of the tags. Please enter a string or leave the field empty.

You can also use plus (must have) and minus (must not have) signs to categorize tags, for example, +snmp;-wmi (must have the tag snmp and must not have the tag wmi). See the section **Tags** 124 for details.

Tags are inherited 124 automatically. So, for example, if you enter the tag of a group 119 here, the report will include all sensors within this group. For detailed information, see the **Inheritance of Settings** 122 section. For sensors you add by tag, the report includes all sensor channels automatically, except if you run a PRTG cluster 116 and select **All nodes** in the **Cluster Node** selection above.

Filter Sensors by Tag

Filter the included sensors further. This option works best in combination with manually added groups and devices. From the sensors that are implicitly added because of their parent objects, the report includes only the ones with the tags you enter here.

Enter one or more tags to include sensors in the report. Confirm a tag with enter, space, or comma key. Please enter a string or leave the field empty.

You can also use plus (must have) and minus (must not have) signs to categorize tags, for example, +snmp;-wmi (must have the tag snmp and must not have the tag wmi). See the section **Tags** 124 for details.

SCHEDULE

Report Schedule	Define at which time you want to run the report. Choose between: ▪ **No schedule (run interactive/on-demand only)**: Only use the options on the **Run Now** tab to start generating this report manually. ▪ **Every full hour**: Run this report every 60 minutes. ▪ **Every day at a specific hour**: Run this report every 24 hours. ▪ **Every specific day of a week**: Run this report every 7 days. Specify the day below. ▪ **Every specific day of a month**: Run this report on a specific day every month. Specify below. ▪ **The day after a quarter is finished (i.e. at 1. April for the 1. January - 31. March Quarter)**: Run this report for every quarter of the year. ▪ **Every specific date**: Run this report on a specific date every year. Specify below.
Specify Hour	This setting is only visible if you select a specific hour above. From the list, select the hour you want to run the report at. PRTG automatically chooses a suitable time within this hour, usually at the beginning of it.
Specify Day	This setting is only visible if you select the day of week or day of month option above. From the list, select a day of week or a date of the month you want to run the report. If you select **Last**, the report will always run on the last day of the month, regardless of how many days the month has. If you select a date that does not exist in every month, for example, February 31st , PRTG will automatically run the report on the last day of this month.
Specify Date	This setting is only visible if you select the specific date option above. Enter a valid date in the format **DD.MM.**, for example, 31.12. The report runs annually on this date.
Scheduled Processing	This setting is only visible if you select one of the schedule options above. Define what to do with a finished report. Choose between: ▪ **Save report to disk and send it by email**: Create a PDF file and, depending on the **Data Files** setting, data files of the report, store it, and send it via email. You find the report in your emails and on the **Stored Reports** tab. Define an email address below.

SCHEDULE

- **Save report to disk only**: Create a PDF file and, depending on the **Data Files** 2881 setting, data files of the report and store it. Once finished, you find them on the **Stored Reports** tab. You receive also a ToDo ticket 201 from PRTG. By default, PRTG sends out a notification email to the administrator in this case.
- **Send report by email only**: Create a PDF file and, depending on the **Data Files** 2881 setting, data files of the report and send them via email once finished. With this option the report is not permanently stored in PRTG. Define an email address below.

For large PDF reports, PRTG automatically splits the output into separate files to avoid huge PDF files. You can change the number of sensors that PRTG includes into each PDF file by editing the report templates manually. For details, see this Knowledge Base article: Can I change the number of PDFs created by a report?

Certain special characters, for example, 4-byte unicode characters, may not be displayed correctly in PDF reports. As workaround, generate an HTML report and save it as PDF.

Email Address

This setting is only visible if you select a send by email option above. Enter a valid email address to which PRTG sends the report. To enter more addresses, separate them by comma. PRTG sends a message with all recipients in the "To" field of the email.

You can change the configuration for outgoing emails in the **System Administration—Notification Delivery** 2961 settings.

Send to User Group

This setting is only visible if you select a send by email option above. From the list, choose a user group to send an email with the report to all members of this group. You can edit user groups in **System Administration—User Groups** 2982.

If you define individual email addresses (see field above) and a user group, PRTG will send the report to the individual email addresses as well as to the members of the selected user group. In both cases, PRTG will send one message with all recipients in the "To" field of the email.

Compression

This setting is only visible if you select a send by email option above. Define if PRTG will compress the attached report files before sending them out. Choose between:

- **Send files uncompressed (default)**: PRTG sends the report files by email in their original size.
- **Send all in one ZIP file**: PRTG will compress the report files to a ZIP file before they are sent by email.

PERIOD

Reported Period	Define the time span the report covers. Choose between: ▪ **Current**: Use monitoring data of the current period. Define the period type below. ▪ **Previous**: Use monitoring data of the last period. Define the period type below.
Report Period Type	Define the type of period you want to create a report for. Choose between: ▪ **Day** ▪ **Week** ▪ **Month** ▪ **Quarter (January-March, April-June, etc.)** ▪ **Year** Depending on your selection, different period selections are shown below.
Day Period	This setting is only visible if you select day period type above. Define the hours when a day starts and ends. Choose from the list of hours. Default setting is **0:00-23:59**.
Week Period	This setting is only visible if you select week period type above. Define when the week starts and ends. Choose between: ▪ **Monday-Sunday**: A reported week starts on Monday. ▪ **Saturday-Friday**: A reported week starts on Saturday. ▪ **Sunday-Saturday**: A reported week starts on Sunday.
Month Period	This setting is only visible if you select month period type above. Define when the month starts and ends. Choose between: ▪ **1.-last day**: A reported month starts on the first and ends on last of the month. ▪ **15.-14.**: A reported month starts on 15th and ends on 14th of the month.
Year Period	This setting is only visible if you select year period type above. Define when the year starts and ends. Choose between: ▪ **1/1-12/31**: A reported year starts on January 1st. ▪ **7/1-6/30**: A reported year starts on July 1st.

PERIOD

Report only for specific hours-of-day (Schedule)	Include certain time spans within the defined period only. If a schedule is selected, the report will include only monitoring data for specified hours or weekdays within the defined period. Select **None** to include all available monitoring data in the report, or choose a schedule. For example, select the schedule **Weekdays** to exclude all weekends from the report. The available schedules depend on your configuration. For more information, please see the **Account Settings—Schedules** 2938 section.

INCLUDE PERCENTILES

Percentile Results	Define if you want to include an additional percentile calculation 3194 of your data in the report. Choose between: ▪ **Do not show percentiles:** PRTG does not use a percentile formula to calculate your monitoring results. It will show only the standard values. ▪ **Show percentiles**: PRTG adds a column to the result data tables, which shows percentiles for every sensor channel. Percentiles are not available for all report templates. If a template does not support percentiles, they will simply not show up in the report, even when you enable this setting. Likewise, percentiles are not available in a cluster setup if you choose the option **All Nodes** in the **Cluster Node** setting in the sensor section above.
Percentile Type	This setting is only visible if you select **Show percentiles** above. Enter the percentile type you want PRTG to use for the calculation. If you choose, for example, to calculate the 95th percentile, enter "95" here and 5 % of peak values will be discarded. Please enter an integer value.
Percentile Average Interval	This setting is only visible if you select **Show percentiles** above. Enter a value to define the averaging interval on which PRTG bases the percentile calculation. The default value is 300 seconds (5 minutes). This means that PRTG takes 5 minute averages as basic values for the percentile calculation. Please enter an integer value.

INCLUDE PERCENTILES

Percentile Mode

This setting is only visible if you select **Show percentiles** above. Choose the mode for percentile calculation:

- **Discrete**: PRTG takes discrete values to calculate percentile results.
- **Continuous**: PRTG interpolates between discrete values and bases the calculation on interpolated values.

DATA FILES

CSV / XML Files

Define if you want to generate CSV and XML files for data tables in the report in addition to the PDF. Choose between:

- **Do not include data files**: PRTG will not generate CSV or XML files for the report but only a PDF file.
- **Include CSV files only (available for templates with data tables)**: PRTG will generate and store CSV files in addition to the PDF. CSV data files are only generated if the report uses a template with data tables.
- **Include XML files only (available for templates with data tables)**: PRTG will generate and store XML files in addition to the PDF. XML data files are only generated if the report uses a template with data tables.
- **Include all data files (available for templates with data tables)**: PRTG will generate and store CSV and XML files in addition to the PDF. CSV and XML data files are only generated if the report uses a template with data tables.

If you run PRTG in a cluster, the report will not generate data files if you select **All nodes** in the sensors selection 2875 above. Please specify a single failover node to get data files.

REPORT COMMENTS

Introduction

Enter a custom text that will show up on the first page of the report. Please enter a string or leave the field empty.

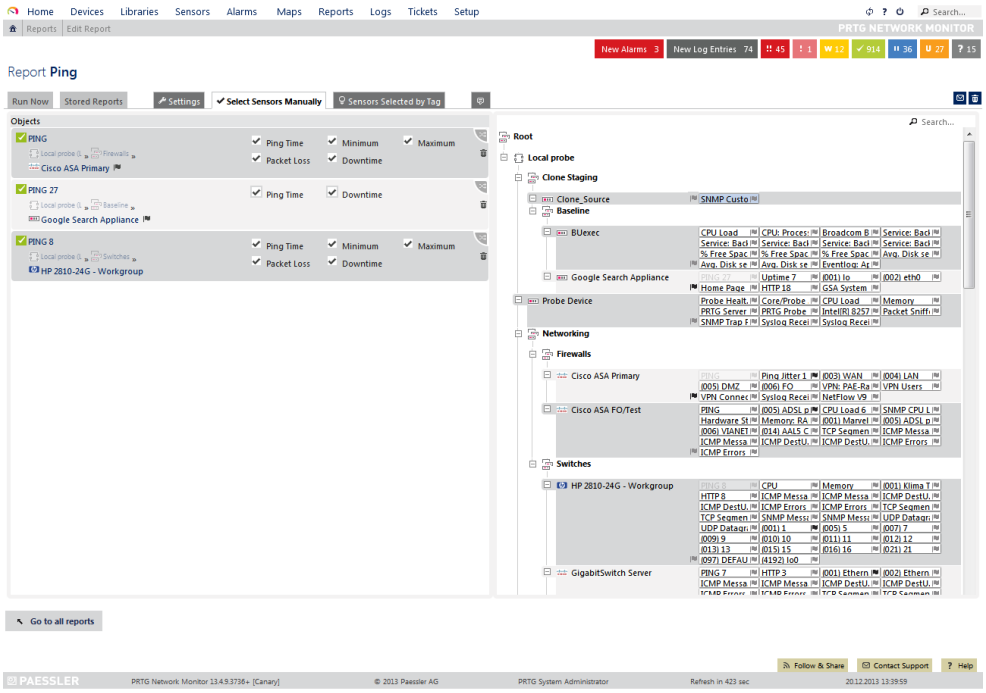
REPORT COMMENTS	
Footer Comments	Enter a custom text that will show up at the end of the report. Please enter a string or leave the field empty.

ACCESS RIGHTS	
User Group Access	Define which user group(s) will have access to the object that you are editing. A table with user groups and rights is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object does not show up in lists. ▪ **Read**: Users in this group can see the object and review its settings. ▪ **Write**: Users in this group can see the object, as well as review and edit its settings. However, they cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, as well as review and edit its settings as well as edit access rights. You can create new user groups in the **System Administration—User Groups** 2982 settings.

Click **Save** to save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Select Sensors Manually

Click the **Select Sensors Manually** tab to manually choose sensors that you want to include in the report. You see a split screen: On the left side, there is a list of objects that the report already contains (empty in the beginning), and on the right side, you see a less colorful view of your device tree, like on the Management 292 tab in the device tree. You can add objects to the report using drag and drop.



Manual Selection for Reports

- **Add Items**
  From the device tree on the right side, drag objects and drop them on the list on the left side. This can be entire probes, groups, devices, or single sensors. Each dropped object is added immediately as a new list item. Repeat this procedure as often as you wish until you have added all desired items to the report.
  The objects you drop on the left side are always added to the end of the list, you cannot add objects directly in another order.

- **Select Sensor Channels**
  If you add a sensor to the selection, you can specify the sensor channels that the report will include. By default, all channels are selected. To exclude a channel from the report, remove the check mark in front of a channel name.
  If you run a PRTG cluster 116, you can only choose between single channels if you select one specific **Cluster Node** in the report settings. If you select **All nodes** the report's **Cluster Node** setting, the channel selection is not available and the report contains only the primary channel of each sensor.

- **Change Order**
  You can change the order of manually selected objects on the left side with drag and drop. Each item you add appears at the end of the list by default. To change the order, point to the drag and drop symbol (two arrows) in the upper right corner of a selected item, drag it to the desired position, and drop it there.

- **Remove**
  To remove any objects from the report, click the trash can symbol next the respective list item, or select several list items while holding down the Ctrl key and click the green trash symbol appearing at the top of the list.

Your selection is saved automatically, and there is no undo function.

The final report will include both sensors selected manually and those selected by tag.

Sensors Selected by Tag

Click the **Sensors Selected by Tag** tab to view all sensors that are added to the report depending on the **Add Sensors by Tag** setting of the report. In the table list 207, you see all sensors that you added to the report by their respective tags. This is for your information only, you cannot change sensors here.

However, you can switch to the **Settings** tab of the report and change the tags that the report uses to include sensors. Additionally, you can also exclude sensors with certain tags there. The final report will include both sensors selected manually and those selected by tag.

For sensors that you add by tag, all sensor channels are included in the report automatically, except you use a PRTG cluster 116 and select **All nodes** in the **Cluster Node** selection of the report. In this case, the report includes only the primary channel of each sensor.

The final report will include both sensors selected manually and those selected by tag.

Comments

On the **Comments** tab you can enter free text for each object. You can use this function for documentation purposes or to leave information for other users.

Click **Save** to save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

More

Knowledge Base: Can I change the number of PDFs created by a report?

- https://kb.paessler.com/en/topic/11863

Knowledge Base: How do I modify PRTG's report templates?

- https://kb.paessler.com/en/topic/263

Knowledge Base: How can I show full channel names below report graphs?

- https://kb.paessler.com/en/topic/58913
- Manual Section: **Calculating Percentiles** 3194

8.11 Maps

With the **Maps** feature (some people might call this 'dashboards') you can create web pages with up-to-the-minute monitoring status information in a customizable layout. Using this unique concept, you can also make your overview pages of live data publicly available, if you like.

Example of a PRTG Map

In this section:

- Introduction 2885
- Start Maps 2886
- Maps Overview 2887
- Maps Rotation 2887
- Working with Maps 2889

Introduction

There are countless possibilities for the implementation of maps. For example, you can use this feature to:

- Create network maps with status icons for each device on the map.
- Create quick views of your network that can be shown on network operations center screens.

- Create a quick network overview for publishing on the Intranet, allowing at-a-glance information for management of other employees.
- Create a custom view of the most important sensors in your monitoring setup.
- Create Top 10 lists of the sensors of a specific group or device.

Technically, a map is a usual HTML web page. You can build a schema of your network by choosing from hundreds of device icons and connect them with lines. A map can consist of the following elements:

- A set of map items, which can include device icons, sensor status icons, graphs, data tables, lists of sensors, connection lines, geographical maps, or custom HTML code.
- An optional background image (a JPG, PNG, or GIF file, for example, your company logo, or a graphical view of your network).

You can also specify the size of the map. Using the AJAX-based map editor, you can place the items anywhere on the map, and you can also change their size. Each map has a unique URL which you can use to link to the map. Users who want to access the map either need an account in your PRTG installation, or can access a public URL of the map if you allow the **Public Access** feature. Public maps contain a unique **Map ID** access key in the URL to block unwanted visitors.

PRTG comes with several pre-configured standard maps that you can use right away. You can also change or delete them, if you like. The following maps are automatically created when you install PRTG for the first time (visible for the PRTG System Administrator 129 user):

- **Sample Dashboard**: By default, this map shows a graphical structure of your device tree, the sunburst view 157 of your device tree, a list of alarms 190, a geo map 2824, and more. This sample map has a 5***** priority 211 so you can also open it under **Home** in the main menu 231. To not show it in the main menu, define a lower priority.
- **Magic Map**: By default, this map shows the sunburst view 157 of your device tree with several graphics that demonstrate customization capabilities of the maps feature.

Start Maps

Click the **Maps** entry from the main menu 240 to view or add custom views of your network's status and monitoring data. Hover over **Maps** to show other menu items. Choose between:

MAPS	
All	Open the Maps overview page where you can view or add custom views of your network's status and monitoring data.
Add Map	Open an assistant to directly add 2890 a new map.
Select Map ›	Open an existing map. Hover over **Select Map** to show other menu items. Follow the menu path (it is specific to your setup) to select a map.

Maps Overview

In the **All** view, you see a list of all existing maps. Using the links next to a map name, you can do the following:

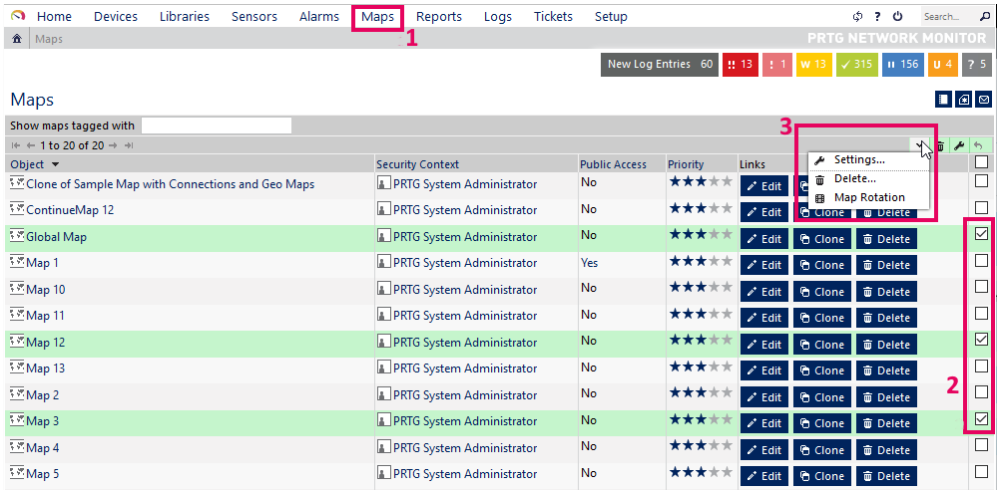
- Click the name of a map to view it.
- Click the **Edit** button to adjust the settings of this map.
- Click the **Clone** button to create an exact copy of this map. As soon as you click this, the map is cloned and the cloned map's settings are shown.
- Click the **Delete** button to remove this map.
- Click the **Add Map** button to add a new map.
- Define the priority 211 of a map. Maps with a 5***** priority appear in the main menu bar 231 under **Home** for direct selection (up to 10 entries).

Please also see **Working with Table Lists** 207. Additionally, the multi-edit functionality is available. This enables you to change properties of several objects simultaneously via bulk changes. For more details, see the **Multi-Edit Lists** 2814 section.

Map Rotation

The Map Rotation feature in PRTG allows you to show several maps or dashboards rotating on one page. Map rotation makes it possible to show different information on one screen based on time. You can compare this with a slide show. Follow the steps below to configure your own map rotation.

1. Open the **Maps** overview page from the PRTG main menu bar 231.
2. Select the maps that you want to rotate using the checkboxes.
3. The **Multi-Edit** 2814 menu appears.
4. Click **Map Rotation** in the multi-edit menu.
5. That's all: PRTG will show the selected maps in rotation on a new page.
   This requires login credentials for PRTG.
6. You can change the time until a new map appears with the arrows symbol in the lower right corner. Hover over the arrows symbol and choose between **10s**, **30s**, **60s** (seconds), **10m** (minutes), and **Refresh** now.



Start Map Rotation

Public Map Rotation

You can also set up a **public map rotation** that you can use without login credentials. For this purpose, you have to create a custom URL that defines which maps will publicly rotate. The public map rotation URL has this format: the address of your PRTG server, followed by **/public/mapshow.htm?ids=**, followed by map IDs and secret keys.

1. **Allow public access** in the settings 2904 of the maps you want to rotate.
2. Find the map IDs and secret keys to add them to the URL that opens the public map rotation.
   a. To find the ID of a map, open the map with your web browser. The map ID is included in the URL of the map as value of the parameter **id**, for example, https://<yourprtgserver>/map.htm?id=**2124**, where the number **2124** is the needed ID.
   b. To find the secret key of a map, open the settings of the map, make sure you have selected a public access option 2904, and copy the entry of the **Secret Key** field.
3. Connect each map ID with the secret key of the same map using a colon, in this format: **mapid:secretkey**
4. Add all IDs with their secret keys to the URL for the public map rotation. Separate each mapid:secretkey token from the next mapid:secretkey token with a comma.
5. The complete URL has this format: **https://yourprtgserver/public/mapshow.htm?ids=mapid1:secretkey1,mapid2:secretkey2,mapid3:secretkey3**
   This is an example URL for public rotation of two maps:
   https://prtg.example.com/public/mapshow.htm?ids=9507:4049BEA1-B89C-4B5D-ACC4-3C8E00566EB8,9358:718D3CE1-DF00-4B92-AE8A-E0253B912C37
6. Open the created URL with your browser and PRTG will start the public map rotation.
7. You can change the time until a new map appears with the arrows symbol in the lower right corner. Hover over the arrows symbol and choose between **10s**, **30s**, **60s** (seconds), **10m** (minutes), and **Refresh** now.

Working with Maps

For detailed information on how to create and edit maps, and to learn how to make them accessible to others, please see the following sections.

- Maps Step By Step 2890
- Map Designer 2893
- Maps Other Settings 2902

8.11.1 Maps Step By Step

To create a new map, follow the steps in this section. In the web interface, click **Maps** in the main menu bar 231 to show the maps main screen.

This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

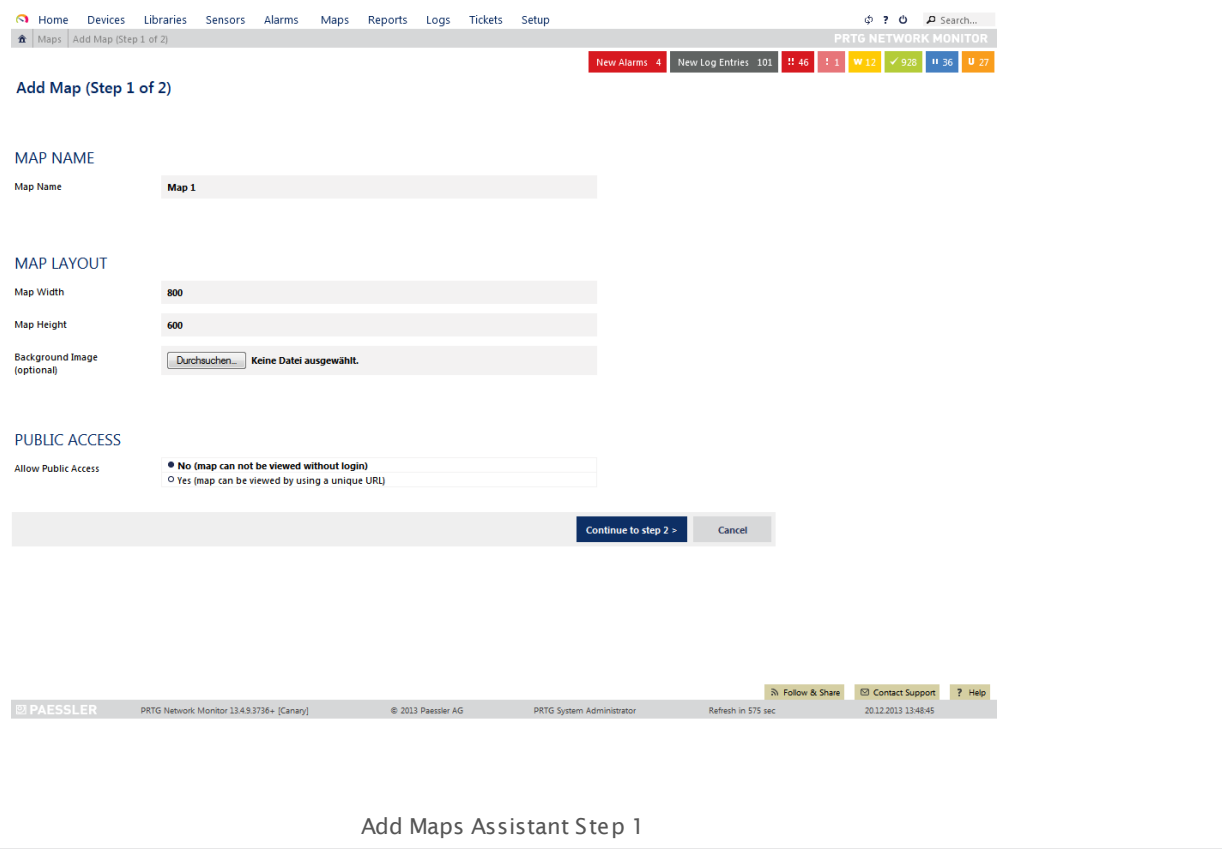
In this section:

- Step 1: Add Map 2890
- Step 2: Add Map Items 2891
- Step 3: View and Share 2891

Step 1: Add Map

Click the **Add Map** button. An assistant appears. Enter a **Map Name** and define **Map Layout** settings (size and optionally a background image). in the **Public Access** section, define the accessibility to your map without login.

For detailed information, see **Maps Settings** 2902 section (Settings).



Add Maps Assistant Step 1

Step 2: Add Map Items

- Click the **Continue to step 2** button to open the **Map Designer**.
- Select an object from the device tree on the left.
- Drag&drop an object from the items list on the right to the main window of the Map Designer.
- The item will immediately appear on the map.
- Define further properties of the item: mark it in the main window of the Map Designer and see section **Properties** on the right. **Save** your changes to the properties.
- Repeat this procedure as often as you wish until you have added all desired items to the map.
- Drag items to change their position. You can also draw connection lines between items and edit the properties of existing items.

For detailed information, see **Map Designer** 2893 section.

Step 3: View and Share

Click the **View Map** tab to see your map. Later, PRTG will show it the way you see it there. If available for an object, you can click most object names as well as all sensors. It depends on the access rights of the object and the currently logged in user account if you can get more detailed information about the object or an error message indicating insufficient access rights.

Click the **Get HTML** tab to get the direct URL of your map that you can share with others.

For detailed information, see **Maps Settings** 2905 section.

The single map items will refresh in the refresh interval you define for this map when viewing it. Hover over the arrows symbol in the lower right corner to define the interval.

Create Advanced Maps

PRTG Maps provide the possibility to publish data from various sources. Besides using the default map items you can create a completely individual map with desired data in any design. See the following articles for more details.

- **Adding External Information to PRTG Maps:** https://kb.paessler.com/en/topic/9263
  Embed information from other sources than PRTG into your map using IFRAME or IMG, for example, weather and traffic maps or webcam images.
- **Map Rotation and Public Map Rotation:** **PRTG Manual: Maps** 2887
  Show several maps rotating on one page just like in a slide show.
- **Nest Maps:** https://kb.paessler.com/en/topic/71833
  Display and link multiple maps within on map.

- **Accumulating Sensor Data with HTTP XML/REST Value Sensor:** https://kb.paessler.com/en/topic/71932
  Display sensor data from various PRTG installations in a single map using the **HTTP XML/REST Value sensor** 976.
- **Use your Own Images in PRTG Maps:** https://kb.paessler.com/en/topic/8043
  Add any browser-compatible image to your map.
- **Adding and Customizing Map Objects:** https://kb.paessler.com/en/topic/1703
  Create customized or completely new map objects.
- **Custom Map Objects for PRTG Maps:** https://kb.paessler.com/en/topic/61263
  Find read-to-use custom map objects and other map customizations.

More

Video Tutorial: How to Create Maps in PRTG

- https://www.paessler.com/support/videos/prtg-advanced/creating-maps

8.11.2 Map Designer

Use the **Map Designer** to create a map web page representing your network.

This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

In this section:

- Use a Proper Browser 2893
- Basic Design Concept 2893
- Device Tree Selection 2894
- Properties Selection 2895
- Edit Existing Map Items—Properties Box 2898
- Edit Existing Map Items—Hover Icons 2898
- Edit Existing Map Items—Using Cursor Keys 2899
- Draw Connection Lines Between Items 2899
- Snap To Grid 2900
- Undo and Redo 2900
- More 2901

Use the Proper Browser

Due to the map designer's extensive scripting capability, it is important that you use a compatible browser when editing maps. We recommend that you use Google Chrome 57 or later (recommended). You can also use Mozilla Firefox 52 or later or Microsoft Internet Explorer 11. The map designer is not fully compatible with earlier versions of Internet Explorer or Opera browsers.

Basic Design Concept

Click the **Map Designer** tab to open the editor. It might take a few moments to load. Here, you can create your map by adding or changing items. The designer screen consists of three main parts: The **Device Tree** on the left side, the current **Map** in the middle, and the **Properties** on the right side.

If you get unresponsive script warnings, please see this Knowledge Base article: Why does my browser show an unresponsive script warning while loading the Map Designer?

Map Designer

Each map item takes attributes from both selections.

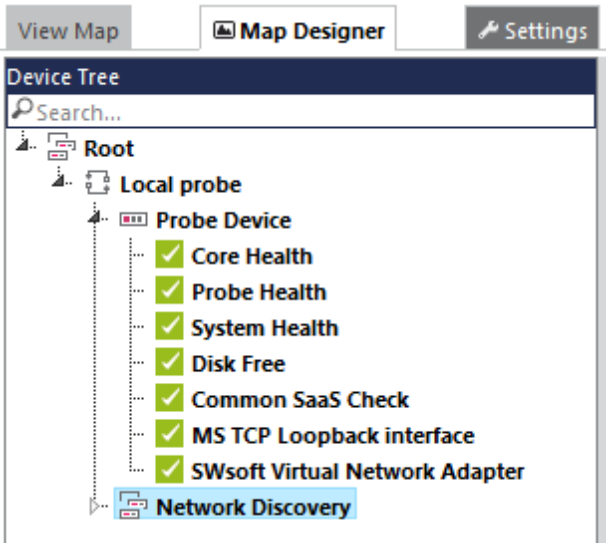
- **Device Tree** (left): Select the monitored object whose data you want to show on the map.
- **Properties** (right): Define how to show the map item.

Simply drag&drop any object from either side onto the map, or double-click on an object. You will always see all changes immediately.

Device Tree Selection

Use the **Device Tree** to select the monitored object whose data you want to show on the map (this can be a probe, a group, a device, or a single sensor). To find the desired object you have the following options:

- Use the arrow symbols at the beginning of each line to open nodes in the device tree and show objects below probes, groups, and devices.
- Enter a few characters into the **Search** box in the upper left corner to search for names (or part of names) of objects in your configuration. You will see the search results immediately. Click the red **x** icon to clear your search.



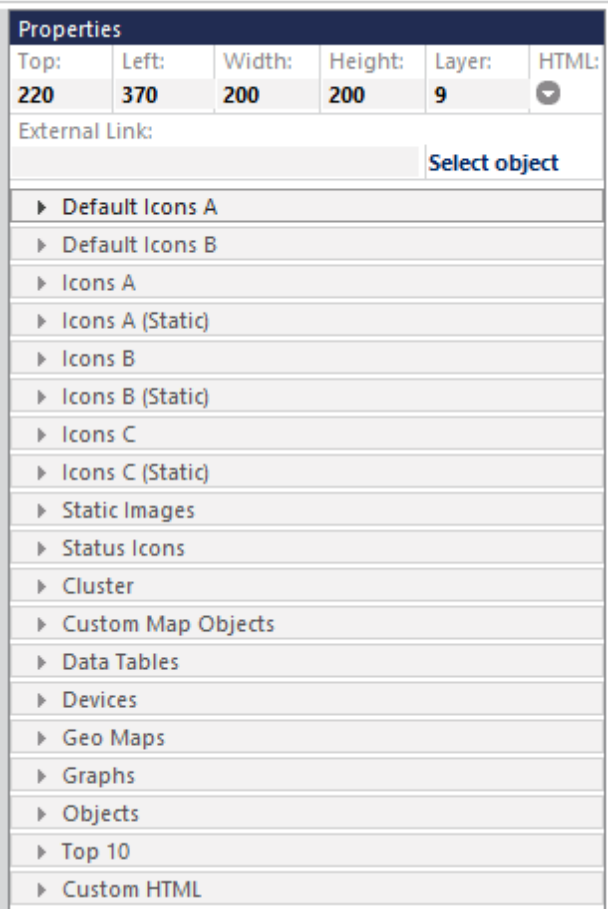
Device Tree Selection in the Map Designer

- No matter which method you choose to find the desired object, you can always drag any object from the **Device Tree** onto a free area of the map to create a new map item.
- If you drag it onto an existing map item, it replaces the existing item while **Properties** and size stay the same.
- You can also select a map item and double click a **Device Tree** object to replace the map item. If no item is selected, double clicking an object adds a new map item.
- To gain more space for map editing, reduce the size of the **Device Tree** box by dragging its right border to the left. Drag it to the right to enlarge it again.

Properties Selection

Use the **Properties** selection to define how to show the map item (for example, as an icon, a map, a table, or a graph). Select the appearance in different categories. Hover over a property object to get a live preview of it (in most cases).

If a certain **Properties** object is not available for the selected **Device Tree** object, you will see a corresponding text note.



Properties Selection in the Map Designer

There are many different property object types available. Simply click one of the categories to show all available types.

- **Default Icons A, Default Icons B**
  These categories offer a variety of iconic symbols of typical network devices in the current PRTG style. Category A comes with object data which category B does not include.
- **Icons A, Icons B, Icons C**
  These three categories offer a variety of iconic symbols of typical network devices. Below each icon you can see the object name and a sensor overview for the object. This shows how many sensors are in which status 163. For some sensors, a mini graph is shown as well.
- **Icons A (Static), Icons B (Static), Icons C (Static)**
  These three categories offer the same variety of iconic symbols of typical network devices as the category described above. Here, no object data is displayed but only the icon.
- **Static Images**
  This category offers free or public domain geographical maps from different sources. Use properties section Geo Maps if you want to show PRTG **Geo Maps** 2824 in the map.

The items in this section are independent from the selected **Device Tree** objects.

For additional geographical maps and other map customizations, please see this Knowledge Base article: Where can I find custom map objects and other map customizations?

- **Status Icons**
  This category offers options to insert status 163 icons in different styles. These show the object name and an overview of how many sensors there are and their status. For example, you can add "traffic lights" or the QR code of a monitoring object to your map. There is also an object available for audible alert that will play a sound when the number of alarms of the monitored object are > 0. Note that your browser must support playing embedded sounds for this icon.

See also this Knowledge Base article: Which audible notifications are available in PRTG? Can I change the default sound?

- **Cluster**
  If you use the PRTG **Clustering** 116 feature, you can add icons to your map which show the status of your cluster.
  The **Map** icon does not scale automatically, so the nodes are displayed on top of each other by default. Please manually enlarge this icon in the main window of the **Map Designer** (downwards and to the right) until it fits your needs.
- **Data Tables**
  Choose from several table lists 207 that show sensor lists for the currently selected object. You can also choose from several lists that show sensors in a certain status only.
- **Devices**
  Add several views of your device tree 157 to the map, including sensor gauges 166 for the select object.
- **Geo Maps**
  In this category you can choose between a globe and a geographical map. You can see the location of the currently selected object in the **Device Tree** on the map. To use this feature, you must enable Geo Maps integration and you have to enter a **Location** in the settings of the monitoring object you want to use this with. For more information, please see the **Geo Maps** 2824 section.
  If Geo Maps integration is disabled, you will only see white boxes instead of map previews.

- **Graphs**
  This category offers different graph styles in several dimensions and detail. You can also select graphs including a legend or sensor states.
- **Objects**
  Add some simple geometric shapes to your map. The items in this section do not depend on the selected object in the **Device Tree**.
- **Top 10**
  Choose from several tables that show the top 10 sensors in certain categories, like least used CPUs, highest bandwidth usage, best availability, or slowest websites.
- **Custom HTML**
  You can use this property, for example, to add external images or applets to your map. To actually add custom HTML code to your map, add the item, and mark it to edit 2898. You can then copy your custom code into the **HTML Before** and **HTML After** fields in the **Properties** box on the right side.

No matter which object you choose, you can always drag any object from the **Properties** box onto a free area of the map to create a new map item. If you drag it onto an existing map item, it replaces this item, while its **Device Tree** object attributes and size stay the same. You can also select a map item and double click an object in the **Properties** box to replace the map item. If no item is selected, double clicking an object will add a new map item.

To gain more space for map editing, reduce the size of the **Properties** box by dragging its left border to the right. Drag it to the left to enlarge it again.

Edit Existing Map Items—Properties Box

Click a map item to select it. You can then edit its attributes using the fields in the upper part of the **Properties** box on the right side:

- **Top**, **Left**, **Width**, and **Height** fields
  Enter position and size values for direct positioning. Click the **Save** button to save your settings. Alternative: Use the mouse to move and resize a map item.

- **Layer** field
  The layer number defines if an item appears on top of or behind another item if they overlap. The item with the higher number appears on top. Enter a positive integer value and click the **Save** button to save your settings. Alternative: Use the arrow symbols in the context menu of a map item to **Bring to front** or **Send to back** an item one layer (see below).

- **External Link**
  PRTG maps are interactive. You can enter the address of any website here. If you click the map item when viewing the map, PRTG will open this page in a browser window. Enter the whole URL to an external website (for example, https://www.paessler.com) or the address of a subpage of your PRTG installation (for example, devices.htm).

- **HTML**
  Click the arrow symbol underneath to show the **HTML Before** and **HTML After** fields. Any HTML code you enter in these fields is added before or respectively after the map item. Enter your custom HTML code that embeds an object and click the **Save** button. Your HTML object is inserted into the map. For example, you can enter the code <img src="http://media.paessler.com/common/img/logoclaim_r1.gif"> to insert an image of a Paessler logo.

Edit Existing Map Items—Hover Icons

Hover over a map item to show the edit icons for it.

- **Bring to front (arrow up symbol)**
  Move this item one layer to the front. This is useful when adding several items to a map that overlap each other.

- **Send to back (arrow down symbol)**
  Move this item one layer to the back. This is useful when adding several items to a map that overlap each other.

- **Delete (trash symbol)**
  Delete this item.
  Be careful! The item will be deleted immediately without notice and you cannot undo this. Alternative: Select the item and press the Del button on your keyboard.

- **Drop Connections (scissors symbol)**
  If there are connection lines between two items, you can delete all lines starting from this item. Connection lines will be dropped immediately.

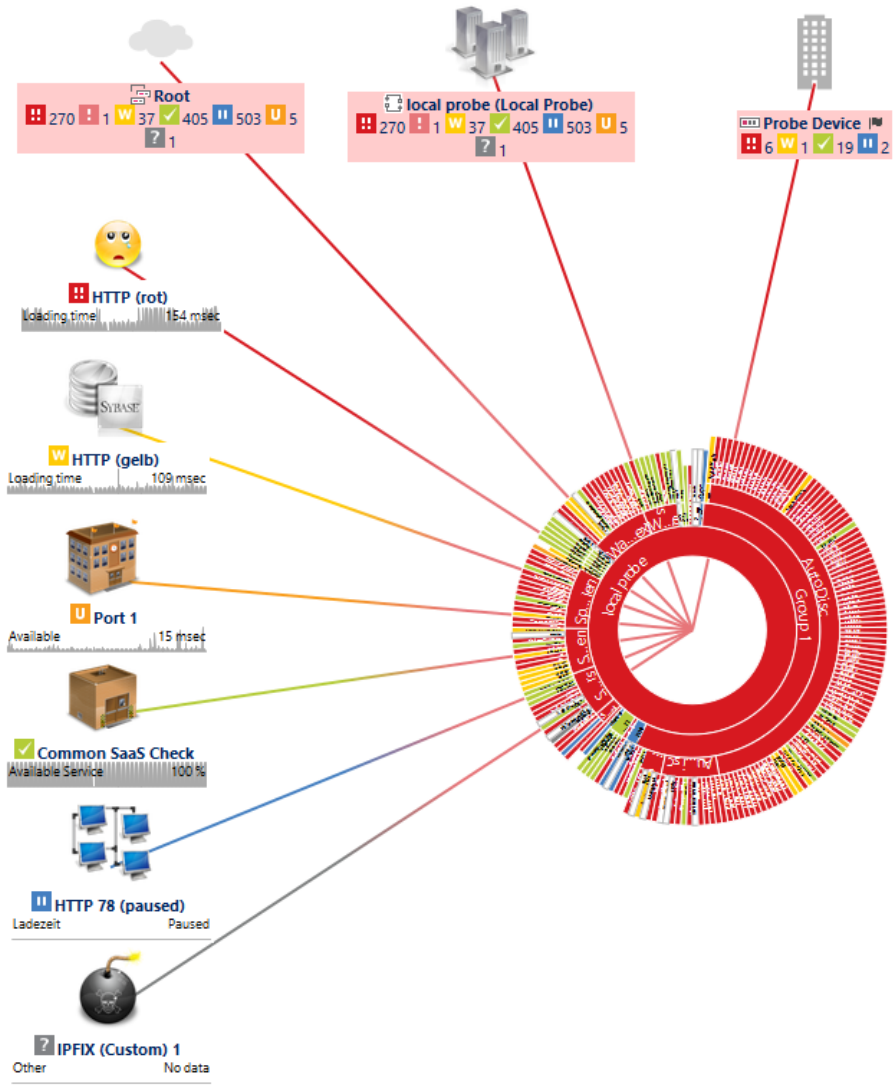
Edit Existing Map Items—Using Cursor Keys

While an object is selected, use the cursor keys to move it one pixel at a time. Hold the Shift key in combination with the cursor keys to move the object 10 pixels at a time.

Draw Connection Lines Between Items

You can draw connection lines between any map items via drag and drop. Click the gray handles next to an item and drag a line to the item you want to draw a connection to. A line between these items appears immediately. This can be useful to indicate network connections or logical coherence between two items. To delete connection lines, click the scissors symbol in the item's edit icons 2898.

Lines between objects are colored dynamically depending on the status 163 of linked objects. For example, a line is red as long as one of the object's icons shows a red **Down** status. This only affects half of the line, at the end where the red sensor is shown. If both objects connected show a red sensor, this results in a continuous red line.



Map with Status Colored Connection Lines

Snap to Grid

Choose **Snap to Grid** below the **Device Tree** box to define how map items are positioned when adding or moving them via drag and drop. The setting is active immediately. With snap to grid enabled, you can place items aligned with the grid only. If you deselect the **Snap to Grid** option, you can place map objects completely free.

Undo and Redo

You can revert previous changes to the map and its objects with the **Undo** button (Ctrl+Z) in the **Device Tree** box. To revert undo actions, use the **Redo** button (Ctrl+Y). You can undo and redo up to 50 changes when you work on a map. Because PRTG saves changes persistently in your configuration, you can even revert changes later.

Both buttons are only available if they can apply, otherwise they are grayed out.

More

Knowledge Base: Why does my browser show an unresponsive script warning while loading the Map Designer?

- http://kb.paessler.com/en/topic/19483

Knowledge Base: How can I add or edit map objects used for PRTG's maps?

- http://kb.paessler.com/en/topic/1703

Knowledge Base: Which audible notifications are available in PRTG? Can I change the default sound?

- http://kb.paessler.com/en/topic/26303

Knowledge Base: Where can I find custom map objects and other map customizations?

- http://kb.paessler.com/en/topic/61263

8.11.3 Maps Settings

Using the Map tabs you can access all functionalities and settings for a map.

Map Tabs

View Map

Click the **View Map** tab any time to show a preview of your map.

Map Designer

Click the **Map Designer** tab to edit the contents of your map.

For details, see manual section Map Designer 2893.

Settings

Click the **Settings** tab to open a map's general settings.

When using the **Add Map** dialog, not all of these settings are available. You can change them later by clicking the **Settings** tab.

BASIC MAP SETTINGS

Map Name	Enter a meaningful name for the map.
Security Context	Define the user account that the map will use for access to monitoring data. The map will only contain objects that the selected user 129 is allowed to view. Please choose a user account from the list. The available users depend on your configuration. By default, this is the user that created the map. PRTG Administrator users can change this setting.
Timezone	Define the time zone that the map will use for all date-specific options. Select a time zone from the list.
Tag Filter	This setting affects table map objects. Enter one or more tags separated by spaces or commas to include sensors in tables. Only sensors with one of the tags entered here will appear in this map's data tables, including sensors that inherit 122 tags from parent objects. Please enter a string or leave the field empty.

BASIC MAP SETTINGS

For some map objects like sunburst and treemap, the tag filter applies to devices, groups, and probes. If you use only tags of sensors, these map objects will not appear on the map. Filtering sunburst and treemap objects with multiple tags may not work properly and is not officially supported.

Use this setting with care because it will affect all tables of the current map!

MAP LAYOUT

Map Width	Define the width of the map in pixels. Please enter an integer value.
Map Height	Define the height of the map in pixels. Please enter an integer value.
Automatic Scaling	Define if you want the map to automatically adapt to your screen size. Choose between: ▪ **Scale map view to fit browser size**: The size of the map adapts automatically to the size of your screen. Choose this method if the map is shown on various screens with different resolutions so that it uses the available place in the browser window the best possible way. ▪ **Do not auto-scale map view**: The map uses always the size that you define above.
Background Picture	Define if you want to use a background picture for the map. Choose between: ▪ **Use an image in the background of the map**: Use a custom background image that you define below. ▪ **Do not use a background image**: Do not use a background image.
Background Image	This option is only visible if you enable a background picture above. Click the **Choose File** button and select an image from your computer or network. Only images in the format JPG, PNG, and GIF are supported. The file size must be smaller than 20 MB. If you try to upload other images, you get an error message.

MAP LAYOUT

Background Color	Select a background color for this map. Either enter a hex color code or choose a color from the color selector. The hex color code field will always display the currently defined color.

PUBLIC ACCESS

Public Access	Define if others can see the map. Choose between: ▪ **No public access (map cannot be viewed without login)**: Do not allow public access to the map. Only users with both a login to the PRTG web interface and sufficient access rights can see the map. ▪ **Allow public access (map can be viewed by using a unique URL)**: Allow access to the map using a unique address. The URL contains a key that you can change below. The map will be an interactive public map. ▪ **Allow public access, disable all links (map can be viewed by using a unique URL)**: Allow access to the map using a unique address. The URL contains a key that you can change below. If you choose this option, all links on the map are disabled, so it will be a non-interactive public map.
Secret Key	This field is only visible if public access is enabled above. The key is automatically generated. It is part of the public URL for the map. You can also enter a customized string. We recommend that you use the default value. For more information on public access, please see the Get HTML 2905 section. The characters comma "," and colon ":" are not allowed in the secret key field!

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object that you are editing. A table with user groups and rights is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object does not show up in lists.

ACCESS RIGHTS

- **Read**: Users in this group can see the object and review its settings.
- **Write**: Users in this group can see the object, as well as review and edit its settings. However, they cannot edit access rights settings.
- **Full**: Users in this group can see the object, as well as review and edit its settings as well as edit access rights.

You can create new user groups in the **System Administration—User Groups** 2982 settings.

Click **Save** to save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Get HTML

Your PRTG map is like a standalone HTML page. You can make it accessible to others, if you like. Depending on the **Public Access** setting 2902 of your map, a visitor needs to provide PRTG user account login data to view the map, or sees the map immediately using a URL containing a secret key. When using this unique key, you can also include your map on another webpage, embedding it via <iframe>.

- **Option 1: Link to a web page with the map that requires login credentials**
  The shown URL requires login credentials in order to display the map. PRTG asks the user trying to view the map via this URL for login credentials.
  In the URL, usually the IP address is given via which the page is available. Maybe a NAT translation is set in your firewall, or you may want to use a domain name or a name from a dynamic DNS service for public access. Please customize the URL you use for access to your needs.
- **Option 2: Link to a web page that displays the map without a login**
  To get the shown URL working for public access without a login, enable **Public Access** in the settings tab 2902 of your map.
  In the URL, usually the IP address is given via which the page is available. Maybe a NAT translation is set in your firewall, or you may want to use a domain name or a name from a dynamic DNS service for public access. Please customize the URL you use for access to your needs.
- **Option 3: Show a map inside other web pages using an IFRAME**
  For your convenience, this shows source code for adding an iframe to another webpage. It includes a URL for direct access. Just copy the code and paste it into your webpage code. Also enable **Public Access** in the settings tab 2902.
  In the URL, usually the IP address is given via which the page is available. Maybe a NAT translation is set in your firewall, or you may want to use a domain name or a name from a dynamic DNS service for public access. Please customize the URL you use for access to your needs.

While a map is shown via these URLs, you can change the refresh interval any time by hovering over the arrows symbol in the lower right corner. Choose between **10**, **30**, or **60** seconds, **10** minutes or **Refresh** now. The map adapts automatically to the size of the browser window if you enable the auto-scaling setting 2902.

Comments

On the **Comments** tab you can enter free text for each object. You can use this function for documentation purposes or to leave information for other users.

Click **Save** to save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

History

In the **History** tab all changes in the settings of an object are logged with a timestamp, the name of the PRTG user who made the change, and a message. The history log retains the last 100 entries.

Delete

You can delete the entire map any time by clicking the trash symbol on the right.

More

PRTG Manual:

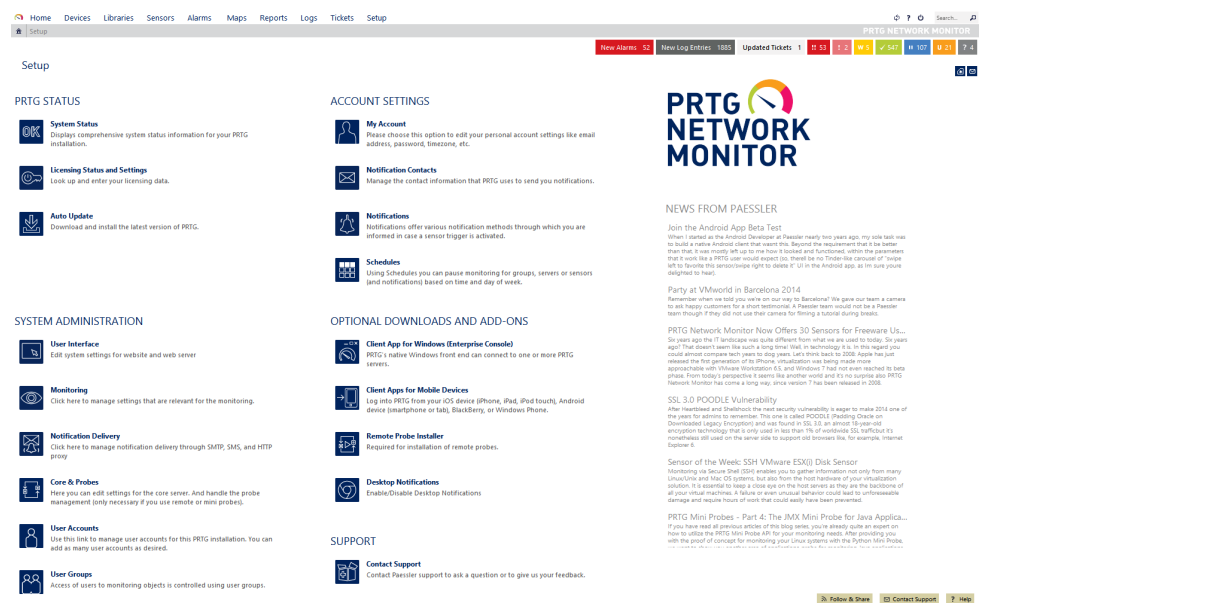
- **Data Reporting** 132

8.12 Setup

In the setup settings of the PRTG web interface, you can define almost all system settings for PRTG. However, some of the machine-oriented settings are defined using two Windows administration tools (see Others 2908 section below).

In the main menu, click on **Setup** to show the available options.

- Some setup options are only available for PRTG on premises (marked with the PRTG on premises icon), so you cannot use these on PRTG on demand instances.
- Some setup options are only available for PRTG on demand (marked with the PRTG on demand icon), so you cannot use these on PRTG on premises instances.



Setup Overview Page

PRTG Status

- PRTG Status—System Status 2994
- PRTG Status—Cluster Status 3010
- PRTG Status—Licensing Status and Settings 3012
- PRTG Status—Auto-Update 3005

Account Settings

- Account Settings—My Account 2909
- Account Settings—Notifications 2916
- Account Settings—Notification Contacts 2934

- Account Settings—Schedules 2938

System Administration

- Manage Subscriptions 69
- System Administration—User Interface 2943
- System Administration—Monitoring 2955
- System Administration—Notification Delivery 2961
- System Administration—Core & Probes 2967
- System Administration—User Accounts 2975
- System Administration—User Groups 2982
- System Administration—Administrative Tools 2987
- System Administration—Cluster 2992

Optional Downloads and Add-Ons

- Downloads—Client App for Windows (Enterprise Console) 3018
- Downloads—Client Apps for Mobile Devices 3018
- Downloads—Remote Probe Installer 3018
- Desktop Notifications 3020

Support

- Support—Contact Support 3022

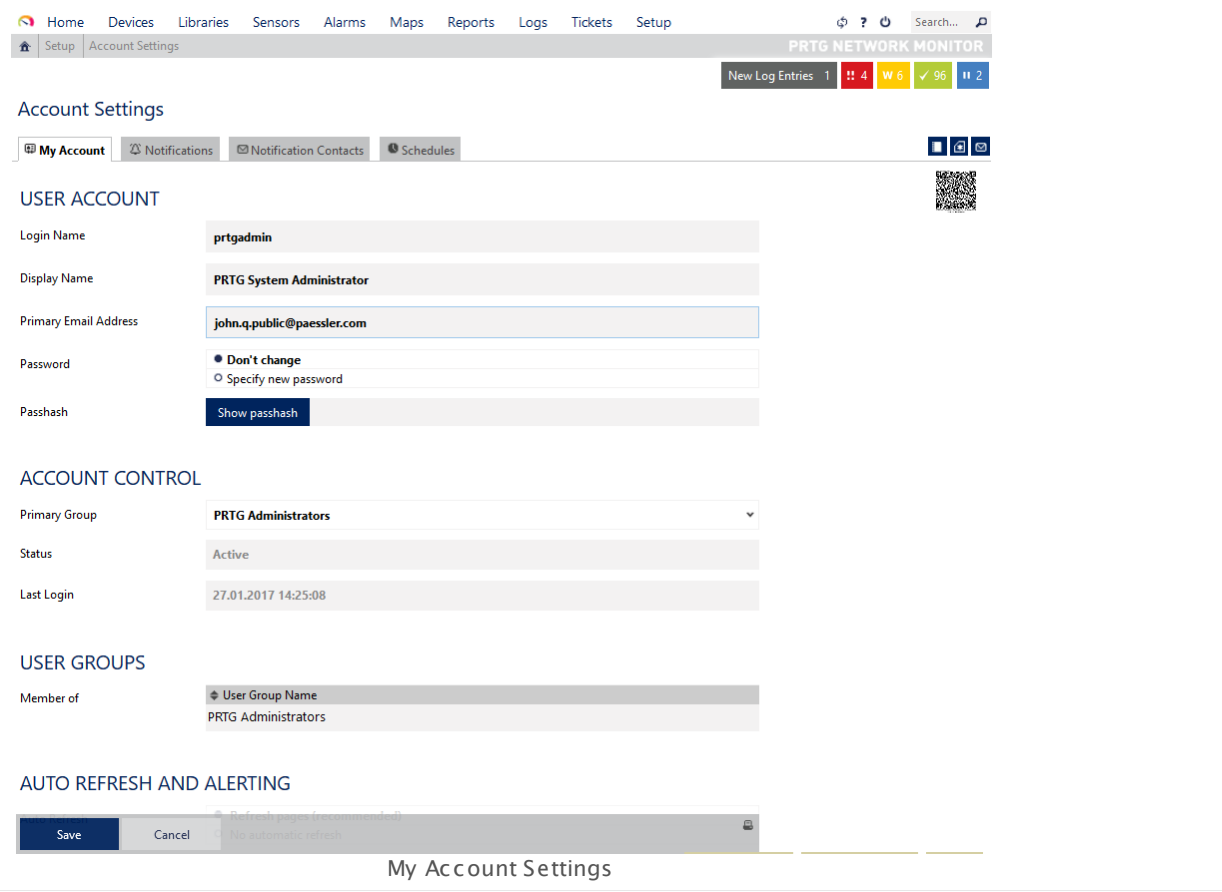
Others

There are some settings that you have to make in the PRTG Administration Tool 3134, running as Windows application. For more details, please see sections PRTG Administration Tool on Core Server System 3135 and PRTG Administration Tool on Remote Probe System 3157.

8.12.1 Account Settings—My Account

In the **My Account** settings you can define values regarding your (currently logged in) PRTG user. All settings in this section are user-specific. Some account options may not be available, but restricted to the administrator.

If you use PRTG on premises and open the system administration page from another administration page, PRTG will ask you to enter your credentials again for security reasons if 15 minutes (900 seconds) have passed since your last credential-based login. A dialog box will appear. Enter your **Login Name** and **Password** for PRTG in the corresponding fields and confirm to continue.



My Account Settings

My Account Settings

This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

USER ACCOUNT

Login Name	Enter the login name for the user. This option is not available in PRTG on demand.
Display Name	Enter a name that the user recognizes. It will not be used for login purposes.
Primary Email Address	Enter the user's email address. Please use an email client that can show HTML emails, otherwise you cannot read emails from PRTG.
Password	Define the user password. For security reasons, the account settings page does not contain the password. Choose between: ▪ **Don't change** ▪ **Specify new password** If you choose to specify a new password, enter the old password and then the new password twice. The new password must be at least 8 characters long. It must contain a number and a capital letter. Leading and trailing whitespaces will be cut. The password of a PRTG Administrator user can only be changed by the same PRTG Administrator user. This option is not available in PRTG on demand.
Passhash	Click **Show passhash** to display the passhash for the selected user. You need the passhash of a user if you use the PRTG Application Programming Interface (API). This setting is shown for your information only and cannot be changed here. This option is not available in PRTG on demand.

API ACCESS

These settings are only available in PRTG on demand.

API ACCESS

API Username	Shows the username of the current user account. You need a username if you use the PRTG Application Programming Interface (API) 3174. This setting is shown for your information only and cannot be changed here.
API Passhash	Click **Show passhash** to display the passhash for the selected user. You need the passhash of a user if you use the PRTG Application Programming Interface (API) 3174. This setting is shown for your information only and cannot be changed here.
Reset API Passhash	Click **Generate new passhash** to reset the passhash of the current user.

ACCOUNT CONTROL

Account Type	This setting is only visible to administrator users. However, it will not show if the user who's account you want to modify is a member of a group with administrative rights. Define the account type for the current user. Choose between: ▪ **Read/Write User**: You can change settings. ▪ **Read Only User**: You cannot edit any settings except your own password. This is a good choice for public or semi-public logins. ⓘ This setting cannot be changed for the default administrator user.
Allow Acknowledge Alarms	This setting is only visible if **Read Only User** is enabled above. Acknowledging an alarm is an action that requires write access rights. However, you can explicitly allow this action to read-only users. If enabled, they still do not have write access, but may acknowledge alarms 191. Choose between: ▪ **Allow**: Allow acknowledging alarms for this user. ▪ **Deny**: The user will not be able to acknowledge alarms.
Password Changes	Decide if you want the user to be able to change their account's password or not. If you allow the user to change the password, this option will be available in the My Account 2909 settings of the respective user. Choose between: ▪ **User may change his account's password**

ACCOUNT CONTROL

	▪ **Deny the right to change the password** (default) ⓘ This field is only visible if you edit this option for read-only users as an administrator.
Primary Group	This setting is available only for administrator users. Select the primary group for the current user. Every user has to be member of a primary group to make sure there is no user without group membership. Membership in other user groups is optional. For user experience there is no difference between the primary and other user groups. ⓘ You cannot change the primary group of Active Directory users. Users that you added with **Active Directory Integration** 3171 can only have this AD group as their primary group. If you need to change this, please delete this user account and add it again.
Status	This setting is only shown for administrator users. Define the status of the current user. Choose between: ▪ **Active**: The current user can login to the account. ▪ **Inactive**: The current user's login is disabled. Use this option to temporarily deny access for this user. ⓘ This setting cannot be changed for the default administrator user.
Last Login	Shows the time stamp of the user's last login. This setting is shown for your information only and cannot be changed here.

USER GROUPS

Member of	Shows the groups the current user is member of. Access rights to the device tree are defined on group level. This setting is shown for your information only and cannot be changed here.

AUTO REFRESH AND ALERTING

Auto Refresh	Define if you want PRTG to reload web pages automatically for the current user. Choose between: ▪ **Refresh pages (recommended)**: Automatically refresh the single page elements on the web pages in PRTG. ▪ **No automatic refresh**: Do not automatically refresh web pages.
Auto Refresh Interval (Sec.)	This setting is only relevant if you enable auto refresh above. Enter the number of seconds that PRTG waits between two refreshes. We recommend that you use **30** seconds or more. Minimum value is 20 seconds. Shorter intervals create more CPU load on the server running PRTG. If you experience load problems while using the web interface (or PRTG maps 2885), please set a higher interval.
Play Audible Alarms	Define when PRTG will play an audible alarm the current user on web pages whenever there are new alarms 190. Choose between: ▪ **Never**: Do not play sound files on any web pages. ▪ **On dashboard pages only**: When there are new alarms, play a predefined sound on dashboard 231 pages only. The sound will be played with every refresh of the dashboard page if there is at least one new alarm. ▪ **On all pages**: When there are new alarms, play a predefined sound on all web pages. The sound will be played with every page refresh if there is at least one new alarm. Audible alarms are only played if the **New Alarms** value in the **Global Header Area** 153 of the PRTG web interface is greater than 0 after a page refresh. The number of existing alarms is not considered. For more information about audible notifications and supported browsers, see this Knowledge Base article: Which audible notifications are available in PRTG? Can I change the default sound?

WEB INTERFACE

Homepage URL	Define the user's default page, which is loaded after logging in or clicking on the Home 231 button in the main menu.

WEB INTERFACE

Max. Groups/Devices per Group	To provide a fast and smooth user experience, PRTG attempts to reduce page size when displaying the device tree. It automatically collapses groups and devices when reaching a specified number of items. Enter this threshold for groups and devices here. We recommend values between **10** and **30**.
Max. Sensors per Device	In order to provide a fast and smooth user experience, PRTG attempts to reduce page size when displaying the device tree. It automatically collapses groups and devices when reaching a specified number of items. Enter this threshold for sensors per devices here. We recommend values between **10** and **30**.
Timezone	Define the time zone for the current user. Depending on the time zone you select here, PRTG shows the current user's local time zone in all data tables and graph legends. PRTG receives the UTC (Coordinated Universal Time) from the system time set on the PRTG core server for this purpose.
Date Format	Define the date format for the current user. This setting will take effect after the next login.

TICKET SYSTEM

Email Notifications	Define if you want to get emails from the ticket system. Choose between: ▪ **I want to receive an email whenever a ticket changes**: You will receive an email each time a ticket is assigned to you or your user group, or if a ticket that is assigned to you or your user group is changed. If you edit tickets that are assigned to you or your user group, or you assign a ticket to yourself or your user group, you will not get an email. ▪ **I do not want to receive any emails from the ticket system**: You will not get any emails about tickets.

Notification Contacts

In the **Notification Contacts** 2934 tab you can define recipients for each user account. Recipients can be email addresses, phone numbers, or push devices (iOS, Android and Windows Phone devices with the corresponding PRTG smartphone app 3082).

Comments

On the **Comments** tab you can enter free text for each object. You can use this function for documentation purposes or to leave information for other users.

Click **Save** to save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

History

In the **History** tab all changes in the settings of an object are logged with a timestamp, the name of the PRTG user who made the change, and a message. The history log retains the last 100 entries.

Click the **Continue** button to save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

More

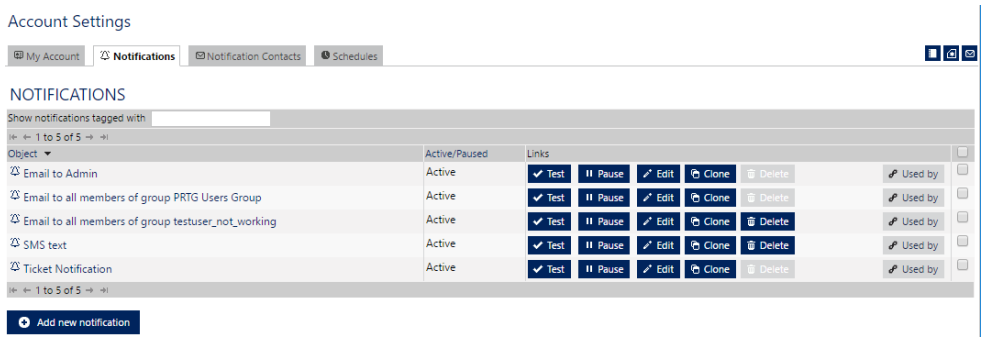
Knowledge Base: Which audible notifications are available in PRTG? Can I change the default sound?

- https://kb.paessler.com/en/topic/26303

8.12.2 Account Settings—Notifications

In the notification settings you can define and change notifications for the current PRTG user. Notifications can be triggered for specific sensor states and values.

If you use PRTG on premises and open the system administration page from another administration page, PRTG will ask you to enter your credentials again for security reasons if 15 minutes (900 seconds) have passed since your last credential-based login. A dialog box will appear. Enter your **Login Name** and **Password** for PRTG in the corresponding fields and confirm to continue.



Notification Settings

Click here to enlarge: https://media-s3.paessler.com/prtg-screenshots/account_settings_notifications.png

Note

This section describes one of four steps to set up the notification system in PRTG. A complete notification setup involves:

1. Checking and setting up the **Notification Delivery** settings. This tells PRTG how and where to send messages.
   For detailed information, see **System Administration—Notification Delivery** 2961.
2. Checking and setting up **Notification Contacts** for the users of your PRTG installation. This defines where to send notifications.
   For detailed information, see **Account Settings—Notification Contacts** 2934.
3. Checking and setting up **Notifications**. This defines the kind of message and its content.
   For detailed information, see **Account Settings—Notifications** 2916.
4. Checking and setting up **Notification Triggers** for objects. This provokes the defined notifications.
   For detailed information, see **Sensor Notifications Settings** 2791.

We recommend that you always set up at least two notifications with different delivery methods for a notification trigger, for example, one email notification 2922 and one SMS notification 2924. If delivery via email fails (due to an email server failure or other reasons), PRTG can still notify you via your smartphone. Simply set your latency setting to a state trigger 2793 and a notification via a delivery method other than the one for the first trigger. Or set up a second trigger with another notification for the corresponding object.

For background information, please see the **Notifications** 2829 section.

Notifications Overview

Click the **Notifications** tab to show a list of existing notifications. Using the buttons in the column **Links**, perform the following actions to set up a notification:

- **Test**: Trigger this notification immediately for testing purposes.
  When testing notifications, PRTG will not resolve the placeholders, but rather send the original variables instead.
- **Pause**: Pause this notification. If a notification is paused 214, PRTG will not send messages when this notification is triggered.
- **Edit**: Open the settings of a notification 2917 to edit them.
- **Clone**: Create an exact copy of this notification. The clone 2812 is added to the notifications list as Clone of [...]
- **Delete**: Delete this notification (not possible for predefined notifications).
- **Used by**: Show all objects that trigger this notification.

Please also see **Working with Table Lists** 207. Additionally, the multi-edit functionality is available. This enables you to change properties of several objects simultaneously via bulk changes. For more details, see the **Multi-Edit Lists** 2814 section.

Notifications Settings

Click the **Add new notification** button to add a new notification, or click the name of an existing notification to edit it.

This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

BASIC NOTIFICATION SETTINGS

Notification Name	Enter a meaningful name for the notification, for example, SMS to service team.
Tags	Enter one or more tags 124. Confirm each tag with the space, comma, or enter key. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. Tags will be automatically inherited 124.
Status	Select the status of the notification. Choose between:

BASIC NOTIFICATION SETTINGS

- **Started**: This notification is active. PRTG executes this notification when it is triggered.
- **Paused**: Pause this notification. If a notification is paused, PRTG does not execute this notification when it is triggered.

Schedule

Define intervals for notifications to pause. You might want the notifications to pause for scheduled maintenance periods or regular server reboots at certain intervals. For continuous notification select **None.** This selection will make your notifications be active 24/7 without pause. You can also choose one of the suggested schedules from the list. Usually schedules define when this notification will be active. Schedules defined as period list set this notification to inactive at the corresponding time spans. The available options depend on your setup. To add or change existing schedules, please see **Account Settings—Schedules** 2938.

Postpone

Define whether PRTG should send you notifications that were triggered while the notification was **Paused** later on, when the notification status is in **Started** again.

- **No**: Discard all notifications that are triggered while the notification is paused.
- **Yes**: Collect all notifications that are triggered while the notification is paused. Send out all these notifications once the **Paused** status ends.

NOTIFICATION SUMMARIZATION

Method

Define if and how PRTG summarizes several notifications into one or more messages (max. 1,000 characters). Define if several notification triggers are to be collected over a specified time period and then send as a single summarized notification. Choose between:

- **Always notify ASAP**: Always send out one notification for each received notification trigger as soon as possible (for example, immediately).
- **Send first DOWN message ASAP, then summarize**: When receiving several **DOWN** triggers, send the first notification immediately, then keep summarizing notification triggers into one message, regardless of sensor state.
- **Send first DOWN and UP message ASAP, then summarize**: When receiving several **DOWN** or **UP** triggers, send each first notification immediately, then keep summarizing notification triggers into one message, regardless of sensor state.
- **Send all DOWN messages ASAP, summarize other trigger types**: When receiving several **DOWN** triggers, send out one notification for each trigger received, but summarize notifications for all non-DOWN triggers into one message.
- **Send all DOWN and UP messages ASAP, summarize other trigger types**: When receiving several **DOWN** or **UP** triggers, send out one notification for each trigger received, but summarize the notifications for all non-DOWN and non-UP triggers into one message.
- **Always summarize notifications**: When receiving several notification triggers, summarize notifications, regardless of the kind of trigger received. Please note, the maximum number of notifications (see below) still applies.

Regardless of the option you choose, PRTG always executes notifications of the types **Ticket**, **Execute HTTP Action** and **Execute Program** immediately. PRTG will always send out one message for each of these notifications immediately. All other notification types can be summarized.

'first DOWN' and 'first UP' messages refer to trigger condition and clear condition respectively. You can also define 'WARNING' or 'UNUSUAL' states as trigger conditions or even thresholds or other triggers notification summarizations. The condition clear triggers, if applicable, are defined in the respective trigger conditions as well. The triggers all qualify as "first DOWN" or "first UP" messages.

NOTIFICATION SUMMARIZATION

PRTG collects up to 25 single notifications for one summarization and will send out the message as soon as this number is reached (or when the gathering time has passed). If there are more than 25 notifications within the defined time span, you will receive more than one message with up to 25 entries each. For example, 74 collected notifications would result in 3 summarized messages with 25, 25, and 24 collected notifications.

Subject for Summarized Messages	Define a subject that PRTG will include when sending summarized notifications. You can use the placeholder %SUMMARYCOUNT for the number of messages that are summarized. The subject you define is only used for **Send Email** and **Amazon SNS** messages.
Length of Gathering (Minutes)	Define a time span in minutes to define how long PRTG collects notifications for summarization. Please enter an integer value. If you enter a rather long time span, for example, **60** minutes, PRTG will collect notifications for one hour before sending them out summarized unless other features (see above) require an earlier message dispatch.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object that you are editing. A table with user groups and rights is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object does not show up in lists. ▪ **Read**: Users in this group can see the object and review its settings. ▪ **Write**: Users in this group can see the object, as well as review and edit its settings. However, they cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, as well as review and edit its settings as well as edit access rights. You can create new user groups in the **System Administration—User Groups** 2982 settings.

Notifications Settings—Choose Notification Methods

With the following settings, you can add one or more methods for how PRTG sends out a notification message. You can choose one method or combine several methods from the list. Whenever the notification is triggered, PRTG sends out messages or performs actions for all configured methods at once.

To choose a method, mark the check box in front of the corresponding notification type. You can then see and set the options as described below. The following notification methods are available.

- Email 2922
- Push Notification 2923
- SMS/Pager Message 2924
- Add Entry to Event Log 2926
- Syslog Message 2927
- SNMP Trap Message 2928
- Execute HTTP Action 2929
- Execute Program 2930
- Amazon SNS Message 2930
- Ticket 2931

In your message, you can use various placeholders. Some of them are already filled in by default. For a complete list of available placeholders, please see this Knowledge Base article: What placeholders can I use with PRTG?

Some notification types are only available for PRTG on premises (marked with the PRTG on premises icon). You cannot use these on PRTG on demand instances.

SEND EMAIL

This notification method uses notification contacts to deliver the messages. Please set up and check them for the desired user accounts in advance under **Account Settings—Notification Contacts** 2935.

The three options for recipients below (user, user group, email address) work simultaneously. Because of this, you can define more than one user as recipient of this notification. PRTG sends the notification email to the active email contacts of the user you select, to the active email contacts of all members of the user group you select, and to all email addresses you enter into the **Send to Email Address** field.

You can include custom email headers and footers into PRTG HTML emails. For details, please see this Knowledge Base article How can I include my own logo into HTML emails?

Send to User	Select a user of your PRTG installation to send the notification email to. PRTG sends this notification to each email contact of this user account. You can add and edit email contacts of a user in **Account Settings—Notification Contacts** 2935. Choose **None** to not use this feature.
Send to User Group	Select a user group to send an email with the notification to all members of this group. PRTG sends this notification to the email contact of every group member. You can edit user groups under **System Administration—User Groups** 2982 and email contacts under **Account Settings—Notification Contacts** 2935. Choose **None** to not use this feature. If you select a user group and a specific member of this group as recipients, the user will only receive a single email. This also applies if you enter an individual email address below that is already defined as an email contact of the selected user. If you define individual email addresses (see below), to a specific user (see above), and a user group, PRTG sends the message to the individual email addresses, to the individual user, as well as to the members of the selected user group. In all cases, PRTG sends one message with all recipients in the "To" field of the email.

SEND EMAIL

Send to Email Address	Enter one or more recipient email addresses to which PRTG sends the notification email. If you enter more than one address, separate them with commas. Leave this field empty to send this notification only to the email contacts of the user or members of the user group you choose above. We recommend that you use the options **Send to User** and/or **Send to User Group** instead because you can manage the notification contacts of users more easily this way.
Subject	Enter the subject of the email notification. Several placeholders (variables) are used here by default: [%sitename] %device %name %status %down (%message)
Format	Define the kind of email that PRTG sends when the notification is triggered. Choose between: ▪ **HTML**: PRTG uses the default HTML email template for the message part of the email. ⓘ Please use an email client that can show HTML emails, otherwise you cannot read emails from PRTG. ▪ **Text**: PRTG uses the default plain text email template for the message part of the email. ▪ **Text with custom content**: PRTG uses custom plain text for the message part of the email. You can enter your individual text below.
Custom Content	This field is only visible if you select the custom text option above. Enter the desired message for this email notification in plain text format. You can use placeholders here.
Priority	Define the priority that PRTG sets for the email. Most email clients can show this priority flag. Choose between: ▪ **highest** ▪ **high** ▪ **normal** ▪ **low** ▪ **lowest**

SEND PUSH NOTIFICATION

Push notifications only work with the apps **PRTG for Android**[3082], **PRTG for iOS**[3082], and **PRTG for Windows Phone**[3083]. You have to activate push notifications in the settings of your app first. For details about the setup, please see this Knowledge Base article: How can I send push notifications with PRTG?

This notification method uses notification contacts to deliver the messages. Please set up and check them for the desired user accounts in advance under **Account Settings—Notification Contacts**[2935].

The PRTG server needs to communicate on port 443 to the PRTG Cloud to send push notifications, which is **https://api.prtgcloud.com:443** (the same as for the **Cloud HTTP Sensor**[571], the **Cloud Ping Sensor**[580] and support tickets[3022]).

The two options for recipients below (user, user group) work simultaneously. Because of this, you can define more than one user as recipient of this notification. PRTG sends the notification to the active push contacts of the user you select and to the active push contacts of all members of the user group you select.

Send to User	Select a user of your PRTG installation to send the push notification to. PRTG sends this notification to each push contact of this user account. You can edit push contacts of a user in **Account Settings—Notification Contacts**[2935] and add push contacts by activating push notifications in the Android or iOS app with this user. Choose **None** to not use this feature.
Send to User Group	Select a user group to send the push notification to all members of this group. PRTG sends this notification to each push contact of every member of this group. You can edit user groups under **System Administration—User Groups**[2982] and push contacts under **Account Settings—Notification Contacts**[2935]. Choose **None** to not use this feature. If you select a user group and a specific member of this group as recipients at the same time, this user receives the text message only one time.
Message	Define the message. A message with information about the sensor status is already predefined. Several placeholders[2933] (variables) are used here: [%sitename] %device %name %status %down (%message) You can change the message to your liking. To reset this field to its default value, enter a single star symbol * (and nothing else).

SEND SMS/PAGER MESSAGE

You have to set up this notification method in the **System Administration—Notification Delivery** 2961 settings first.

This notification method uses notification contacts to deliver the messages. Please set up and check them for the desired user accounts in advance under **Account Settings—Notification Contacts** 2935.

The three options for recipients below (user, user group, email address) work simultaneously. Because of this, you can define more than one user as recipient of this notification. PRTG sends the notification to the active SMS contacts of the user you select, to the active SMS contacts of all members of the user group you select, and to every phone number you enter into the **Send to Number** field.

This notification method uses the central proxy settings that you define for your PRTG core server. For details, please see **System Administration—Core & Probes** 2967 (section **Proxy Configuration**).

This option is not available in PRTG on demand.

Send to User	Select a user of your PRTG installation to send the notification to. PRTG sends this notification to each SMS contact of this user account. You can add and edit SMS contacts of a user in **Account Settings—Notification Contacts** 2935. Choose **None** to not use this feature.
Send to User Group	Select a user group to send a text message with the notification to all members of this group. PRTG sends this notification to each SMS contact of every member of this group. You can edit user groups under **System Administration—User Groups** 2982 and SMS contacts under **Account Settings—Notification Contacts** 2935. Choose **None** to not use this feature. If you select a user group and a specific member of this group as recipients at the same time, this user receives the text message only one time. This also counts if you enter an individual phone number below that is already defined as an SMS contact of the selected user.
Recipient Number	Define the number to which PRTG sends the text message. The format depends on the SMS provider. Usually, you use a plus sign "+", followed by country code and number. For example, enter +1555012345. Ensure the number format meets the requirements of your SMS provider or the hardware that you use in combination with an API call. Sometimes a preceded plus sign is not required. A wrong format may result in undelivered messages!

SEND SMS/PAGER MESSAGE

	If you enter more than one number, separate them by comma. Leave this field empty to send this notification only to the SMS contacts of the user or members of the user group you choose above. We recommend that you use the options **Send to User** and/or **Send to User Group** instead because you can manage the notification contacts of users more easily this way.
Message	Define the message. A message with information about the sensor status is already predefined. Several placeholders (variables) are used here: [%sitename] %device %name %status %down (%message) You can change the message to your liking. To reset this field to its default value, enter a single star symbol * (and nothing else).

ADD ENTRY TO EVENT LOG

This option is not available in PRTG on demand.

Logfile	Define the log file into which PRTG writes the message. Choose between: ▪ **Application**: Use the Windows application log file in the event log. ▪ **PRTG Network Monitor**: Write messages to the PRTG Network Monitor log file in the Windows event log.
Event Source	This setting is only relevant when using the **Application** log file. Enter the source for the event. Usually, this is the name of the application.
Event Type	Select the type of the event. Choose between: ▪ **Error** ▪ **Warning** ▪ **Information**

ADD ENTRY TO EVENT LOG

Event Log Message	Define the message. A message with information about the sensor status is already predefined. Several placeholders (variables) are used here. You can change it to your liking. To reset this field to its default value, enter a single star symbol * (and nothing else).

SEND SYSLOG MESSAGE

This option is not available in PRTG on demand.

Host/IP	Define the IP address or DNS name of the computer running the syslog server. You can receive and analyze syslog messages with the **Syslog Receiver Sensor**.
Syslog Port	Enter the port number on which syslog messages are sent. By default, this is port number **514**. Only User Datagram Protocol (UDP) is supported.
Facility	Define the facility information. There are several options available from the list.
Encoding	Define the encoding of the syslog message that PRTG sends to your syslog receiver. Choose between: ▪ **ANSI** ▪ **UTF-8**
Message	Define the message. A message with information about the sensor status is already predefined. Several placeholders (variables) are used here. You can change it to your liking. To reset this field to its default value, enter a single star symbol * (and nothing else).

SEND SYSLOG MESSAGE—SYSLOG MESSAGE SEVERITY STATUS

Depending on the status of the sensor that triggers the syslog notification, PRTG sets the **Severity** level of the message automatically.

OK	Severity level: Notice (5)
Warning	Severity level: Warning (4)
Error	Severity level: Error (3)

SEND SNMP TRAP

For information about the OIDs that PRTG uses in the content of the SNMP traps, please see this Knowledge Base article: Is it possible to send SNMP traps using PRTG?

This option is not available in PRTG on demand.

Host/IP	Define the IP address or DNS name of the computer running the trap receiver. You can receive and analyze SNMP trap messages with the **SNMP Trap Receiver Sensor**.
SNMP Port	Enter the port number on which trap messages are sent. By default, this is port number **162**.
Community String	Enter the community string of the device. By default, this is set to **public**. Please enter a string or leave the field empty.
Specific Trap Code	Enter a code that can help you identify the purpose of the trap. Default value is **0**. Please enter an integer value.
Message ID	Enter an ID that helps you identify the origin of the trap. Please enter an integer value. PRTG sends it on the OID 1.3.6.1.4.1.32446.1.1.1.

SEND SNMP TRAP

Message	Define the message. A message with information about the sensor status is already predefined. Several placeholders (variables) are used here. You can change it to your liking. To reset this field to its default value, enter a single star symbol * (and nothing else).
Agent IP	Define the IP address of the agent. Leave this field empty to use the IP address of your PRTG web server.

EXECUTE HTTP ACTION

Regardless of the **Notification Summarization** method chosen above, PRTG sends notifications of the type **Execute HTTP Action** always as soon as possible (ASAP). They are never summarized.

This notification method uses the central proxy settings that you define for your PRTG core server. For details, please see **System Administration—Core & Probes** (section **Proxy Configuration**).

For more details, please see the PRTG **Application Programming Interface (API) Definition** in your PRTG web interface. You can find ready-to-use custom notifications in the PRTG Script World, please see below.

URL	Enter the URL to which PRTG sends the request. HTTP notifications work with and without SSL.
SNI (Server Name Indication)	Select if PRTG will send the SNI extension to the TLS protocol along with the HTTP request. Choose between: ▪ **Do not send SNI (default)**: PRTG will not send an SNI when executing the HTTP action. ▪ **Send SNI**: PRTG will send an SNI when calling the target URL. Specify the SNI below.
Virtual Host (SNI)	This field is only visible if you select the SNI option above. Enter the SNI name that your endpoint configuration requires. Usually, this is the Fully Qualified Domain Name (FQDN) of the virtual host.
Postdata	Enter postdata if you want to send this data to the URL. You can use placeholders here. Line breaks are supported.

EXECUTE PROGRAM

Regardless of the **Notification Summarization** method chosen above, PRTG sends notifications of the type **Execute Program** always as soon as possible (ASAP). They are never summarized.

For more details about **Custom Notifications**, please see the **Application Programming Interface (API) Definition** 3174 in your PRTG web interface. You can find ready-to-use custom notifications in the PRTG Script World, please see below 2932.

This option is not available in PRTG on demand.

Program File	Select an executable file from the list. PRTG runs it every time the notification is triggered. In this list, you see the files which are in the corresponding **/Notifications/EXE** sub-directory of your PRTG core server system. To appear in this list, store the files as BAT, CMD, DLL, EXE, PS1, or VBS. To find this path, please see section **Data Storage** 3226. In a cluster setup, copy your files to every cluster node installation manually. This makes sure PRTG can execute the notification even when the master node fails. If your custom notification executes an external program, install it on all cluster nodes as well.
Parameter	Enter parameters with which the program file will be started. You can use placeholders 2933 here. For example, is you use a batch file that contains a %1 variable, you can provide a value for this variable here.
Domain or Computer Name	Enter a Windows authority if you want to use another security context for the program than the security context of the PRTG probe service.
Username	Enter the username for Windows access.
Password	Enter the password for Windows access.
Timeout	Enter a timeout in seconds. After this time has passed, PRTG stops the process if it has not terminated yet. Please enter an integer value.

SEND AMAZON SIMPLE NOTIFICATION SERVICE MESSAGE

AWS Access Key ID	Enter your access key as shown in your login area at aws.amazon.com. Please enter a string.
AWS Secret Access Key	Enter your secret access key as shown in your login area at aws.amazon.com. Please enter a string.
Location	Define the location of your Amazon service. Choose one of the shown locations: ▪ US-East (Northern Virginia) ▪ US-West (Northern California) ▪ EU West (Ireland) ▪ US West (Oregon) ▪ Asia Pacific (Singapore) ▪ Asia Pacific (Tokyo) ▪ Asia Pacific (Sydney) ▪ South America (Sao Paulo) ▪ EU Central (Frankfurt)
ARN	Enter the Amazon resource name. Please enter a string.
Subject	Enter the subject of the message. Please enter a string. ⓘ The maximum length for the subject is 202 characters. Characters that exceed this number will be cut off.
Message	Define the message. A message with information about the sensor status is already predefined. Several placeholders 2933 (variables) are used here. You can change it to your liking. To reset this field to its default value, enter a single star symbol * (and nothing else). ⓘ The message part is only sent if you use email based notifications delivered by Amazon SNS. For SMS delivery, only the subject is sent while the message part is ignored because of SMS size restrictions.

ASSIGN TICKET

Regardless of the **Notification Summarization** method chosen above, PRTG sends notifications of the type **Assign Ticket** always as soon as possible (ASAP). They are never summarized.

For details about the ticket system, please see manual section **Tickets** 200.

Assign to User or User Group	Specify whether to assign the notification ticket to a user group or to a single user. Choose between: ▪ **To User Group**: Select a user group below to which PRTG assigns this ticket. ▪ **To User**: Select the dedicated user below to whom PRTG assigns this ticket.
Assign Ticket to this User Group / User	Select the user resp. user group to which PRTG assigns the notification ticket.
Subject	Enter the subject of the ticket. Several placeholders (variables) are used here by default. You can change it to your liking.
Content	Define the message in the ticket. A message with information about the sensor status is already predefined. Several placeholders 2933 (variables) are used here. You may change it as you wish.
When Condition Clears	Specify if PRTG closes the ticket automatically when the defined trigger condition clears. Choose between: ▪ **Close ticket automatically (recommended)**: PRTG closes the ticket automatically if the trigger condition is not met anymore. ▪ **Leave ticket open**: PRTG does not close the ticket after the condition has cleared.

Click **Save** to save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Script World Notifications

In addition to the built-in notification, you can create your own notifications. Just write a script or a program and use it with an **Execute Program** notification or execute an HTTP action. There are already many free, useful scripts, plugins, and add-ons for PRTG in the **PRTG Script World** available for download. Here is a list of the custom notifications that you can find there.

- How to Send Custom HTML Notifications
- Microsoft Teams

- Sending Notifications Using Telegram Bots
- Slack

Others

For information about the comments and history tabs, please see **Object Settings** 188 section.

More

- **Application Programming Interface (API) Definition** 3174
- **Setting Up Notifications Based on Sensor Limits: Example** 2832
- **Setting up Notifications Based on Libraries: Example** 2840

Knowledge Base: What placeholders can I use with PRTG?

- https://kb.paessler.com/en/topic/373

Knowledge Base: Documentation of SNMP Traps Sent by PRTG

- https://kb.paessler.com/en/topic/1133

Knowledge Base: How can PRTG send instant messages to Jabber, ICQ, MSN, Yahoo, etc., using external software?

- https://kb.paessler.com/en/topic/14803

Knowledge Base: Which audible notifications are available in PRTG? Can I change the default sound?

- https://kb.paessler.com/en/topic/26303

Knowledge Base: How can I send push notifications with PRTG?

- https://kb.paessler.com/en/topic/60892

How can I include my own logo into HTML emails?

- https://kb.paessler.com/en/topic/65782

8.12.3 Account Settings—Notification Contacts

In the notification contacts settings you can define and change notification contacts for the currently logged in PRTG user. Notifications contacts contain information about how and where to PRTG will send you notifications 2829. They are unique for each user account. Recipients of notifications can be email addresses, phone numbers (PRTG on premises only), and push devices (these are Android 3082 or iOS 3082 devices or a Windows Phone 3083 with the corresponding PRTG app). This way, every user with a PRTG installation can individually define how and where to receive messages from PRTG.

When you set up one of the notification methods 2921 **Send Email**, **Send SMS/Pager Message**, or **Send Push Notification**, you can choose a PRTG user to send a notifications to all **active** notification contacts of this user. If you select a user group, PRTG sends the notification to all contacts of all users that this group contains. A user can also pause one or more of the contacts to temporarily not receive any messages with this recipient.

If you use PRTG on premises and open the system administration page from another administration page, PRTG will ask you to enter your credentials again for security reasons if 15 minutes (900 seconds) have passed since your last credential-based login. A dialog box will appear. Enter your **Login Name** and **Password** for PRTG in the corresponding fields and confirm to continue.

Note

This section describes one of four steps to set up the notification system in PRTG. A complete notification setup involves:

1. Checking and setting up the **Notification Delivery** settings. This tells PRTG how and where to send messages.
   For detailed information, see **System Administration—Notification Delivery** 2961.
2. Checking and setting up **Notification Contacts** for the users of your PRTG installation. This defines where to send notifications.
   For detailed information, see **Account Settings—Notification Contacts** 2934.
3. Checking and setting up **Notifications**. This defines the kind of message and its content.
   For detailed information, see **Account Settings—Notifications** 2916.
4. Checking and setting up **Notification Triggers** for objects. This provokes the defined notifications.
   For detailed information, see **Sensor Notifications Settings** 2791.

We recommend that you always set up at least two notifications with different delivery methods for a notification trigger, for example, one email notification 2922 and one SMS notification 2924. If delivery via email fails (due to an email server failure or other reasons), PRTG can still notify you via your smartphone. Simply set your latency setting to a state trigger 2793 and a notification via a delivery method other than the one for the first trigger. Or set up a second trigger with another notification for the corresponding object.

For background information, please see the **Notifications** 2829 section.

Notification Contacts Overview

Click on the **Notification Contacts** tab to show a list of all existing notification contacts of the currently logged in PRTG user. Using the buttons in the particular contact rows, you can do the following:

- **Pause**: Pause this notification contact. If a notification contact is paused 214, PRTG does not send any messages to this contact when a notification for this user is triggered.
- **Edit**: Open the settings of this notification contact 2935 and change its description and recipient.
  This is not possible for predefined notification contacts, for example, the primary email address. You can change the primary email address under **Account Settings—My Account** 2909.
- **Delete**: Delete this notification contact.
  This is not possible for predefined notification contacts, for example, the primary email address.

Notification Contacts Settings

Click **Add Email Contact** button or **Add SMS Contact** button (PRTG on premises only) to add a new notification contact, or click the **Edit** button of an existing notification contact to edit it. A dialog box appears where you can enter the contact settings.

PRTG adds push contacts automatically for the corresponding user when you install a PRTG mobile app on your smartphone or tablet, connect to the PRTG server, and activate push notifications. You cannot add push contacts manually. If your mobile device rejects push notifications actively for an existing push contact, for example, because you deactivated push on the target device or reset it, the PRTG server will pause this contact automatically. The affected PRTG user account will receive a ToDo ticket 201 in this case.

ADD NEW / EDIT NOTIFICATION CONTACT

Description	Enter a meaningful name for the notification contact, for example, SMS to Admin Mobile or similar.
Recipient	Enter a valid email address for the contact type **Email**. On PRTG on premises instances you can add an **SMS** contact by entering a valid phone number. The format of the phone number depends on the SMS provider. Usually, you use a plus sign "+", followed by country code and number. For example, enter +1555012345 Ensure the number format meets the requirements of your SMS provider or the hardware that you use in combination with an API call. Sometimes a preceded plus sign is not required. A wrong format may result in undelivered messages!

ADD NEW / EDIT NOTIFICATION CONTACT

	For the contact type **Push**, this field shows a unique token that you cannot change here. This token is needed to send push notifications through the cloud. For details, see this Knowledge Base article: How can I use push notifications with PRTG?
Contact Type	Shows the type of contact, either **Email**, **SMS** (PRTG on premises only), or **Push**. This setting is shown for your information only and cannot be changed here. If you want to use another contact type, create a new contact with **Add Email Contact** or **Add SMS Contact** (PRTG on premises only), or activate push notifications in your PRTG for iOS, Android, or Windows Phone app.

Click the **Save** or **Add** button to save your settings, or click **Cancel** to close the dialog box without changes to your configuration.

A cloud contact is added automatically when you install the PRTG app on your smartphone, connect to the PRTG server, and enable push notifications.

More

Knowledge Base: How can I use push notifications with PRTG?

- https://kb.paessler.com/en/topic/60892

Setup—Topics

- Account Settings—My Account 2909
- Account Settings—Notifications 2916
- Account Settings—Notification Contacts 2934
- Account Settings—Schedules 2938
- System Administration—User Interface 2943
- System Administration—Monitoring 2955
- System Administration—Notification Delivery 2961
- System Administration—Core & Probes 2967
- System Administration—User Accounts 2975
- System Administration—User Groups 2982
- System Administration—Cluster 2992
- System Administration—Administrative Tools 2987
- PRTG Status—System Status 2994
- PRTG Status—Auto-Update 3005
- PRTG Status—Cluster Status 3010
- PRTG Status—Activation Status 3012
- Downloads and Add-Ons 3018
- Desktop Notifications 3020
- Support—Contact Support 3022

Others

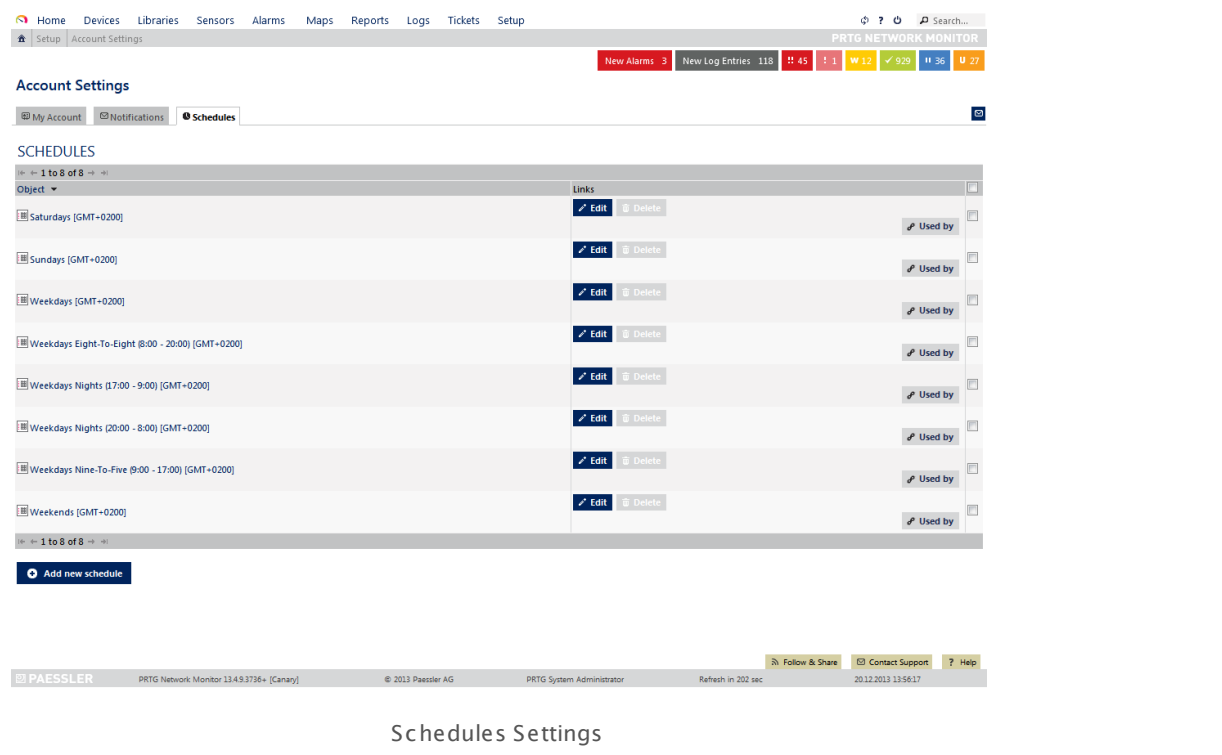
There are some settings that you must make in the PRTG Administration Tool 3134, available as native Windows application. For more details, please see the sections:

- PRTG Administration Tool on Core Server System 3135
- PRTG Administration Tool on Remote Probe System 3157

8.12.4 Account Settings—Schedules

In the schedule settings you can define or change schedules for the currently logged in user. You can use schedules to pause 214 monitoring/notification at for certain time periods with the period lists option. Also you can activate it at certain times with the time table option. You can also use schedules to define the time periods that are to be covered when creating reports 2862 .

If you use PRTG on premises and open the system administration page from another administration page, PRTG will ask you to enter your credentials again for security reasons if 15 minutes (900 seconds) have passed since your last credential-based login. A dialog box will appear. Enter your **Login Name** and **Password** for PRTG in the corresponding fields and confirm to continue.



Schedules Settings

Schedules Settings

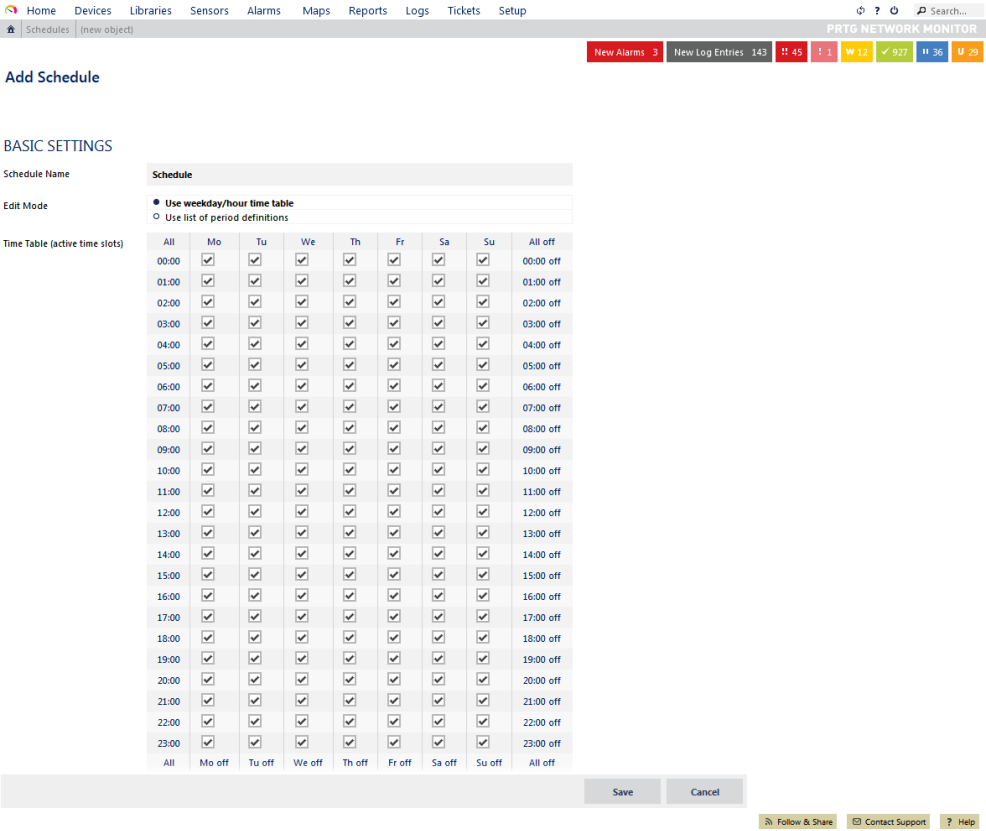
This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

Click on the **Schedules** tab to show a list of all existing schedules. By following the links next to the notification name, you can perform the following actions:

- **Delete**: Delete this notification (not possible for predefined notifications)
- **Used by**: Show a list of objects using this notification.

Please also see Working with Table Lists 207. Additionally, the multi-edit functionality is available. This enables you to change properties of several objects simultaneously via bulk changes. For more details, see the Multi-Edit Lists 2814 section.

Click the **Add new schedule** button or click the name of an existing notification to edit.



Edit Schedule Time Table

BASIC SETTINGS

Schedule Name	Enter a meaningful name for the schedule that describes the defined time span(s) or their purpose.
Edit Mode	Select how you want to define a schedule. Choose between: ▪ **Use weekday/hour time table**: Define a schedule by adding check marks to available checkboxes. The lowest possible increment is one hour. ⓘ This time table defines which time slots are active.

BASIC SETTINGS

- **Use list of period definitions**: Define a schedule by entering text lines using a specific syntax (see below).
  This time table defines which time slots are inactive.

Time Table

This selection is only visible if you enable the time table option above. Define the schedule. It will be used for monitoring objects, reporting, and notifications.

You can set time spans with a precision of one full hour by adding check marks. If a box is checked, it means the object is active during this hour, if unchecked, the object will be paused during this hour. You can set check marks individually, or change complete ranges for certain days of the week or time spans.

- To add ranges of check marks, use the buttons **All**, **Mo**, **Tu**, **We**, **Th**, **Fr**, **Sa**, and **Su**, as well as the time buttons on the left side.
- To remove ranges of check marks, use the buttons **All Off**, **Mo Off**, **Tu Off**, **We Off**, **Th Off**, **Fr Off**, **Sa Off**, and **Su Off**, as well as the time **Off** buttons on the right side.

Period List

This field is only visible if you enable period definitions above. Define the date/time ranges in which the objects using this schedule will be inactive (for example, paused). During other times, the objects will be active. Enter the ranges in this format:

- **ww:hh:mm-ww:hh:mm**

Ensure you enter each period exactly in the required syntax! Otherwise you will receive an error message. Please go back to the schedule and correct the according entry in this case.

For details and examples, see Schedules Settings—Period Definition Syntax 2941 below.

Schedules use the time zone of the computer on which your PRTG core server is running. This may diverge to other time displays in PRTG which are saved in UTC.

- If you define a schedule with the Time Table option in the schedule settings 2939, the time to which the schedule applies is converted to the time zone of your PRTG user account 2913. This means that the schedule is executed according to the time that your user account shows.
- If you use the Period List option, PRTG will not adjust the schedule to the time zone of your user account! The schedule will apply according to the time on your PRTG server in this case. Because of this, you will encounter time shifts for schedules if there are changes to the time zone on the server or in case of different daylight saving and standard time changes.

ACCESS RIGHTS

User Group Access	Define which user group(s) will have access to the object that you are editing. A table with user groups and rights is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ **Inherited**: Use the settings of the parent object. ▪ **None**: Users in this group cannot see or edit the object. The object does not show up in lists. ▪ **Read**: Users in this group can see the object and review its settings. ▪ **Write**: Users in this group can see the object, as well as review and edit its settings. However, they cannot edit access rights settings. ▪ **Full**: Users in this group can see the object, as well as review and edit its settings as well as edit access rights. You can create new user groups in the **System Administration—User Groups** 2982 settings.

Click **Save** to save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Schedules Settings—Period Definition Syntax

Define one or more periods of time during which the object using this schedule will be inactive. In each line, enter one range in the format ww:hh:mm-ww:hh:mm: weekday, hour, minute.

- **Possible values for** ww: mo, tu, we, th, fr, sa, su.
- **Possible values for** hh: Enter the hour in 24 hour format (no AM/PM allowed), for example, a number between 00 and 23.
- **Possible values for** mm: Enter the minute, for example, a number between 00 and 59.

Example

This example shows a schedule that pauses an object during the weekend as well as on Wednesday evenings.

```
fr:19:30-mo:06:05
we:18:45-we:23:00
```

Any object using this schedule will be paused from Friday, 7:30 p.m. to Monday, 6:05 a.m. as well as on Wednesday from 6:45 p.m. to 11 p.m. It will be active during the other times.

Others

For information about the comments and history tabs, see the **Object Settings** 188 section.

8.12.5 System Administration—User Interface

In the user interface settings you can define global values regarding the PRTG web site appearance, PRTG web server settings and performance, geo maps, and graph settings.

If you use PRTG on premises and open the system administration page from another administration page, PRTG will ask you to enter your credentials again for security reasons if 15 minutes (900 seconds) have passed since your last credential-based login. A dialog box will appear. Enter your **Login Name** and **Password** for PRTG in the corresponding fields and confirm to continue.

User Interface Settings

This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

WEBSITE

PRTG Site Name	When using the web interface, the site name is shown in the title bar of your browser window. It is also used by default in notification emails. Please enter a string.
DNS Name	If your PRTG web interface is (additionally) reachable via a DNS name, enter it here. It is used, for example, by default in notification emails to generate links. Please enter a string. This option is not available in PRTG on demand.
Website Language	Choose the system language from the dropdown list. Default is **English**. Depending on your installation, you may be able to choose other languages here. This setting defines the language of the PRTG web interface 136, as well as of the **PRTG Administration Tool** 3134. If you change this setting, PRTG needs to restart the core server to apply your changes. After clicking the **Save** button, a dialog box appears which asks you to confirm the required core server restart. Click **OK** to trigger the restart and follow the instructions on the screen. During the restart all the users of the PRTG web interface, of the **Enterprise Console** 3028, or of **PRTG Apps for Mobile Network Monitoring** 3082 will be disconnected and reconnected.
Graph Type	Select how graphs will be displayed throughout the web interface and in reports 2862.

WEBSITE

- **Use area graphs (recommended)**: Display filled graphs.
- **Use line graphs**: Display graphs using single lines only.

We recommend using area charts, as they're better to read.
Graphs containing data from more than one cluster node will always be displayed with line graphs automatically.

Automatic Logout

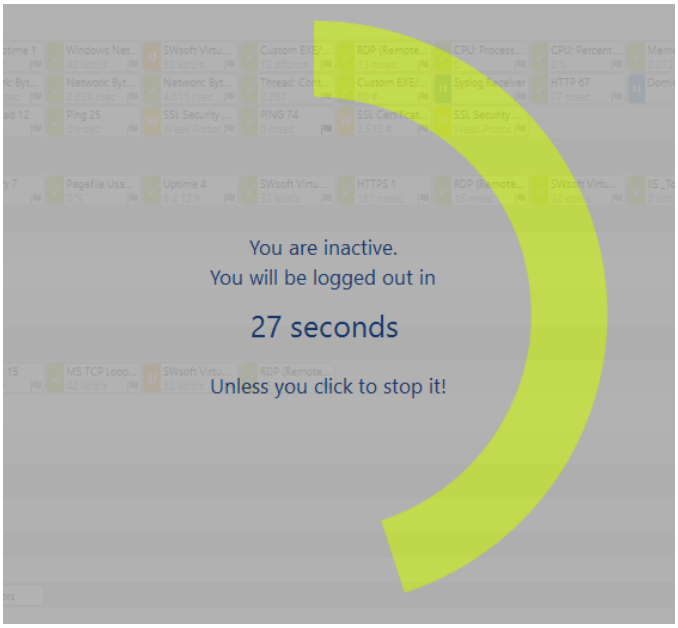
Define if a user who is inactive for a certain period of time will be logged out from the PRTG interface automatically for security reasons. Choose between:

- **Keep user logged in, even for a longer period of inactivity.**
- **Logout user automatically after a certain period of inactivity.**

Automatic Logout after Minutes

This field is only visible if you select the logout option above. Specify in minutes after which time of inactivity a user will be logged out automatically. Please enter an integer value. PRTG will redirect to the login page once this time has expired.

If the value you enter here is greater than 1 minute, a logout countdown will appear 1 minute before you are logged out. If the value is 1 minute, you will see the logout countdown 30 seconds before you are logged out. Click into the browser to stop the countdown and stay logged in.



Logout Countdown

WEBSITE

Google Analytics Tracking ID

You can track the usage of PRTG web pages with Google Analytics by entering your Google Universal Analytics Tracking ID into this field. You need a Google Analytics account for this feature. Create a tracking ID within the Google Analytics portal and provide it here. PRTG will then dynamically integrate it into the website.

Please enter a string or leave the field empty. The string will look like this: **UA-xxxxxx-xx**

For details, please see this Knowledge Base article: How can I integrate Google Analytics in PRTG?

This option is not available in PRTG on demand.

GEO MAPS

Map Service Provider

Select if and how you want to integrate the Geo Maps feature into the web interface. If enabled, PRTG uses the first line of the location setting of an object to show it on a geographical map. Please choose a map provider:

- **Do not show maps (disables Geo Maps integration)**: Disable Geo Maps integration and do not show geographical maps in the web interface.
- **Default (recommended)**: The recommended default option currently reroutes the map requests to Nokia Maps. See this blog article for details: **Geo Maps Requires a Change of Map Service Provider**
- **Nokia Maps**: Use Nokia Maps to show geographical maps.
- **CloudMade (API key required)**: Use CloudMade to show geographical maps. Please sign up for an API key on their developer website to use this service.
- **Google Static Maps (API key required)**: Use Google Static Maps to show geographical maps. Please sign up for a Google Maps **API v3 key** to use this service as of PRTG version 13!

For more information about the different map providers, please see this Knowledge Base article: Which provider should I use for PRTG's "Geo Maps" feature?

GEO MAPS

Map Type	This setting is only visible for some map providers. Depending on the chosen provider, several options are shown. Each will show map tiles in a different appearance. Please choose a map type from the list.
API Key (required)	This field is only visible if you selected a provider that requires an API key. Please obtain your personal key and paste it here. For more information on how to get a Google API key, please see this Knowledge Base article: How do I get a Google Maps API key for use in PRTG?

WEB SERVER

Performance Strategy	Select if you want to enable performance improvements for the web interface. ▪ **All Features: Show all features and live data (recommended)**: Provide full functionality and show all menu items. ▪ **More Speed: Limit features and delay display (experimental)**: Improve reaction time and speed of the web interface by delaying display of monitoring data and hiding some features. For more information on how to speed up the web interface, please see this Knowledge Base article: How can I speed up PRTG—especially for large installations?
IP Address for Web Server	PRTG is running a web server in order to provide access via the web and Windows interface. Please specify the IP address this web server will run on. Later, you can log in to PRTG by simply pointing your browser to the specified IP address. Choose between: ▪ **Localhost, 127.0.0.1 (PRTG will not be accessible from other computers)**: Use 127.0.0.1 only. The PRTG web interface and the Enterprise Console will only be accessible from the computer PRTG is installed on. Either the selected port or at least one port in the range from **8080** to **8089** has to be available on 127.0.0.1. If you run PRTG on localhost, please do not use the DNS name http://localhost to log in to the web server, as this may considerably slow down the PRTG web interface. Please use your local IP address or http://127.0.0.1 instead.

WEB SERVER

- **All IPs available on this computer**: Use all IP addresses available on this computer and enable access to the web server for all of these addresses. The TCP port selected below must be free on every available IP address.

- **Specify IPs**: Select specific IP addresses on which the PRTG Web server will run. A list specific to your system is shown. Add a check mark in front of every IP address you want the PRTG web server to be available at. You can also select and deselect all addresses by clicking on the check box in the table header. Either the selected port or at least one port in the range from **8080** to **8089** has to be available on the specified IP address.

Regardless of the selected setting above, one port in the range from **8080** to **8180** has to be available on the specified IP address so PRTG can create reports. The report engine will try to connect to the core server on one of these ports.

If PRTG does not find a network card on startup it will switch the IP setting to **Localhost**. This setting will remain, even if a network card is available later on. If you disabled or removed the network card on the machine running the PRTG core server, please re-check this setting.

If you change this setting, PRTG needs to restart the core server to apply your changes. After clicking the **Save** button, a dialog box appears which asks you to confirm the required core server restart. Click **OK** to trigger the restart and follow the instructions on the screen. During the restart all the users of the PRTG web interface, of the [Enterprise Console](3028), or of [PRTG Apps for Mobile Network Monitoring](3082) will be disconnected and reconnected.

This option is not available in PRTG on demand.

TCP Port for Web Server

PRTG runs a web server in order to provide access via the web interface and the Enterprise Console. Please specify on which port this web server will run. Choose between:

WEB SERVER

- **Secure HTTPS server (recommended, mandatory for internet access)**: We recommend this setting and you need it to access the PRTG server via the internet. Use a secure HTTPS connection that is encrypted via SSL on port 443.
  Although the connection is secure, you will see an SSL Certificate Warning 142 in your browser when logging in to the PRTG web interface, because the default certificate is unknown to your browser. You can install another SSL certificate for PRTG later. Please see Using Your Own SSL Certificate 3228.

  If port 80 is free, PRTG will reserve it as well. When users try to connect on port 80 via HTTP, they will then be redirected to port 443 via HTTPS. You can change this behavior by using a registry setting.
  If port 443 is not available, PRTG will try port 8443 as fallback. If this port is also not available, PRTG searches from port 32000 upwards for a free port. PRTG will send a ticket 200 that shows you the currently used port number and will switch back to 443 as soon as it is available again.
- **Insecure HTTP server (standard port 80, not recommended)**: Use a standard web server without SSL encryption on port 80. This setting is not recommended for WAN connections.
  If you use an insecure web server on the internet, attackers could potentially spy on credentials you enter into PRTG. We strongly recommend that you use this option in a LAN only.
- **Expert configuration**: This setting allows you to specify a custom web server port and the security of the connection. This option is intended for systems with an existing web server on the standard port. Define port and encryption below.
  If PRTG always uses a fallback port after a server restart, check for other programs that use the same port as PRTG. For example, the Microsoft IIS web server also uses the port 80 (443 for SSL) by default and blocks it. Please disable such programs and services on startup.

If you change this setting, PRTG needs to restart the core server to apply your changes. After clicking the **Save** button, a dialog box appears which asks you to confirm the required core server restart. Click **OK** to trigger the restart and follow the instructions on the screen. During the restart all the users of the PRTG web interface, of the Enterprise Console 3028, or of PRTG Apps for Mobile Network Monitoring 3082 will be disconnected and reconnected.

This option is not available in PRTG on demand.

WEB SERVER

Web Server Port

You will see this setting only if you select **Expert configuration** above. Enter the TCP port number you want the PRTG web server to run on. Please enter an integer value.

If you use a secure connection and port 80 is free, PRTG will reserve it as well. When users try to connect on port 80 via HTTP, they will be redirected to the custom port via HTTPS. You can change this behavior by using a registry setting.

If the defined port for a secure connection is not available, PRTG will try port 8443 as fallback. If this port is also not available, PRTG searches from port 32000 upwards for a free port. PRTG sends a ticket [200] that shows you the currently used port number and will switch back to the original port as soon as it is available again.

If you change this setting, PRTG needs to restart the core server to apply your changes. After clicking the **Save** button, a dialog box appears which asks you to confirm the required core server restart. Click **OK** to trigger the restart and follow the instructions on the screen. During the restart all the users of the PRTG web interface, of the **Enterprise Console** [3028], or of **PRTG Apps for Mobile Network Monitoring** [3082] will be disconnected and reconnected.

This option is not available in PRTG on demand.

Web Server Security

You will see this setting only if you select **Expert configuration** above. Specify if you want to use an SSL encryption. Choose between:

- **Use SSL encryption (HTTPS)**: Use a secure HTTPS connection that is encrypted via SSL on a custom port as defined above.
  Although the connection is secure, you will see an **SSL Certificate Warning** [142] in your browser when you log in to the PRTG web interface, because the default certificate is unknown to your browser. You can install another SSL certificate for PRTG later. Please see **Using Your Own SSL Certificate** [3228].
- **Don't use encryption (not recommended)**: This setting is not recommended for WAN connections. Use a standard web server without SSL encryption on a custom port as defined above.

If you use a web server without encryption on the internet, attackers could potentially spy on credentials you enter into PRTG. We strongly recommend that you use this option in a LAN only.

WEB SERVER

If you change this setting, PRTG needs to restart the core server to apply your changes. After clicking the **Save** button, a dialog box appears which asks you to confirm the required core server restart. Click **OK** to trigger the restart and follow the instructions on the screen. During the restart all the users of the PRTG web interface, of the Enterprise Console 3028, or of PRTG Apps for Mobile Network Monitoring 3082 will be disconnected and reconnected.

This option is not available in PRTG on demand.

SSL Security

Specify the security level which will be used for SSL connections from and to the PRTG web server. Choose between:

- **High security (recommended)**: The web server will only accept high security connections from clients like web browsers, apps 3082, the Enterprise Console 3028, or API clients. These clients must be able to support modern ciphers which support authentication and encryption of 128 bits or stronger and forward secrecy. All modern web browsers do this.
- **Weakened security (necessary for old web browser and old client software)**: If you have clients which do not support the high security setting, you can choose this 'normal security level' setting to connect (for example, older browsers, browsers running on Windows XP, some default browsers on Android systems). However, we strongly recommend that you update your clients in this case.

This option is not available in PRTG on demand.

Currently Active IP Address/Port Combination(s)

Shows all currently active combinations of IP addresses and ports on which the PRTG server listens for web requests. This setting is shown for your information only and cannot be changed here.

PRTG internally uses port 8085 for report generation.

This option is not available in PRTG on demand.

GRAPH SETTINGS: SELECT FOR HOW MANY DAYS HISTORIC DATA REMAINS ACCESSIBLE

PRTG shows several graphs in the objects' detail pages 166 in the web interface. These are kept in RAM memory for fast display without causing extra CPU load or disk usage. The longer the time frames and the shorter the intervals are, the more memory will be used for this. You can adapt the details for all four graphs. This setting will also change the caption of the objects' tabs in the web interface 136 and Enterprise Console 3028.

If you change this setting, PRTG needs to restart the core server to apply your changes. After clicking the **Save** button, a dialog box appears which asks you to confirm the required core server restart. Click **OK** to trigger the restart and follow the instructions on the screen. During the restart all the users of the PRTG web interface, of the **Enterprise Console** 3028, or of **PRTG Apps for Mobile Network Monitoring** 3082 will be disconnected and reconnected.

Live Graph	The live graph is available for sensors only. For the live graph, no fixed time span is given, but you can define how many values will be displayed. The actual time span covered by the live graph depends on the scanning interval set for the sensor you're viewing and is calculated automatically. By default, **120 Values** is set, which results in a graph covering a time span of two hours, if a scanning interval of 60 seconds is set for the sensor. Other scanning intervals will result in graphs covering different time spans. Choose between: ▪ **60 Values**: This corresponds to a live graph covering a time span of one hour if a 1 minute scanning interval is set. Uses least RAM memory. We recommend this setting for installations with 10,000 sensors or more. ▪ **120 Values**: This corresponds to a live graph covering a time span of two hours if a 1 minute scanning interval is set. ▪ **240 Values**: This corresponds to a live graph covering a time span of four hours if a 1 minute scanning interval is set. ▪ **480 Values**: This corresponds to a live graph covering a time span of eight hours if a 1 minute scanning interval is set. ▪ **960 Values**: This corresponds to a live graph covering a time span of 16 hours if a 1 minute scanning interval is set. Uses most RAM memory.
Graph 1	By default, this is the **2 days** graph in the web interface. You can change it to more or less detail by choosing a time span and a monitoring interval average associated with it. Monitoring results will be averaged regardless of the actual scanning interval set for the sensors. Choose between: ▪ **1 day with 1 minute averages**: Results in 1440 values. ▪ **1 day with 5 minutes averages**: Results in 288 values.

GRAPH SETTINGS: SELECT FOR HOW MANY DAYS HISTORIC DATA REMAINS ACCESSIBLE

	▪ **1 day with 15 minutes averages**: Results in 96 values. Uses least RAM memory. We recommend this setting for installations with 10,000 sensors or more. ▪ **2 days with 1 minute averages**: Results in 2880 values. Uses most RAM memory. ▪ **2 days with 5 minutes averages**: Results in 576 values. ▪ **2 days with 15 minutes averages**: Results in 192 values. ▪ **4 days with 1 hour averages**: Results in 96 values. Uses least RAM memory. We recommend this setting for installations with 10,000 sensors or more.
Graph 2	By default, this is the **30 days** graph in the web interface. You can change it to more or less detail by choosing a time span covered and a monitoring interval average associated with it. Choose between: ▪ **10 days with 1 hour averages**: Results in 240 values. ▪ **20 days with 1 hour averages**: Results in 480 values. ▪ **30 days with 1 hour averages**: Results in 720 values. ▪ **30 days with 6 hour averages**: Results in 120 values. Uses least RAM memory. We recommend this setting for installations with 10,000 sensors or more. ▪ **40 days with 1 hour averages**: Results in 960 values. ▪ **40 days with 6 hour averages**: Results in 160 values. ▪ **60 days with 1 hour averages**: Results in 1440 values. Uses most RAM memory. ▪ **60 days with 6 hour averages**: Results in 240 values.
Graph 3	By default, this is the **365 days** graph in the web interface. You can change it to more or less detail by choosing a time span covered and a monitoring interval average associated with it. Choose between: ▪ **100 days with 1 day averages**: Results in 100 values. Uses least RAM memory. We recommend this setting for installations with 10,000 sensors or more. ▪ **200 days with 1 day averages**: Results in 200 values. ▪ **365 days with 1 day averages**: Results in 365 values.

GRAPH SETTINGS: SELECT FOR HOW MANY DAYS HISTORIC DATA REMAINS ACCESSIBLE

- **400 days with 1 day averages**: Results in 400 values.
- **750 days with 1 day averages**: Results in 750 values. Uses most RAM memory.

REPORT COMMENTS

Introduction	Define a custom text that will show up on the first page of the report. Please enter a string or leave the field empty.
Footer Comments	Define a custom text that will show up on the last page of the report. Please enter a string or leave the field empty.

Click **Save** to save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

More

Knowledge Base: What placeholders can I use with PRTG?

- https://kb.paessler.com/en/topic/373

Knowledge Base: How can I speed up PRTG—especially for large installations?

- https://kb.paessler.com/en/topic/2733

Knowledge Base: Which provider should I use for PRTG's "Geo Maps" feature?

- https://kb.paessler.com/en/topic/34603

Knowledge Base: Which domains and ports does the GeoMaps feature use?

- https://kb.paessler.com/en/topic/35823

Knowledge Base: How do I get a Google Maps API key for use in PRTG?

- https://kb.paessler.com/en/topic/32363

Knowledge Base: Which limitations apply when using the Google Maps API in PRTG?

- https://kb.paessler.com/en/topic/7913

Knowledge Base: How and where does PRTG store its data?

- https://kb.paessler.com/en/topic/463

Knowledge Base: How can I integrate Google Analytics in PRTG?

- https://kb.paessler.com/en/topic/61406

Paessler Blog: Geo Maps Requires a Change of Map Service Provider

- https://www.paessler.com/blog/2016/07/12/all-about-prtg/geo-maps-requires-a-change-of-map-service-provider

8.12.6 System Administration—Monitoring

In the monitoring settings you can define global values regarding scanning intervals, unusual and similar sensors detection, auto-discovery, and uptime threshold.

If you use PRTG on premises and open the system administration page from another administration page, PRTG will ask you to enter your credentials again for security reasons if 15 minutes (900 seconds) have passed since your last credential-based login. A dialog box will appear. Enter your **Login Name** and **Password** for PRTG in the corresponding fields and confirm to continue.

Monitoring Settings

This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

SCANNING INTERVALS

This option is not available in PRTG on demand.

Available Intervals	Define the intervals available in the dropdown list of every object's settings 188. In the text field, enter one value in each line. Use **s**, **m**, **h**, and **d** for defining seconds, minutes, hours, and days. By default, there are the following scanning intervals defined: **30s**: 30 seconds **1m**: 1 minute **5m**: 5 minutes **10m**: 10 minutes **15m**: 15 minutes **30m**: 30 minutes **1h**: 1 hour **4h**: 4 hours **6h**: 6 hours **12h**: 12 hours **1d**: 1 day

SCANNING INTERVALS

We recommend that you do not use intervals shorter than 10 seconds to prevent system overload. Intervals below 10 seconds are not officially supported! The maximum supported scanning interval is 10 days.

You can also define specific points in time to indicate when PRTG executes scanning actions. Enter up to 50 concrete UTC points in time according to the formula

@ UTC hh:mm, hh:mm

Your local time may be different from the UTC time!

For more information on how to set specific points in time as a scanning time for sensors, see this Knowledge Base article: Can I set a sensor to run at a specific time?

UNUSUAL DETECTION

The unusual detection can set sensors to an **Unusual** status 163 when there are values that are untypical for the time span in which they are measured. PRTG compares the current average values to the historic monitoring results for this purpose. If the current values show a big difference to the values that are normally retrieved by a sensor, this sensor will indicate this with the unusual status.

You can define the granularity of the unusual detection here (this means, how big the difference must be to cause an unusual status). If you disable the unusual detection (both settings to **Never**), sensors will never show an unusual status.

You can enable and disable unusual detection for specific devices, entire groups, and probes in the respective **Object Settings** 188.

Show Unusual When	Define when a sensor shows the unusual status, comparing the weekday. If you enable the detection here, the average of the values which were measured on the day before is compared to the average of the same weekday in previous weeks. Choose between: ▪ **Never**: Disable unusual detection for weekday average. ▪ **24h average is <80% or >120% of weekday average**: The average of the values measured on the day before is either lower than 80% or higher than 120% than usually on the same weekday.

UNUSUAL DETECTION

- **24h average is <50% or >200% of weekday average**: The average of the values measured on the day before is either lower than 50% or higher than 200% than usually on the same weekday.
- **24h average is <20% or >500% of weekday average (recommended)**: The average of the values measured on the day before is either lower than 20% or higher than 500% than usually on the same weekday.
- **24h average is <10% or >1,000% of weekday average**: The average of the values measured on the day before is either lower than 10% or higher than 1,000% than usually on the same weekday.
- **24h average is <1% or >10,000% of weekday average**: The average of the values measured on the day before is either lower than 1% or higher than 10,000% than usually on the same weekday.

For example, consider a traffic sensor that usually measures 100 MB average traffic on a weekday. If you choose the first option, it would show an unusual status if the average from the day before is below 80 MB or above 120 MB.

Show Unusual When

Define when a sensor shows the unusual status, comparing the hour-of-day. If you enable the detection here, the average of the values which were measured in the hour before is compared to the average of the same hour on the same weekday in previous weeks. Choose between:

- **Never**: Disable unusual detection for hour-of-day average.
- **Hourly average is <80% or >120% of hour-of-day average**: The average of the values measured in the hour before is either lower than 80% or higher than 120% than usually in this hour of this weekday.
- **Hourly average is <50% or >200% of hour-of-day average**: The average of the values measured in the hour before is either lower than 50% or higher than 200% than usually in this hour of this weekday.
- **Hourly average is <20% or >500% of hour-of-day average (recommended)**: The average of the values measured in the hour before is either lower than 20% or higher than 500% than usually in this hour of this weekday.
- **Hourly average is <10% or >1,000% of hour-of-day average**: The average of the values measured in the hour before is either lower than 10% or higher than 1,000% than usually in this hour of this weekday.

UNUSUAL DETECTION

- **Hourly average is <1% or >10,000% of hour-of-day average**: The average of the values measured in the hour before is either lower than 1% or higher than 10,000% than usually in this hour of this weekday.

Consider a traffic sensor that usually measures 10 MB average traffic within an hour. If you choose the first option, it would show an unusual status if the average from the hour before is below 8 MB or above 12 MB.

Logging

Define if unusual events will be written to the log file. Choose between:

- **Do not log unusual events**
- **Write unusual events into the log**

SIMILAR SENSORS DETECTION

Similar sensors detection enables PRTG to analyze sensor data for similarities. The detection will run in the background with low priority. The recommended setting for similar sensors detection is to let PRTG automatically decide how many channels will be analyzed. However, you can also override this setting.

When similar sensors analysis is turned off or you have exceeded 1,000 sensors and have chosen the automatic analysis depth option, the similar sensors entry will not be shown in the main menu bar.

Analysis Depth

Define the number of channels PRTG will analyze to detect similarities between sensors or turn the analysis off. Choose between:

- **Manage automatically based on sensor count (recommended)**: The analysis depth depends on the total number of sensors you have configured. PRTG will analyze all channels for up to 500 sensors, and only the primary sensor channels for up to 1,000 sensors. If exceeding 1,000 sensors, the analysis will be turned off.
- **Analyze primary channels only**: Only the primary channels of sensors are analyzed. Be aware of potentially high CPU load of PRTG when choosing this setting for more than 1,000 sensors.
- **Analyze all channels (higher CPU load)**: Similarity detection is applied to all channels. Be aware of potentially high CPU load of PRTG when choosing this setting for more than 500 sensors.

SIMILAR SENSORS DETECTION

- **Turn analysis off**: No similarity detection takes place. Choose this option if you are not interested in the analysis results or you want to keep the CPU load of PRTG at a minimum.

RECOMMENDED SENSORS DETECTION

With the sensor recommendation engine, PRTG can analyze devices in your network and suggest sensors that are still missing for a complete monitoring. The analysis runs with low priority in the background when you add a new device, when the last analysis was executed more than 30 days ago, or when you manually start 185 it.

See the manual section **Recommended Sensors** 184 for more information, for example, on SNMP settings 185, on the results 185 you get and on how you add the suggested sensors 186.

This option is not available in PRTG on demand.

Detection Engine

Define if you want PRTG to analyze your devices to recommend useful sensor types. Choose between:

- **Manage automatically based on sensor count (recommended)**: PRTG runs the detection engine for installations with up to 5,000 sensors by default. If you exceed this threshold, PRTG disables the detection engine for performance reasons. We recommend that you set this option so you do not miss any important monitoring data about your network, without risking to run into performance issues.
- **Always show recommendations**: PRTG always analyzes your devices even if your installation exceeds 5,000 sensors and you will never miss any suggestion to complete your monitoring. But if you enable this option, please keep in mind this setting in case you encounter performance issues.
- **Turn recommendations off**: PRTG never recommends sensors. Select this option if you have performance issues with PRTG or if you do not want to see this information on device overview tabs 166. Moreover, you will not find the option **Recommend Now** in device context menus 222 or on overview tabs anymore.

AUTO-DISCOVERY

Run Discovery at	Define the time when PRTG automatically runs an **Auto-Discovery** [249] in your network if you configured a daily or weekly **Discovery Schedule** in the auto-discovery group settings [251]. Choose a full hour between **0:00** and **23:00**. We recommend that you choose a time when there is little user activity in your network, because auto-discoveries can produce a certain amount of load.

UPTIME THRESHOLD

Desired Minimum Uptime	Define which uptime in percent PRTG regards as 100 percent. This setting affects the colors shown next to the sensor icons in reports. Select one of the predefined values between **90 %** and **99.999 %**.

Click **Save** to save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

More

Knowledge Base: How can I speed up PRTG—especially for large installations?

- https://kb.paessler.com/en/topic/2733

Knowledge Base: How and where does PRTG store its data?

- https://kb.paessler.com/en/topic/463

Knowledge Base: Can I set a sensor to run at a specific time?

- https://kb.paessler.com/en/topic/3723

8.12.7 System Administration—Notification Delivery

In the notification delivery settings you can define global settings for notification delivery. If you do not want to use a specific notification method, just leave the respective fields empty.

This option is not available in PRTG on demand.

If you use PRTG on premises and open the system administration page from another administration page, PRTG will ask you to enter your credentials again for security reasons if 15 minutes (900 seconds) have passed since your last credential-based login. A dialog box will appear. Enter your **Login Name** and **Password** for PRTG in the corresponding fields and confirm to continue.

Note

This section describes one of four steps to set up the notification system in PRTG. A complete notification setup involves:

1. Checking and setting up the **Notification Delivery** settings. This tells PRTG how and where to send messages.
   For detailed information, see **System Administration—Notification Delivery** 2961.
2. Checking and setting up **Notification Contacts** for the users of your PRTG installation. This defines where to send notifications.
   For detailed information, see **Account Settings—Notification Contacts** 2934.
3. Checking and setting up **Notifications**. This defines the kind of message and its content.
   For detailed information, see **Account Settings—Notifications** 2916.
4. Checking and setting up **Notification Triggers** for objects. This provokes the defined notifications.
   For detailed information, see **Sensor Notifications Settings** 2791.

We recommend that you always set up at least two notifications with different delivery methods for a notification trigger, for example, one email notification 2922 and one SMS notification 2924. If delivery via email fails (due to an email server failure or other reasons), PRTG can still notify you via your smartphone. Simply set your latency setting to a state trigger 2793 and a notification via a delivery method other than the one for the first trigger. Or set up a second trigger with another notification for the corresponding object.

For background information, please see the **Notifications** 2829 section.

Notification Delivery Settings

This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

SMTP DELIVERY

SMTP Delivery Mechanism	Define how PRTG sends emails using Simple Mail Transfer Protocol (SMTP). Choose between: ▪ **Direct delivery using built-in email relay server (default)**: Use the SMTP relay server built into PRTG. This server manages its own email queue. For each email, it looks up the target SMTP server via the MX record of the target domain, and send the email. ▪ **Use SMTP relay server (recommended inside LANs/NATs)**: Set up your own SMTP relay server to send emails. Enter data below. ▪ **Use two SMTP relay servers (primary and fallback server)**: Set up two own SMTP relay servers—one primary and one as fallback server. Enter data below. ⓘ When monitoring inside your NAT or LAN, it is often a good idea to use your own LAN-based relay server to deliver notification emails quicker.
Sender Email	Enter an email address to use as sender of all emails. This setting is global and can only be changed centrally here.
Sender Name	Enter a name to use as sender of all emails. This setting is global and can only be changed centrally here.
HELO Ident	Enter the HELO Ident for SMTP. This must be a unique name, preferably the DNS name of the machine running PRTG. See SMTP RFC 2821: The sender-SMTP must ensure that the domain parameter in a HELO command is a valid principal host domain name for the client host.
SMTP Relay Server	This field is only visible if you enable SMTP relay server above. Enter the IP address or DNS name of the SMTP relay server.
SMTP Relay SMTP Port	This field is only visible if you enable SMTP relay server above. Enter the port number the SMTP relay server is running on. Standard value is **25**.
SMTP Relay Authentication	This field is only visible if you enable SMTP relay server above. Select the kind of authentication required for the SMTP server. Choose between: ▪ **No authentication is required**: Use SMTP without authentication. ▪ **Use standard SMTP authentication**: Use standard authentication.

SMTP DELIVERY

	▪ **SASL authentication is required**: Use secure authentication via Simple Authentication and Security Layer (SASL).
SMTP Relay User	This field is only visible if you enable SMTP authentication above. Enter a valid username.
SMTP Relay Password	This field is only visible if you enable SMTP authentication above. Enter a valid password.
Use Encrypted Connection	This field is only visible if you enable SMTP relay server above. Enter the security level for SMTP connections. Choose between: ▪ **Never:** Use insecure connection with plain text transfer. ▪ **If supported by server:** Use a secure connection (default).
SSL Method	This setting is only visible if you enable SMTP relay server and encryption above. It is only relevant for secure connections. Select the SSL or TLS version that your SMTP device supports. We recommend that you use the default value. If you do not get a connection, try with another setting. Choose between: ▪ **SSL V2** ▪ **SSL V2 or V3** ▪ **SSL V3** ▪ **TLS V1**
SMTP Relay Server (Fallback)	
SMTP Relay SMTP Port (Fallback)	
SMTP Relay Authentication (Fallback)	These fields are only visible if you enable the option for two SMTP relay servers above. Please see also the settings that you made for your primary SMTP relay server.
Use Encrypted Connection (Fallback)	
SSL Method (Fallback)	
SMTP Relay User (Fallback)	

SMTP DELIVERY

SSL Method (Fallback)

SMTP Relay User (Fallback)

SMTP Relay Password (Fallback)

Security (Fallback)

SMS DELIVERY

Although PRTG has built-in support for the Application Programming Interface (API) of some SMS providers, we cannot officially provide support regarding these SMS service providers. If you have technical questions about SMS delivery beyond PRTG, please contact your SMS provider directly.

Instead of using a pre-configured provider you can always use a custom URL, enabling you to use extended parameters (this is also an alternative when using providers for which we offer pre-configured options).

You need an internet connection to send text messages via the HTTP API.

For information about sending SMS via separate hardware using third party software, please see this Knowledge Base article: How can I send SMS text message notifications via a modem or a mobile phone with PRTG?

Configuration Mode	Define how you want to select an SMS provider. Choose between: ▪ **Select an SMS provider from a list of providers**: Select a provider from a list below. ▪ **Enter a custom URL for a provider not listed**: Use another provider and enter the service URL manually below.
Service Provider	This field is only visible if you choose the provider list above. Select a service provider from the list. PRTG offers a small incomplete list of providers. Some providers might require a port configuration in your firewall. For details, please see this Knowledge Base article: Which URLs does PRTG use for its preconfigured SMS providers?
User	This field is only visible if you choose the provider list above. Enter a username for the service provider account.

SMS DELIVERY

Password	This field is only visible if you choose the provider list above. Enter a password for the service provider account.
API ID / Account	This field is only visible if you choose the provider list above. Some providers need an additional API ID or account information. If provided, enter it here. Please enter a string or leave the field empty.
Custom URL	This field is only visible if you enable the custom provider option above. From the documentation of your SMS provider, please enter the service URL that is used to send SMS messages. Use the following placeholders for the recipient phone number and the text message: ▪ **%SMSNUMBER** ▪ **%SMSTEXT** Please use the GET method to request the custom URL. POST requests are not supported.
Custom URL-SNI	Select if PRTG will send the SNI extension to the TLS protocol along with the HTTP request. Choose between: ▪ **Do not send SNI (default)**: PRTG will not send an SNI when executing the HTTP action. ▪ **Send SNI**: PRTG will send an SNI when calling the target URL. Specify the SNI below.
Virtual Host (SNI)	This field is only visible if you select the SNI option above. Enter the SNI name that your endpoint configuration requires. Usually, this is the Fully Qualified Domain Name (FQDN) of the virtual host.
Encoding for SMS	Define the encoding of the URL string that PRTG sends to your provider. Choose between: ▪ **ANSI local system codepage (default)** ▪ **UTF-8** ▪ **UTF-16**
Maximum Length of Text	Some SMS providers will not allow SMS messages exceeding a certain amount of characters. PRTG will restrict the number of characters according to the length specified in this field. A value of **0** means the SMS is sent at its full length.

The notification 2916 methods **Send SMS/Pager Message** and **Execute HTTP Action** will use the central proxy settings defined for your PRTG core server. For details, please see System Administration—Core & Probes 2967 (section **Proxy Configuration**).

Click **Save** to save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

More

Knowledge Base: How can I send SMS text message notifications via a modem or a mobile phone with PRTG?

- https://kb.paessler.com/en/topic/393

Knowledge Base: Why do I get a connection timeout message when sending SMS via bulksms?

- https://kb.paessler.com/en/topic/12253

Knowledge Base: Which URLs does PRTG use for its preconfigured SMS providers?

- https://kb.paessler.com/en/topic/13123

Knowledge Base: How can PRTG send instant messages to Jabber, ICQ, MSN, Yahoo, etc., using external software?

- https://kb.paessler.com/en/topic/14803

Knowledge Base: Can GMail / Google Apps be used for SMTP relay?

- https://kb.paessler.com/en/topic/2823

Knowledge Base: How can I enable Notification Delivery Logging?

- https://kb.paessler.com/en/topic/55363

Knowledge Base: How can I include my own logo into HTML emails?

- https://kb.paessler.com/en/topic/65782

8.12.8 System Administration—Core & Probes

In the core and probe management settings you can define settings for the core server, as well as the settings for probe connections if you use remote or mini probes.

If you cannot save changes to **Core & Probes** settings because you get an **Error (Bad Request)** with the message Active Directory Domain not accessible, ensure you provide the correct access type for your domain in section Active Directory Integration 2971! For example, change from "local user" to **Use explicit credentials** and provide correct credentials for the domain. Please note that PRTG automatically sets the access type "local system" by default, so you might need to change this.

If you use PRTG on premises and open the system administration page from another administration page, PRTG will ask you to enter your credentials again for security reasons if 15 minutes (900 seconds) have passed since your last credential-based login. A dialog box will appear. Enter your **Login Name** and **Password** for PRTG in the corresponding fields and confirm to continue.

Core and Probes Settings

This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

PROXY CONFIGURATION

This option is not available in PRTG on demand.

Use Proxy Server	We recommend that you use PRTG with a direct internet connection. However, if you need to use a proxy, you can configure the relevant settings here. Choose between: ▪ **No, use direct connection to the Internet (default)**: Do not use a proxy. Use this setting if there is a direct internet connection available to the server running the PRTG core server. ▪ **Yes, in our network a proxy is mandatory**: Define proxy settings below. Proxy settings are valid for Auto-Update 3005, Activate the Product 91, obtaining Geo Maps 2824 tiles, and for sending out HTTP, push, and SMS text message Notifications 2921. The sensor types Cloud HTTP 571 and Cloud Ping 580 use these proxy settings as well.

PROXY CONFIGURATION

Proxy Server	This setting is only visible if proxy usage is enabled above. Enter the address of the proxy server that you use for outbound connections. Please enter a valid address.
Port	This setting is only visible if proxy usage is enabled above. Enter the port number of the proxy server that you use for outbound connections. Please enter an integer value.
Use Proxy Credentials	This setting is only visible if proxy usage is enabled above. Determine whether the proxy server needs credentials or not. Choose between: ▪ **Yes, the proxy server requires credentials**: Define credentials (username and password) below. ▪ **No, there are no credentials necessary**: Do not use credentials for proxy connections.
User	This setting is only visible if proxy credentials are enabled above. Enter a username for proxy authentication. Please enter a string.
Password	This setting is only visible if proxy credentials are enabled above. Enter a password for proxy authentication. Please enter a string.

PROBE CONNECTION SETTINGS

Probe Connections IPs	Define how PRTG handles incoming connections from probes. Choose between the following options: ▪ **Local Probe only, 127.0.0.1 (PRTG will not be accessible for Remote Probes)**: The PRTG core server 112 only accepts local probe connections. You cannot use remote probes 3195 with this setting enabled. This is the default setting in PRTG on premises. ▪ **All IPs available on this computer**: The PRTG server will always accept incoming connections from remote probes, no matter on which IP address of the core server they come in. This is the default setting in PRTG on demand. ▪ **Specify IPs**: The PRTG server will accept Incoming connections from remote probes 3206 only on the selected IP address(es) of the core server. In the list, select the IP addresses by adding a check mark in front of the desired IPs.

PROBE CONNECTION SETTINGS

You can also change this setting in the **PRTG Administration Tool on Core Server System** [3139].

If you change this setting, PRTG needs to restart the core server to apply your changes. After clicking the **Save** button, a dialog box appears which asks you to confirm the required core server restart. Click **OK** to trigger the restart and follow the instructions on the screen. During the restart all the users of the PRTG web interface, of the **Enterprise Console** [3028], or of **PRTG Apps for Mobile Network Monitoring** [3082] will be disconnected and reconnected.

This option is not available in PRTG on demand.

Access Keys

Enter a list of access keys, one per line. Every (remote) probe that wants to connect to this PRTG installation has to use one of these keys. For more information on how to set this key for a probe, please see the **PRTG Administration Tool** [3158] section.

Allow IPs

Enter a list of remote probe IPs or DNS names that will be accepted when connecting to this PRTG installation. Provide one IP address or DNS name per line. The local probe (127.0.0.1) is always allowed automatically. PRTG will check the list of allowed addresses first before the list of denied addresses.

- ***[Empty]***: An empty field does not allow any remote probes (but only the local probe). Please enter IP addresses or DNS names to allow remote probe connections.
  We recommend that you use IP addresses rather than DNS names, because DNS name resolution may be cached.
- **any**: Enter the word **any** to automatically allow all remote probe connections. This is the default setting in PRTG on demand.
  We recommend that you only use this option in intranets in PRTG on premises!

If the IP address of your remote probe changes regularly (for example, due to an internet provider assigning IP addresses dynamically), please enter the potential IP range for this remote probe or use the **any** option.

You can use the PRTG syntax for IP address ranges here. For more information, please see the **Define IP Ranges** [3182] section.

PROBE CONNECTION SETTINGS

Deny IPs

Enter a list of remote probe IPs or DNS names that will not be accepted when connecting to this PRTG installation. Provide one IP address or DNS name per line. This is useful to explicitly deny connections from certain remote probes you do not want to include in your setup any more (for example, for a certain time).

Access to IP addresses or DNS names you allowed above will be denied if you enter them here. This is useful to allow access to an IP range in the field above, but deny access to a single IP address. You can use the PRTG syntax for IP address ranges here (see the **Define IP Ranges** 3182 section).

We recommend that you use IP addresses rather than DNS names, because DNS name resolution may be cached.

Deny GIDs

Enter a list of GIDs, one global ID (GID) per line. The access to matching GIDs will be denied. If you remove a remote probe from the device tree or if you deny a remote probe after installation, its global ID (GID) will be automatically entered here. This specific remote probe will not be able to connect anymore. Denying GIDs is more precise than denying IPs, where other remote probes at the same location could be excluded too.

Mini Probes

Define if you want to allow Mini Probe connections to your PRTG server. If you want to use Mini Probes, you need to set up your PRTG web server to accept connections of Mini Probes here and choose the secure HTTPS server option in the web server settings 2946. Choose between:

- **No Mini Probes**: Mini Probes cannot connect to your PRTG web server. You are not able to monitor with Mini Probes if you choose this option.
- **Allow Mini Probes to connect to the web server**: Mini Probes can connect to your PRTG web server and use the defined TCP port for the web server 2946 for this purpose. The default port for SSL connections is **443**.
- **Allow Mini Probes to connect to an extra port**: Mini Probes can connect via a specific port to your PRTG web server. This is useful if you do not want to have your whole PRTG web server reachable from other networks all the time only because of Mini Probes.
  SSL is always required to be active on the Mini Probe port.

Please refer to the PRTG API 3174 for the full Mini Probe documentation. See also this Knowledge Base article: Where can I find PRTG Mini Probes which are ready to use?

PROBE CONNECTION SETTINGS

If you change this setting, PRTG needs to restart the core server to apply your changes. After clicking the **Save** button, a dialog box appears which asks you to confirm the required core server restart. Click **OK** to trigger the restart and follow the instructions on the screen. During the restart all the users of the PRTG web interface, of the Enterprise Console 3028, or of PRTG Apps for Mobile Network Monitoring 3082 will be disconnected and reconnected.

This option is not available in PRTG on demand.

Mini Probe Port

This field is only visible if you select the extra Mini Probe port option above. Enter the number of the port that you want to use for Mini Probe connections. Ensure that SSL is available on this port.

If you change this setting, PRTG needs to restart the core server to apply your changes. After clicking the **Save** button, a dialog box appears which asks you to confirm the required core server restart. Click **OK** to trigger the restart and follow the instructions on the screen. During the restart all the users of the PRTG web interface, of the Enterprise Console 3028, or of PRTG Apps for Mobile Network Monitoring 3082 will be disconnected and reconnected.

This option is not available in PRTG on demand.

ACTIVE DIRECTORY INTEGRATION

This option is not available in PRTG on demand.

Domain Name

To use the Active Directory Integration 3171 enter the name of your local domain. Please enter a string or leave the field empty.

Access Type

Define which user account PRTG will use to configure Active Directory (AD) access. PRTG uses this account to query the AD for existing groups. Choose between:

ACTIVE DIRECTORY INTEGRATION

- **Use the PRTG core service account (usually LOCAL SYSTEM)**: Use the same Windows user account configured for the "PRTG Core Server Service". In a default installation, this is the "local system" Windows user account. If this account does not have the right to query all groups of your Active Directory, do not use this option.
- **Use explicit credentials:** Define a user account that PRTG will use to authenticate against the Active Directory. This should be a user account with full access to all of your Active Directory groups.

Access User	This field is only visible if you enable the use of explicit credentials above. Enter the Windows user account name that PRTG will use to authenticate for Active Directory configuration.
Access Password	This field is only visible if you enable the use of explicit credentials above. Enter the password for the Windows user account that PRTG will use to authenticate for Active Directory configuration.

HISTORIC DATA PURGING: DEFINE FOR HOW MANY DAYS HISTORIC DATA REMAINS ACCESSIBLE

Data purging enables you to automatically delete unnecessary data to free up disk space and improve system performance. You can define different time spans for several kinds of data. Select here for how many days historic data remains accessible.

For further information on storage locations, please see the **Data Storage** 3226 section.

This option is not available in PRTG on demand.

PRTG on demand purges historic data using the default purging limits of PRTG on premises (see the table below). You cannot modify historic data purging limits in PRTG on demand.

Logfile Records	Define how long records in the system logfile Log Database.db will be kept. Enter a value in days. All entries older than this value will be deleted from the logfile automatically. This also affects the content of the **Logs** 198 tab of monitoring objects like sensors. Keep this value as low as possible to enhance system performance. Default value is **30** days.

HISTORIC DATA PURGING: DEFINE FOR HOW MANY DAYS HISTORIC DATA REMAINS ACCESSIBLE

Web Server Log Records	PRTG creates one web server logfile every day. Define how many web server logfiles are kept. Enter a value in days. All web server logfiles older than this value will be deleted automatically. Default value is **30** days.
Historic Sensor Data	Define for how many days historic sensor data are kept for all sensors. It is used to create reports 2862 of monitoring data. Enter a value in days. Depending on the used intervals and the number of sensors in your setup, the file containing this data can become large. For smaller installations (500 sensors or less) a value of 365 is usually fine. Historic sensor data is the basis for reports on monitoring data. If you decrease this value, there will be less historic monitoring data available! Default value is **365** days.
Toplist Records	Define how long toplist records for Flow 3099 and Packet Sniffer 3097 sensors are kept. Enter a value in days. We recommend using 30 days here. Old toplist data will be purged automatically as soon as a limit of 2 GB is reached. The oldest data is deleted first from the database. Default value is **30** days.
Closed Tickets	Define how long tickets that are in status closed are kept. Enter a value in days. Default value is **365** days.
Reports	Reports generated in PDF format are stored on disk for later reference. Define the maximum age for these reports. Enter a value in days. All reports older than this value are deleted automatically. Default value is **365** days.
Configuration Auto-Backups	PRTG creates one backup of your configuration every day. Define the maximum age for these backups. Enter a value in days. All configuration backup files older than this value will be deleted automatically.

HISTORIC DATA PURGING: DEFINE FOR HOW MANY DAYS HISTORIC DATA REMAINS ACCESSIBLE

Default value is **365** days.

Full HTTP Sensor Screenshots	Define how long the screenshots of the **HTTP Full Web Page Sensor** 918 (PhantomJS browser engine) are kept. Enter a value in days. PRTG will delete older screenshots with every sensor scan.

Default value is **10** days.

Click **Save** to save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Remote Probe Setup

Find more information about setting up remote probes in the **Multiple Probes and Remote Probes** 3195 section.

More

- **Define IP Ranges** 3182

Knowledge Base: Where can I find PRTG Mini Probes which are ready to use?

- https://kb.paessler.com/en/topic/61215

8.12.9 System Administration—User Accounts

PRTG administrator users can change all user account settings and add new users.

If you use PRTG on premises and open the system administration page from another administration page, PRTG will ask you to enter your credentials again for security reasons if 15 minutes (900 seconds) have passed since your last credential-based login. A dialog box will appear. Enter your **Login Name** and **Password** for PRTG in the corresponding fields and confirm to continue.

User Accounts Overview

The **User Accounts** tab shows a list of all user accounts which exist on this PRTG server. The **Users** table shows various information about each user at a glance.

- **Object**: the name of the user account. Click it to open the **User Account Settings** 2976.
- **Type**: the account type, for example, PRTG Administrator user or Read Only User
- **Email**: the Primary Email Address of this user account
- **Primary Group**: the Primary Group of this user account. Click it to open this user group's settings 2983.
- **Group Memberships**: all user groups that contain this user account
- **Active/Paused**: the status of this user account

See also section **Working with Table Lists** 207 for more information.

You have several options to manage user accounts and groups on this page:

- To change a user's settings, select it from the list by clicking the username. The available setting options are the same as shown in the **My Account** 2909 settings of the currently logged in user (plus some account control options).
- To add a new user to PRTG on premises, click the **New User** button. The options are the same as for existing users (with slight differences).
- To add a new user to PRTG on demand, click the **Invite User** button. The options are almost the same as for existing users, but the initial login password will be generated automatically. The new user can change it later. Click **Send Invite** to save your settings and to send the invitation per email to the defined **Primary Email Address**.
- To batch-add several users at once in a simple way, please click the **Multiple New Users** button. In the dialog box that appears, select an existing user group 2982 from the dropdown menu and enter or paste a list of email addresses. They can be separated by a space, comma, semicolon, or a new line. Click the **Add** button to confirm. For each address, PRTG will create a new local user account within the selected user group, carrying the email address as value for **Login Name**, **Username**, and **Email Address**. A new password will be generated automatically and sent to the email address.
- To add a new user group, click the **New User Group** button. The options are the same as for existing groups (with slight differences).

- Access rights in PRTG are given via user groups. Please make sure a user account is member of the correct user group 2982 and give access to this group in your device tree object's settings 188.

Predefined objects cannot be deleted!

User Accounts Settings

This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

USER ACCOUNT

Login Name	Enter the login name for the user. This option is not available in PRTG on demand.
Display Name	Enter a name that the user recognizes. It will not be used for login purposes.
Primary Email Address	Enter the user's email address. Please use an email client that can show HTML emails, otherwise you cannot read emails from PRTG.
Password	Define the user password. For security reasons, the account settings page does not contain the password. Choose between: ▪ **Don't change** ▪ **Specify new password** If you choose to specify a new password, enter the old password and then the new password twice. The new password must be at least 8 characters long. It must contain a number and a capital letter. Leading and trailing whitespaces will be cut. The password of a PRTG Administrator user can only be changed by the same PRTG Administrator user. This option is not available in PRTG on demand.
Passhash	Click **Show passhash** to display the passhash for the selected user. You need the passhash of a user if you use the PRTG Application Programming Interface (API) 3174. This setting is shown for your information only and cannot be changed here.

USER ACCOUNT

This option is not available in PRTG on demand.

API ACCESS

These settings are only available in PRTG on demand.

API Username	Shows the username of the current user account. You need a username if you use the PRTG Application Programming Interface (API). This setting is shown for your information only and cannot be changed here.
API Passhash	Click **Show passhash** to display the passhash for the selected user. You need the passhash of a user if you use the PRTG Application Programming Interface (API). This setting is shown for your information only and cannot be changed here.
Reset API Passhash	Click **Generate new passhash** to reset the passhash of the current user.

ACCOUNT CONTROL

Account Type	This setting is only visible to administrator users. However, it will not show if the user who's account you want to modify is a member of a group with administrative rights. Define the account type for the current user. Choose between: ▪ **Read/Write User**: You can change settings. ▪ **Read Only User**: You cannot edit any settings except your own password. This is a good choice for public or semi-public logins. This setting cannot be changed for the default administrator user.

ACCOUNT CONTROL

Allow Acknowledge Alarms	This setting is only visible if **Read Only User** is enabled above. Acknowledging an alarm is an action that requires write access rights. However, you can explicitly allow this action to read-only users. If enabled, they still do not have write access, but may acknowledge alarms 191. Choose between: ▪ **Allow**: Allow acknowledging alarms for this user. ▪ **Deny**: The user will not be able to acknowledge alarms.
Password Changes	Decide if you want the user to be able to change their account's password or not. If you allow the user to change the password, this option will be available in the **My Account** 2909 settings of the respective user. Choose between: ▪ **User may change his account's password** ▪ **Deny the right to change the password** (default) ⓘ This field is only visible if you edit this option for read-only users as an administrator.
Primary Group	This setting is available only for administrator users. Select the primary group for the current user. Every user has to be member of a primary group to make sure there is no user without group membership. Membership in other user groups is optional. For user experience there is no difference between the primary and other user groups. ⓘ You cannot change the primary group of Active Directory users. Users that you added with **Active Directory Integration** 3171 can only have this AD group as their primary group. If you need to change this, please delete this user account and add it again.
Status	This setting is only shown for administrator users. Define the status of the current user. Choose between: ▪ **Active**: The current user can login to the account. ▪ **Inactive**: The current user's login is disabled. Use this option to temporarily deny access for this user. ⓘ This setting cannot be changed for the default administrator user.
Last Login	Shows the time stamp of the user's last login. This setting is shown for your information only and cannot be changed here.

USER GROUPS

Member of	Shows the groups the current user is member of. Access rights to the device tree are defined on group level. This setting is shown for your information only and cannot be changed here.

AUTO REFRESH AND ALERTING

Auto Refresh	Define if you want PRTG to reload web pages automatically for the current user. Choose between: ▪ **Refresh pages (recommended)**: Automatically refresh the single page elements on the web pages in PRTG. ▪ **No automatic refresh**: Do not automatically refresh web pages.
Auto Refresh Interval (Sec.)	This setting is only relevant if you enable auto refresh above. Enter the number of seconds that PRTG waits between two refreshes. We recommend that you use **30** seconds or more. Minimum value is 20 seconds. Shorter intervals create more CPU load on the server running PRTG. If you experience load problems while using the web interface (or PRTG maps 2885), please set a higher interval.
Play Audible Alarms	Define when PRTG will play an audible alarm the current user on web pages whenever there are new alarms 190. Choose between: ▪ **Never**: Do not play sound files on any web pages. ▪ **On dashboard pages only**: When there are new alarms, play a predefined sound on dashboard 231 pages only. The sound will be played with every refresh of the dashboard page if there is at least one new alarm. ▪ **On all pages**: When there are new alarms, play a predefined sound on all web pages. The sound will be played with every page refresh if there is at least one new alarm. Audible alarms are only played if the **New Alarms** value in the **Global Header Area** 153 of the PRTG web interface is greater than 0 after a page refresh. The number of existing alarms is not considered. For more information about audible notifications and supported browsers, see this Knowledge Base article: Which audible notifications are available in PRTG? Can I change the default sound?

WEB INTERFACE

Homepage URL	Define the user's default page, which is loaded after logging in or clicking on the Home 231 button in the main menu.
Max. Groups/Devices per Group	To provide a fast and smooth user experience, PRTG attempts to reduce page size when displaying the device tree. It automatically collapses groups and devices when reaching a specified number of items. Enter this threshold for groups and devices here. We recommend values between **10** and **30**.
Max. Sensors per Device	In order to provide a fast and smooth user experience, PRTG attempts to reduce page size when displaying the device tree. It automatically collapses groups and devices when reaching a specified number of items. Enter this threshold for sensors per devices here. We recommend values between **10** and **30**.
Timezone	Define the time zone for the current user. Depending on the time zone you select here, PRTG shows the current user's local time zone in all data tables and graph legends. PRTG receives the UTC (Coordinated Universal Time) from the system time set on the PRTG core server for this purpose.
Date Format	Define the date format for the current user. This setting will take effect after the next login.

TICKET SYSTEM

Email Notifications	Define if you want to get emails from the ticket system. Choose between: ▪ **I want to receive an email whenever a ticket changes**: You will receive an email each time a ticket is assigned to you or your user group, or if a ticket that is assigned to you or your user group is changed. If you edit tickets that are assigned to you or your user group, or you assign a ticket to yourself or your user group, you will not get an email. ▪ **I do not want to receive any emails from the ticket system**: You will not get any emails about tickets.

Notification Contacts

In the **Notification Contacts** 2934 tab you can define recipients for each user account. Recipients can be email addresses, phone numbers, or push devices (iOS, Android and Windows Phone devices with the corresponding PRTG smartphone app 3082).

Comments

On the **Comments** tab you can enter free text for each object. You can use this function for documentation purposes or to leave information for other users.

Click **Save** to save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

History

In the **History** tab all changes in the settings of an object are logged with a timestamp, the name of the PRTG user who made the change, and a message. The history log retains the last 100 entries.

Click the **Continue** button to save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

More

Knowledge Base: Which audible notifications are available in PRTG? Can I change the default sound?

- https://kb.paessler.com/en/topic/26303

8.12.10 System Administration—User Groups

The PRTG administrator users can change existing user groups or add new ones, and define the users that are member of a certain group.

If you use PRTG on premises and open the system administration page from another administration page, PRTG will ask you to enter your credentials again for security reasons if 15 minutes (900 seconds) have passed since your last credential-based login. A dialog box will appear. Enter your **Login Name** and **Password** for PRTG in the corresponding fields and confirm to continue.

All the security settings as well as further rights management are conducted via the user groups. This means that group membership controls what a user may do and which objects the user will see when logged in. The actual rights for each object can be defined in an object's settings. There, you can define different rights for each user group.

The **User Groups** table shows you all existing user groups with various information at a glance. You can see all **Members** of a group as well as all user accounts that have this group as **Primary Group** or as **Active Directory Group**.

- To change a user group's settings, select it from the list by clicking on the group name.
- To add a new user to PRTG on premises, click the **New User** button. The options are the same as for existing users (with slight differences).
- To add a new user to PRTG on demand, click the **Invite User** button. The options are almost the same as for existing users, but the initial login password will be generated automatically. The new user can change it later. Click **Send Invite** to save your settings and to send the invitation per email to the defined **Primary Email Address**.
- To batch-add several users at once in a simple way, please click the **Multiple New Users** button. In the dialog box that appears, select an existing user group 2982 from the dropdown menu and enter or paste a list of email addresses. They can be separated by a space, comma, semicolon, or a new line. Click the **Add** button to confirm. For each address, PRTG will create a new local user account within the selected user group, carrying the email address as value for **Login Name**, **Username**, and **Email Address**. A new password will be generated automatically and sent to the email address.
- To add a new user group, click the **New User Group** button. The options are the same as for existing groups (with slight differences).
- For each user group you create, PRTG automatically adds a new device group 119 with the name [group_name] home to the device tree.
- For each user group you create, PRTG automatically adds a new email notification 2922 to notifications 2829 with read access rights 129 for this user group. It has the name Email to all members of group [group_name].
- By default, there are no access rights 129 on existing objects for a newly created PRTG user group. Initially, users in this group will not see any objects in the PRTG device tree except the automatically created home group (with write access rights). Please edit the object settings 188 in your device tree and set access rights for your newly created user group in the **Inherit Access Rights** section.
  The easiest way is to set these rights in the **Root Group Settings** 294.

The multi-edit option is not available for the standard user groups PRTG Administrators and PRTG Users Group.

Predefined objects cannot be deleted!

If you want to delete an Active Directory group, you have to delete all users that are in this group in PRTG first. This is because users that you add with **Active Directory Integration** 3171 always have this group as their primary group.

User Groups Settings

This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

USER GROUP SETTINGS

User Group Name	Enter a name for the user group.
Administrative Rights	Define if the members of this group will be PRTG administrators. If you enable this option, all members of this group will have full access to all monitoring objects, maps, reports, user accounts and user groups, and they can change the PRTG monitoring configuration. Choose between: ▪ **Yes**: Give full PRTG administrator rights to all members of this group. ▪ **No**: Do not make members of this group administrators. Access to monitoring objects for users that are member of this group will be controlled by the **Access Rights** settings defined in the **Object Settings** 188 of Probes, Groups, Devices, or Sensors. This option is especially useful in combination with the Active Directory option below.
Default Homepage	Enter a PRTG internal web page. This will set the default homepage for all new users created with this group. A user will be redirected to this page after logging in. This concerns new users either added by an **Active Directory** login or by the **Add multiple users** feature.
Use Active Directory	Define if this PRTG user group will be connected to a group in your active directory. Choose between:

USER GROUP SETTINGS

	▪ **Yes**: Connect this group to an AD group. Choose below. For detailed information, please see Active Directory Integration 3171. ▪ **No**: Do not use Active Directory integration for this group, but choose local user accounts instead. This option is not available in PRTG on demand.
Active Directory Group	If a valid Active Directory Domain is set in the System Administration—Core & Probes 2971 settings and Active Directory integration is enabled above, a drop down menu will appear, showing the groups in your Active Directory. Choose the group whose members will be able to log in to PRTG using their Active Directory domain credentials. All of those AD users will be in the security context of the PRTG group you're about to create/edit. For detailed information, please see Active Directory Integration 3171. If your Active Directory contains more than 1000 entries in total, PRTG will display an input field instead of a drop down menu. This is done due to performance reasons. In the input field, you can enter the group name only. PRTG will then add the prefix automatically. This option is not available in PRTG on demand.
New User Type	If Active Directory integration is enabled above, define the default rights for all new users in this user group. If a user logs in for the first time using Active Directory credentials, PRTG will automatically create a new local user account for this user, applying the user type defined here. Choose between: ▪ **Read/Write User**: The user may change settings. ▪ **Read Only User**: The user may not edit any settings except the own password. This is a good choice for public or semi-public logins.
Allowed Sensors	Define if members of this user group will be able to create all available sensor types or only specific ones. Choose between: ▪ **Users may always create all sensor types**: No restrictions for group members are applied. ▪ **Users may create certain sensor types only**: Choose the allowed sensor types below. This option is especially interesting for a Managed Service Provider (MSP).

USER GROUP SETTINGS

Users May Create These Sensor Types	This field is only visible if you defined that the users in this group are only allowed to create certain sensor types. A list of all available types is shown with their name. Select the desired types by adding check marks in front of the respective lines. You can also select and deselect all items by using the check box in the table head.
Ticket System Access	Define if the members of this user group will be able to use the PRTG ticket system 200. Choose between: ▪ **Members can use the Ticket System**: No restrictions for group members are applied. ▪ **Members can NOT use the Ticket System**: The **Tickets** 242 option in the main menu bar 242 will not be visible to users in this group.

MEMBERS

Members	This setting is available only if Active Directory integration is disabled above. Define which local user accounts will be a member of this group. To add a user account from the list, add a check mark in front of the username. The user accounts available depend on your setup.

PRIMARY USERS

User List	Shows a list of all user accounts with this group set as primary group. This is shown for information purposes only. You can change it in a user account's settings 2975.

Comments

On the **Comments** tab you can enter free text for each object. You can use this function for documentation purposes or to leave information for other users.

Click **Save** to save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

History

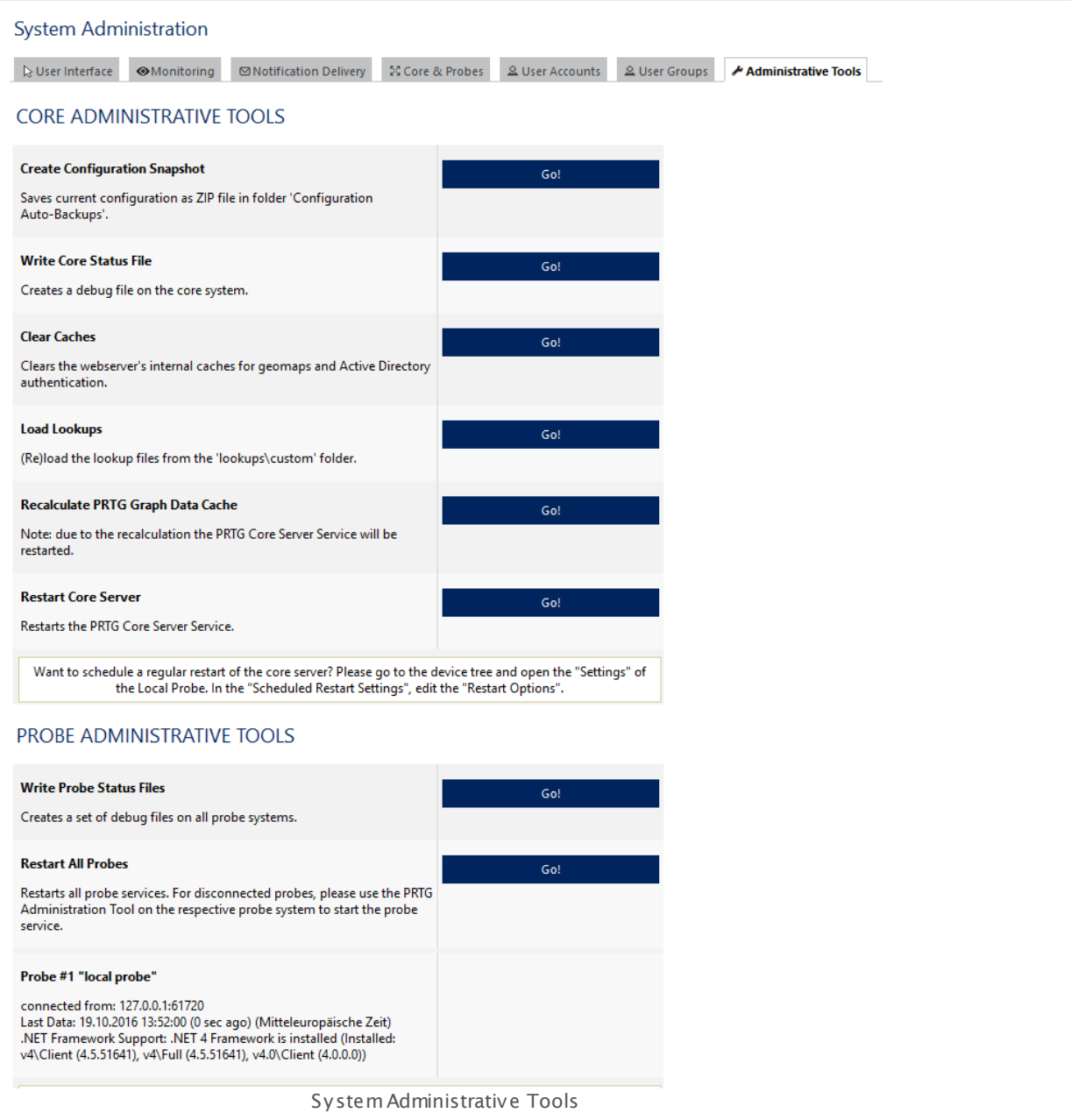
In the **History** tab all changes in the settings of an object are logged with a timestamp, the name of the PRTG user who made the change, and a message. The history log retains the last 100 entries.

Click the **Continue** button to save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

8.12.11 System Administration—Administrative Tools

With the administrative tools you can start system specific processes for debugging purposes. Use them if our technical support advises you to do so. You can start the respective processes by clicking the **Go!** button on the right.

If you use PRTG on premises and open the system administration page from another administration page, PRTG will ask you to enter your credentials again for security reasons if 15 minutes (900 seconds) have passed since your last credential-based login. A dialog box will appear. Enter your **Login Name** and **Password** for PRTG in the corresponding fields and confirm to continue.



System Administrative Tools

Core Administrative Tools

CORE ADMINISTRATIVE TOOLS

Create Configuration Snapshot	Create a snapshot of your PRTG configuration. This action can take up to 100 seconds. Once finished, you will find a ZIP file that contains a *.dat file in the **Configuration Auto-Backups** subfolder of your PRTG data directory 3226. If you run a PRTG cluster, this action is executed on the cluster node you are currently logged in to. The ZIP file follows the name pattern PRTG Configuration (Snapshot YYYY-MM-DD HH-MM-SS).zip. This option is not available in PRTG on demand.
Write Core Status File	Create status files of your PRTG core server. You will find the two text files in the **Logs (System)** sub folder of your PRTG data directory 3226. If you run a PRTG cluster, this action is executed on the cluster node you are currently logged in to. The files are named Core Status.txt and Core Memory.txt. They are overwritten each time you click this button. This option is not available in PRTG on demand.
Clear Caches	PRTG caches tiles for **Geo Maps** 2824 and user data for **Active Directory Integration** 3171. Use this button to delete the cache if you encounter broken Geo Maps tiles, or if you changed a user's password in the Active Directory. This option is not available in PRTG on demand.
Load Lookups	(Re)load the lookup files 3183 from the **\lookups\custom** folder. In this folder your customized lookup files are stored. If you have created a new lookup file or changed something in an existing lookup file, it might be necessary to load or to reload these files. This option is not available in PRTG on demand.
Recalculate PRTG Graph Data Cache	PRTG constantly writes monitoring data to disk and keeps the graphs for your graph tabs in memory. If PRTG is ended unexpectedly, the graph cache may get corrupted. In this case, graphs may be shown empty or show wrong data. If you experience graph display problems, a graph recalculation will fix the problem. Click **Go!** to delete the data cache file and recalculate it automatically.

CORE ADMINISTRATIVE TOOLS

If you apply recalculation, PRTG needs to restart the core server. Because of this, all users of the PRTG web interface, of the Enterprise Console 3028, or of Smartphone Apps 3082 will be disconnected. After clicking the **Go!** button, a dialog window will appear which asks you to confirm the required core server restart. Click **OK** to trigger the restart and follow the instructions on the screen.

Directly after this action your graphs will be empty. They will be re-filled successively while recalculation in the background progresses. Until recalculation is finished, performance of the PRTG web interface may be affected due to high disk I/O activity.

Restart Core Server	Restart the PRTG core server service manually. Click the **Go!** button for this purpose. If you restart the core server, all users of the PRTG web interface, of the Enterprise Console 3028, or of Smartphone Apps 3082 will be disconnected. After clicking the **Go!** button, a dialog window will appear which asks you to confirm the required core server restart. Click **OK** to trigger the restart and follow the instructions on the screen. If you want to schedule an automatic restart of Windows services for both core server and probe service, you can do this in the corresponding Probe Settings 330. This option is not available in PRTG on demand.

Probe Administrative Tools

PROBE ADMINISTRATIVE TOOLS

Write Probe Status Files	Create status files of your PRTG probes. PRTG writes status files for the local probe running on the PRTG core server (if you run a PRTG cluster, on the cluster node you are currently logged in to) as well as for all remote probes configured (if any). On the respective systems, you will find four text files in the **Logs (System)** sub folder of the PRTG data directories 3226. The files follow the name pattern Probe Memory XX.txt, ProbeState XX.txt, ProbeState AXX.txt, and ProbeState BXX.txt. They are overwritten each time you click this button.

PROBE ADMINISTRATIVE TOOLS

Restart All Probes	Restart all PRTG probes as well as the local probe Windows service. If there are any remote probes 3195 configured, the probe Windows services on the respective remote systems will be restarted as well. To restart single probes only, please see below. Disconnected probes cannot be restarted here. Please use the **PRTG Administration Tool** 3134 on the probe system to start a disconnected probe. If you run a PRTG cluster, this action is executed on the cluster node you are currently logged in to. In this case, remote probes are only restarted if you are logged in to the primary master node. The cluster probe Windows service of failover nodes is not restarted if you execute this action on the master node. If you want to restart the cluster probe Windows service of a failover node, please log in to this failover node's web interface and click the **Go!** button there.
Probe [#Number] "[Name]"	This section shows information about the connection status. If the probe is currently connected, the field shows the source IP address and port number used by the probe. For the **Local Probe**, the IP will always be 127.0.0.1. You will also see information about the date when the last data packet was received from the probe. If you want to restart a single probe, click the corresponding **Restart Probe** button. Entries for every single probe are following. Disconnected probes cannot be restarted here. Please use the **PRTG Administration Tool** 3134 on the probe system to start a disconnected probe. This option is not available for local probes in PRTG on demand.

Setup—Topics

- Account Settings—My Account 2909
- Account Settings—Notifications 2916
- Account Settings—Notification Contacts 2934
- Account Settings—Schedules 2938
- System Administration—User Interface 2943
- System Administration—Monitoring 2955
- System Administration—Notification Delivery 2961
- System Administration—Core & Probes 2967
- System Administration—User Accounts 2975
- System Administration—User Groups 2982
- System Administration—Cluster 2992
- System Administration—Administrative Tools 2987
- PRTG Status—System Status 2994
- PRTG Status—Auto-Update 3005
- PRTG Status—Cluster Status 3010
- PRTG Status—Activation Status 3012
- Downloads and Add-Ons 3018
- Desktop Notifications 3020
- Support—Contact Support 3022

Others

There are some settings that you must make in the PRTG Administration Tool 3134, available as native Windows application. For more details, please see the sections:

- PRTG Administration Tool on Core Server System 3135
- PRTG Administration Tool on Remote Probe System 3157

8.12.12 System Administration—Cluster

In the cluster settings you can define the cluster settings. During **Failover Cluster Configuration**[3212], the cluster settings were already pre-defined. See the cluster status[3010] to see if all nodes in your cluster are properly connected.

This feature is not available in PRTG on demand.

If you use PRTG on premises and open the system administration page from another administration page, PRTG will ask you to enter your credentials again for security reasons if 15 minutes (900 seconds) have passed since your last credential-based login. A dialog box will appear. Enter your **Login Name** and **Password** for PRTG in the corresponding fields and confirm to continue.

Cluster Settings

This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

You can set up two, three, four, or five nodes in one cluster for PRTG on premises. In the table of the cluster settings, the information of each node is written in one line.

CLUSTER NODE SETUP

Node Name	Enter the name of the node (for display purposes).
Node ID	The ID is unique for every node. We recommend that you use the default value.
Node State	You can set the state for every failover node. Choose between: ▪ **Active**: Set the node to be active. ▪ **Inactive**: Set the node to be not active. It will be disabled in the cluster configuration. It will then be not an active part of the cluster and will not appear in the cluster status[3010] any more. This setting is not available for the master node of a cluster. The master is always set to **Active**.
IPs/DNS Names Used for Connections Between Nodes	Define the IP addresses or DNS names that will be used for the connections between the nodes. You can enter different values for every node-node connection.

CLUSTER NODE SETUP

For example, in the field **#2 => #1**, enter the address under which the master node server can be reached from the second cluster member. Usually, this is the IP address or DNS name of the master node. Do this for all available node connections, for example, if you run three nodes, enter the address under which second node can be reached from the third cluster member into the field **#3 => #2**.

See also section **Failover Cluster Step by Step, Step 4** 3221 and following.

If you use remote probes 3196 outside your local network or outside your Network Address Translation (NAT), ensure the IP addresses or DNS names you enter here are valid for both the cluster nodes to reach each other and for remote probes to reach all cluster nodes individually. These addresses must not be private and have to be reachable from the outside, otherwise your remote probes will not be able to connect.

Click **Save** to save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

For how to set a cluster node into **Maintenance Mode**, see **PRTG Status—Cluster Status** 3010.

The entire setup process for a cluster requires several different steps. For more information and step-by-step guidance, see **Failover Cluster Configuration** 3212.

8.12.13 PRTG Status—System Status

To view the status of your PRTG installation, select **Setup | PRTG Status** from main menu. Click on the tabs to change the different settings.

PRTG Status Tabs

You can view the following aspects of the PRTG status:

- PRTG Status—System Status 2994
- PRTG Status—Cluster Status 3010

System Status

Click on the **System Status** tab to view relevant system information. You might need this data for debugging or when you contact our support team. They ask you in some cases to provide PRTG status information to analyze your issues with PRTG. Furthermore, this page shows interesting usage statistics.

SOFTWARE VERSION AND SERVER INFORMATION

PRTG Version	Shows the exact version of the build your PRTG installation is currently running on.
Auto-Update Status	Shows the latest auto-update message available from Software Auto-Update 3005. For example, the message will indicate any PRTG updates ready to be installed. This information is not displayed in PRTG on demand.
Operating System	Shows the exact Windows version build and service packs, the number and kind of CPUs, and the computer name, of the system the PRTG core server is installed on. If you run a PRTG cluster, this will show information for the system of the cluster node you're currently logged in to. When running PRTG on virtual systems, not all of the mentioned values may be available. This information is not displayed in PRTG on demand.

SOFTWARE VERSION AND SERVER INFORMATION

Server Time	Shows the date and time of the system the PRTG core server is installed on. If you run a PRTG cluster, this will show information for the system of the cluster node you're currently logged in to.
Server CPU Load	Shows the current CPU load of the system the PRTG core server is installed on. If you run a PRTG cluster, this will show information for the system of the cluster node you're currently logged in to.
Username	Shows the username 2909 of the PRTG user you're currently logged in as.
Browser	Shows the name and user agent string of the browser you're currently viewing this page with.

LICENSING

License Status	Shows the activation status of this installation of PRTG. Usually, PRTG completes the activation automatically during installation or when you change your license information. Only if PRTG cannot connect directly to the internet, a manual activation is necessary. For details, please see **Activate the Product** 91.
License Name	Shows the owner of the license 89 that you use for this installation of PRTG. License Name, license key, and system ID together build your license information. You will find the label License Owner in some documents from the Paessler shop. License Owner is the same as License Name for which you will be asked while installing PRTG or when you change your license key 89.
License Key	Shows the license 89 key that you use for this installation of PRTG. License Name, license key, and system ID together build your license information.
System ID	The system ID is a fixed value that is automatically assigned to your PRTG installation.
Licensed Edition	Shows the PRTG edition that you use for this installation of PRTG. This determines how many sensors you can use in your monitoring (see below).

LICENSING

Last Update	Shows the date of the last update for this PRTG installation. We recommend that you use the PRTG **Auto-Update** 3005 to get the most out of PRTG.
Maintenance until	Shows the expiry date and the days remaining for your active maintenance contract. You can buy maintenance for each PRTG license. With an active maintenance contract you may download any available updates and use our premium email support.
Number of Sensors	Shows the number of sensors you can use in your monitoring with your current edition of PRTG (see above). If you reach the limit, PRTG will set each new sensor that you add to a **Pause** status 163 automatically. To upgrade your license right now, click the **Need more sensors? Click here to upgrade!** button to visit our web shop. Editions that allow an **unlimited** number of sensors do not restrict the number of possible sensors by license, so you can create sensors until the performance limit 25 is reached. This means that you can use about 10,000 sensors per core server (depending on your system's performance, sensor types, and scanning intervals). For details, see section **Detailed System Requirements** 25.

SYSTEM STARTUP LOG

Shows the log information created during the last startup of the PRTG core server. If you run a PRTG cluster, this will show information for the system of the cluster node you're currently logged in to.

SYSTEM WARNINGS

If there are any warnings, PRTG will show them here. Usually, you will see "None" system warnings.

CLUSTER STATUS

This box is only visible if you run a PRTG cluster. This section lists all cluster nodes configured in your monitoring.

Node [Number]	Shows the name of the cluster node as well as the node type (primary/secondary node) and status (current master/failover node). Additionally, all connections from this node to the other cluster nodes are shown, as illustrated on the **PRTG Status—Cluster Status** 3010 page.

LOCAL STATUS

This box is only visible if you run a PRTG cluster. This section lists information about the cluster node you're currently logged in to.

Server State Cluster Messages	Shows internal summary information about the current node and the communication between the nodes. You might be asked about this by Paessler's technical support staff.

CLUSTER CONNECTIONS

This box is only visible if you run a PRTG cluster. This section lists information about the connections between the different cluster nodes.

State of Local Node	Shows Treeversion and size of the Server Volume, both internal system information.
State of Cluster Members	For each cluster node, the name and IP address is shown, as well as a state CRC code, the time stamp of the last "keep alive" signal sent, the current size of the buffer, and the remote IP.
Message State of Cluster Members	For each cluster node, the name, IP address, and unique identifier is shown, as well as the connection state, and statistic information about the cluster message system which is used for the communication between the different nodes.

CORE SYSTEM MEMORY

Shows machine-oriented information regarding the memory usage of the core server system. If you run a PRTG cluster, this will show information for the system of the cluster node you're currently logged in to.

See the Knowledge Base for more information: What do the PRTG core system memory parameters mean?

THREAD INFORMATION

Shows machine-oriented information regarding the threads running on the core server system. If you run a PRTG cluster, this will show information for the system of the cluster node you're currently logged in to.

ACTIVITY HISTORY

The "Activity History" shows how busy PRTG was for you in the past. The graphs indicate the number of activities on the last 365 days. Right to the graphs, you see statistics about the past day.

Sensor Scans	Shows how often all sensors 120 in this PRTG installation refreshed their data in the past.
Sensor State Changes	Shows how often the **Sensor States** 163 changed in the past.
Notifications Sent	Shows how many **Notifications** 2829 PRTG sent out in the past.
Reports Generated	Shows how many **Reports** 2862 PRTG created in the past.
Page Views	Shows how often pages in the PRTG web interface were opened in the past.
Sensors	Shows how many sensors 120 existed in this PRTG installation in the past.
Devices	Shows how many devices 120 existed in this PRTG installation in the past.

ACTIVITY HISTORY

Reports	Shows how many **Reports** 2862 existed in this PRTG installation in the past.
Maps	Shows how many **Maps** 2885 existed in this PRTG installation in the past.

AUTO-DISCOVERY TASKS

Currently Running	Shows the number of auto-discovery tasks that are currently running. A high number of auto-discovery tasks can negatively influence system performance.

BACKGROUND TASKS

Historic Data	Shows if PRTG is re-calculating the historic data cache in the background. If so, you will see the tasks to do until done. Usually, this calculation is done after every core server restart.
Toplist Buffer	When using xFlow 3099 or Packet Sniffer 3097 sensors, PRTG stores Toplist data. The data stream received is buffered and written to the data directory of the core system. Depending on the number and size of the data stream as well as the hard disk and system performance of the core system, the buffer size can rise. When reaching a buffer size of 500, Toplist data is dropped which can lead to incorrect Toplist values for the sensors.
Toplist Upgrade	If you recently updated from an older PRTG version (7 or 8), Toplist data needs to run through a one-time conversion process. While conversion is running you may experience a considerably slow monitoring system. Usually, you will see n/a here.
Similar Sensors Analysis	Shows the current status and the selected setting for the analysis depth of the **Similar Sensors** 180 analysis.
Recommended Sensors Detection	Shows the current status of the detection engine and the current tasks of the **Recommended Sensors Detection** 2959.

DATABASE OBJECTS

Shows statistic information about your monitoring configuration. This information might be necessary when contacting Paessler's technical support staff.

Probes	Shows the total number of probes 312 configured.
Groups	Shows the total number of groups 334 in your configuration.
Devices	Shows the total number of devices 360 in your configuration.
Sensors	Shows the total number of sensors 384 in your configuration.
User Groups	Shows the total number of user groups 2982 in your configuration.
Users	Shows the total number of users 2975 configured.
Notifications	Shows the total number of notifications 2916 configured.
Schedules	Shows the total number of schedules 2938 configured.
Maps	Shows the total number of created maps 2885 in your installation.
Libraries	Shows the total number of created libraries 2845 in your installation.
Reports	Shows the total number of reports 2862 in your installation.
Requests/Second	Shows a value calculated from the total number of sensors and the average scanning interval configured. This number indicates how many monitoring requests per second are sent from the probe(s) to the devices in your network. There are no general guidelines what is a "good" value here. This depends on the sensor types used as well as on your system's performance.
Sensors	Shows a list with numbers and types of sensors used in your configuration. In the list, internal short names are used for sensor types instead of the official designations.

SENSORS BY PERFORMANCE IMPACT

Shows all sensor types used in your configuration ordered by performance impact (from very low to very high). If your PRTG system is very slow, you can see which sensors might cause this issue. Please consider the recommended number of sensors in the respective manual sections [384] for sensors with high and very high performance impact.

In the list, internal short names are used for sensor types instead of the official designations.

SENSORS BY INTERVAL

Shows all sensor types used in your configuration ordered by scanning interval. Please choose reasonable scanning intervals for sensors which can affect the system performance. See the respective manual sections [384] for sensors for more information.

In the list, internal short names are used for sensor types instead of the official designations.

PROBES

This section lists all probes configured in your monitoring. If there are no remote probes configured, only the **Local Probe** appears in the list, which always runs on the PRTG core server.

If you run a PRTG cluster, this will show information for the system of the cluster node you're currently logged in to. Remote probes (if any) will only be shown when you are logged in to the primary master node. When logged in to a failover node, the cluster probe running on this node will appear as **Local Probe**.

Probe [#Number] "[Name]"	Information about the connection status is shown. If the probe is currently connected, the field shows the source IP address and port number used by the probe. For the **Local Probe**, the IP will always be 127.0.0.1. You will also see information about the date when the last data packet was received from the probe. If you want to restart a single probe, please open the Administrative Tools Settings [2987].

SYSTEM SETTINGS

Web Server URL	Shows the URL to access the PRTG web interface 136. If you run a PRTG cluster, this will show information for the system of the cluster node you're currently logged in to.
Web Server IPs	Shows all IP addresses the PRTG web server is running at. If you run a PRTG cluster, this will show information for the system of the cluster node you're currently logged in to.
Web Server Ports	Shows the port the PRTG web server is running at. If you run a PRTG cluster, this will show information for the system of the cluster node you're currently logged in to.
Web Server Port Usage	Shows the number of ports used by the PRTG web server.
Incoming Probe Connection Binding	Shows a combination of the two values below.
Incoming Probe Connection IPs	Shows a list of all IP addresses on which your current PRTG installation listens to incoming remote probe connections. This is the same information as shown in the **System Administration—Core & Probes** 2967 settings. 0.0.0.0 means that the core server listens on all local network adapter IPs.
Incoming Probe Connection Port	Shows the port number on which your current PRTG installation listens to incoming remote probe connections. The default port is 23560.
Probe Allow IPs	Shows all source IP addresses that will be accepted by the core server for incoming remote probe connections. This is the same information as shown in the **System Administration—Core & Probes** 2967 settings and can be changed there. any means that all remote probe connections are accepted, regardless of the IP address of the remote probe system.
Probe Deny IPs	Shows all source IP addresses that will be denied by the core server for incoming remote probe connections. This is the same information as shown in the **System Administration—Core & Probes** 2967 settings and can be changed there. Denied IPs are superior to allowed IPs. If this field is empty, there are no denied IPs. PRTG automatically adds the IP address of a remote probe system to this list when you delete a remote probe from your device tree 118.

SYSTEM SETTINGS

DataPath — Shows the path where PRTG stores its configuration, monitoring database, etc. If you run a PRTG cluster, this will show information for the system of the cluster node you're currently logged in to. In order to change this setting, please open the **PRTG Administration Tool** 3135 on the system of the PRTG core server (or of the respective cluster node, if applicable).

WEB SERVER ACTIVITY

Shows statistic information about the web server since last startup. All values are reset when the core server is restarted. If you run a PRTG cluster, this will show information for the system of the cluster node you're currently logged in to.

Time Since Startup	Shows the time that has passed since the PRTG web server was started.
Page Views	Shows the total number of page views on this core server.
Geo Maps	Shows the total number of geo maps shown on this core server.
HTTP Requests	Shows the total number of HTTP requests to this core server.
HTTP Requests > 500/1000/5000 ms	Shows for how many (percent) of the HTTP requests above the page delivery took longer than 500, 1,000, or 5,000 milliseconds.
Slow Request Ratio	Shows a calculated number of the HTTP request values above. The lower this number, the faster is your installation's web interface.

SYNCHRONIZATION

The core server holds the configuration of the entire monitoring and deploys it to the probes. This section shows statistic information about the synchronization of the core server with the local probe and all connected remote probes (if any), since last startup of the core server. All values shown here are reset when the core server is restarted. If you run a PRTG cluster, this will show information for the system of the cluster node you're currently logged in to.

SYNCHRONIZATION

Only when logged in to the primary master node, you will see synchronization data for remote probe connections.

Last Synchronization with a Probe	Shows the time stamp of the last probe synchronization, and if there is still something to do.
Probe/Core Message Count	Shows the total number of messages sent between core and probe(s), as well as a calculated message speed value.
Raw Buffer Count	Shows the number of raw buffers and a corresponding status indicator.
Sync Cycle Speed	Shows the time necessary for a full synchronization, as well as an evaluation comment of this time (usually, this will be "OK").
Configuration Requests Sent	Shows the total number of configuration requests and the requests that still have to be sent.
Configuration Requests Deleted	Internal debug information. Usually, this value will be 0.
Configuration Requests With Response	Internal debug information. Usually, this value will be 0.

More

Paessler Website: System Requirements for PRTG Network Monitor—Recommended Setup for Most PRTG Users

- https://www.paessler.com/prtg/requirements

Knowledge Base: How can I speed up PRTG—especially for large installations?

- https://kb.paessler.com/en/topic/2733

Knowledge Base: What do the PRTG core system parameters mean?

- https://kb.paessler.com/en/topic/71671

8.12.14 PRTG Status—Auto-Update

Whenever a new version of the software is available from the Paessler website PRTG will download the setup file automatically if a direct internet connection is available. The **PRTG System Administrator** user will then receive a ToDo ticket 201 with instructions to initiate the update installation.

For customers using a Freeware or Trial Edition 21, automatic software updates are available at any time. Customers using a Commercial Edition 21 need to have an active maintenance contract to receive updates.

This option is not available in PRTG on demand.

Status

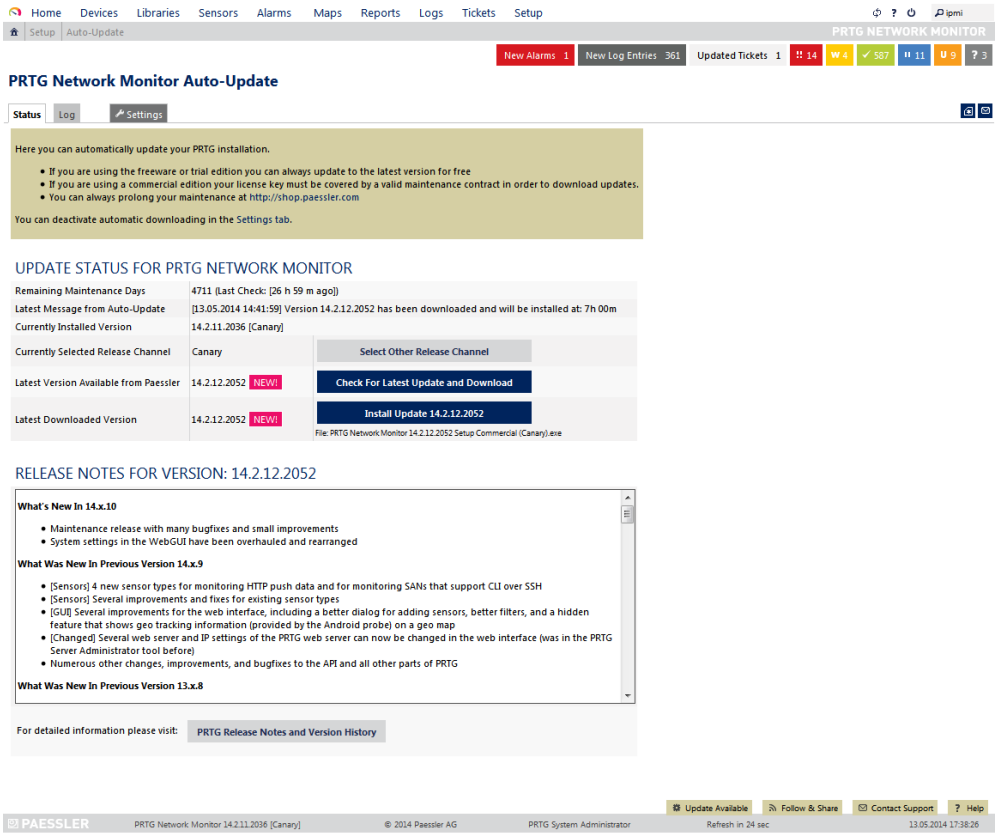
This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

To view the auto-update page of your PRTG installation, select **Setup | Auto-Update** from main menu. On the **Status** tab you can download and perform updates.

Using Auto-Update

If there is a new version available, you will see detailed information about the available version. Please read these notes carefully! You find a summary of current and past release notes below the update section. For detailed release notes, click **PRTG Release Notes and Version History** which will redirect you to the version history page on paessler.com.

To install the latest available version, click **Install Update [version number]**. PRTG will ask you to confirm installation and license—and that's it!



Automatic Software Update Page

Manually Install an Interim Update

Not all available updates from Paessler will be pushed to all customers, but they are still available from the website. Sometimes Paessler support may ask you to update to the latest version.

In this case please click the **Check For Latest Update and Download** button. PRTG will then connect to the Paessler servers and download the setup file, regardless of the status of the update-check. Then **Install Update [version number]**.

To use this function, a direct internet connection is necessary on the computer running the PRTG core server.

Select Other Release Channel

PRTG is available in three different release channels.

For details about continuous rollout and release channels, see the Paessler Blog: [Version 12 of PRTG will introduce "Continuous Rollout"]

To change the release channel you receive updates from, please open the auto-update **Settings** 3007 tab and choose the desired release channel in the **Release Channel** section.

Log

Click the **Log** tab to show log information about the update status of PRTG, newest first. In the table list 207 appearing, you can filter the items by using the respective options 207.

For more information, see the **Logs** 198 section.

Settings

Click the **Settings** tab to configure the PRTG **Software Auto-Update**.

SOFTWARE AUTO-UPDATE

When a New Version is Available	Define what to do when there are software updates available. Choose between: ▪ **Automatically download and install the latest version**: PRTG automatically downloads and installs any new version as soon as PRTG detects that there is a newer version available (PRTG checks this once per day). The installation of a new version will restart the PRTG Windows services and may also include a server restart. ▪ **Automatically download the latest version and alert the admin**: PRTG automatically downloads any new version as soon as PRTG detects that there is a newer version available (PRTG checks this once per day). After successful download, PRTG will create a ToDo ticket 201 for the PRTG System Administrator user. ▪ **Alert the admin only**: When PRTG detects that there is a newer version available, it will not download updates automatically, but create a ToDo ticket 201 only. You can still download updates manually on the **Auto-Update** 3006 page.
Installation Time	If you select the automatic installation option above, choose the desired time for installation of updates from the drop-down menu.
Release Channel	PRTG updates are delivered in different release channels. You can choose between maximum stability, or most early access to new features. Please choose between:

SOFTWARE AUTO-UPDATE

- **Stable: Updated about once per month (most conservative option, recommended)**: These are our best tested versions. Choose this channel for live environments you have to depend on!
- **Preview: Updated about once per week**: Versions in this channel are already thoroughly tested in our labs, but may still contain limitations in certain monitoring configurations. Choose this channel if you are willing to take a little risk for the benefit of getting new features and bug fixes a little earlier. We strongly recommend to not use those versions in live environments you have to depend on!
- **Canary: Updated daily (testing only, should not be used on live systems)**: Updated every night. Use with CAUTION! Software versions in this channel are not tested yet, might contain severe bugs, and are provided for testing purposes only. We strongly recommend to not use those versions in live environments you have to depend on!

For details about continuous rollout and release channels, see the Paessler Blog: Version 12 of PRTG will introduce "Continuous Rollout"

Click **Save** to save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Notes

There are a few things we ask you to consider regarding automatic software updates:

- In order for auto-update to work the machine running the PRTG core server needs direct internet access. If a proxy connection is needed, please configure it in the **System Administration—Core & Probes** 2967 settings.
  For details about the update servers, see this Knowledge Base article: Which servers does PRTG connect to for Software Auto-Update and for Activation?
- During installation the core server may be restarted without notice.
- PRTG updates existing remote probes automatically, causing short downtimes in monitoring of remote locations. In rare cases a manual update of remote probes is required after you update the core server. In these cases you will be notified in the device tree, and monitoring of remote locations will be interrupted until you perform the manual update 93 on the system(s) running the remote probe(s). If a server with a probe uses several network connections with different IP addresses, ensure these addresses are included in the list of allowed IPs 2968. Otherwise the remote probe on this machine might be disconnected after an update.

- In a cluster installation the update needs to be installed on one node only. The new version will then be deployed to all other cluster nodes automatically (causing a short downtime for the monitoring on the cluster nodes, one after another).
- If you run several individual PRTG core servers that are not in a cluster, for example, in combination with the **Enterprise Console** 3028, an update has to be initiated and confirmed for each single core server.
- You can disable automatic downloading on the **Auto-Update Settings** 3007 tab. Updates will then only be downloaded on request, when you click the **Check For Latest Update and Download** button.
- PRTG does not start auto-update downloads if there is less than 500 MB disk space available on the core server system. If this is the case, you can check this on the **Log** 3007 tab.

More

Knowledge Base: Which servers does PRTG connect to for Software Auto-Update and for Activation?

- https://kb.paessler.com/en/topic/32513

Knowledge Base: Which information does PRTG send back to Paessler?

- https://kb.paessler.com/en/topic/28103

Paessler Blog: Version 12 of PRTG will introduce "Continuous Rollout"

- https://www.paessler.com/blog/2012/04/25/news/prtg-12-introduces-continuous-rollout

8.12.15 PRTG Status—Cluster Status

To view the status of your PRTG installation, select **Setup | PRTG Status** from main menu. Click on the tabs to change the different settings.

PRTG Status Tabs

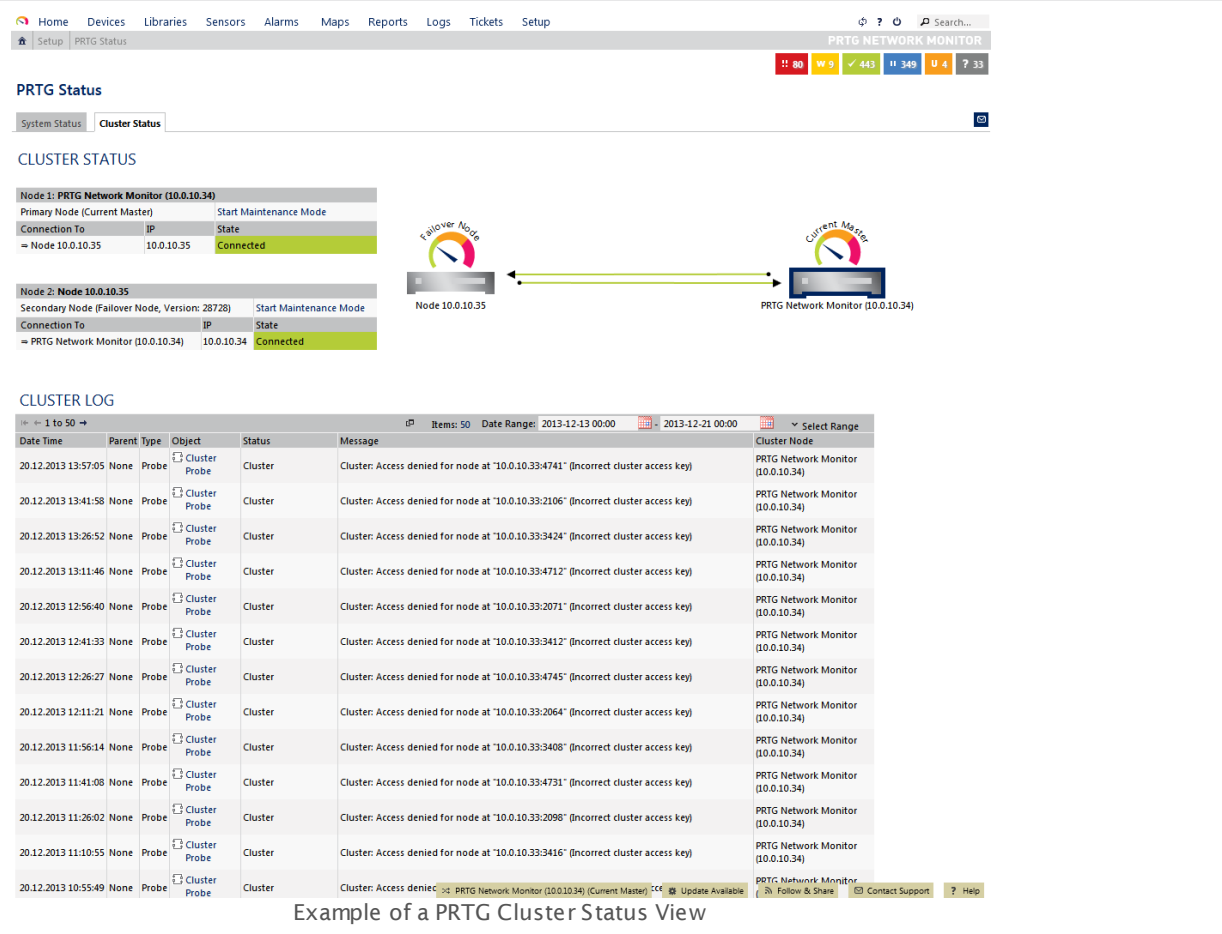
You can view the following aspects of the PRTG status:

- **PRTG Status—System Status** 2994
- **PRTG Status—Cluster Status** 3010

Cluster Status

Click the **Cluster Status** tab to view all nodes connected to the cluster. This tab is only available if you run PRTG in cluster mode 116. The following information is available:

- **Cluster Status** with all connected nodes as table and graphic
- **Cluster Log** with all log entries for cluster connections



Example of a PRTG Cluster Status View

Click the **Start Maintenance Mode** link to put a cluster node in maintenance mode. A node in this mode is still connected to the cluster, but its monitoring results are discarded until you click the **Stop Maintenance Mode** link. You can use this functionality to explicitly exclude a node from monitoring if you know that the monitoring values will not be accurate, for example, because you reconfigure the failover server. During maintenance, a cluster node is displayed with a transparent color in the overview graphic.

On this page, you will not see if your remote probes are connected to failover nodes 3215. Please connect to your failover nodes and check explicitly if remote probes are connected (for example, in the device tree of the PRTG web interface on a cluster node).

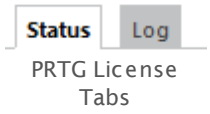
For more information about cluster settings, see section System Administration—Cluster 2992.

This feature is not available in PRTG on demand.

8.12.16 PRTG Status—Licensing Status and Settings

To view information about the license of your PRTG installation and to enter your license key, select **Setup | License** from the main menu.

This option is not available in PRTG on demand.



PRTG License Tabs

You can view the following aspects of your PRTG license:

- **Your License—Status** 3012
- **Your License—Log** 3013
- **Update Your License** 3014

If you use PRTG on premises and open the system administration page from another administration page, PRTG will ask you to enter your credentials again for security reasons if 15 minutes (900 seconds) have passed since your last credential-based login. A dialog box will appear. Enter your **Login Name** and **Password** for PRTG in the corresponding fields and confirm to continue.

This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

Status

Click the **Status** tab to view information about your license.

LICENSING

License Status	Shows the activation status of this installation of PRTG. Usually, PRTG completes the activation automatically during installation or when you change your license information. Only if PRTG cannot connect directly to the internet, a manual activation is necessary. For details, please see **Activate the Product** 91.
License Name	Shows the owner of the license 89 that you use for this installation of PRTG. License Name, license key, and system ID together build your license information.

LICENSING

	You will find the label License Owner in some documents from the Paessler shop. License Owner is the same as License Name for which you will be asked while installing PRTG or when you change your license key 89.
License Key	Shows the license 89 key that you use for this installation of PRTG. License Name, license key, and system ID together build your license information.
System ID	The system ID is a fixed value that is automatically assigned to your PRTG installation.
Licensed Edition	Shows the PRTG edition that you use for this installation of PRTG. This determines how many sensors you can use in your monitoring (see below).
Last Update	Shows the date of the last update for this PRTG installation. We recommend that you use the PRTG **Auto-Update** 3005 to get the most out of PRTG.
Maintenance until	Shows the expiry date and the days remaining for your active maintenance contract. You can buy maintenance for each PRTG license. With an active maintenance contract you may download any available updates and use our premium email support.
Number of Sensors	Shows the number of sensors you can use in your monitoring with your current edition of PRTG (see above). If you reach the limit, PRTG will set each new sensor that you add to a **Pause** status 163 automatically. To upgrade your license right now, click the **Need more sensors? Click here to upgrade!** button to visit our web shop. Editions that allow an **unlimited** number of sensors do not restrict the number of possible sensors by license, so you can create sensors until the performance limit 25 is reached. This means that you can use about 10,000 sensors per core server (depending on your system's performance, sensor types, and scanning intervals). For details, see section **Detailed System Requirements** 25.

Log

Click the **Log** tab to show a table list 207 of all system log entries with all messages and status changes regarding your license.

Change and Update License Information

Use the buttons to edit your license or refresh your maintenance information.

- **Change License Key**: If you want to use another license for this PRTG installation, for example, after an license upgrade, click this button to change your license information. See below 3014 for more details.
- **Refresh Information**: If you have renewed your maintenance and the licensing information above does not show the new maintenance period yet, click this button to manually refresh your maintenance information. An automatic refresh of the maintenance information may take several days. See below 3014 for more details.
- **Deactivate this License**: If you want to use the license of the current PRTG installation on another computer, click this button to deactivate the license. This is necessary, for example, when you move PRTG to another computer, because a PRTG license can be active on only one computer at the same time. Once you have deactivated the license, the PRTG installation on this computer will revert to the Freeware Edition 21 after a grace period of 30 days.

Please see also section **Activate the Product** 91.

Update Your License Information

Click **Change License Key** or **Refresh Information** on the PRTG **License** page to update your license. Provide the necessary information and click **Update License** to complete the activation of your license.

If you have any issues with license activation or update, please click the **Contact Support** button to contact us directly via the **Paessler Service Center** in our shop (internet access required).

STEP 1: CHOOSE ACTIVATION TYPE

Activation Type	Define how you want to validate and activate your license. Choose between: ▪ **Automatic (online activation with optional HTTP proxy)**: PRTG will connect to the activation server and validate your license. The license will be activated automatically. For automatic activation, internet access is necessary from the the computer running this PRTG installation. ▪ **Manual (offline activation)**: Choose manual activation if the PRTG server has no access to the internet and cannot connect to activation.paessler.com. This is the default selection if the PRTG server is offline.

STEP 2: VERIFY YOUR PRTG LICENSE

License Name	Enter the License Name that you have received from us, the Paessler AG. It must exactly match. To avoid typing errors, please copy and paste the **License Name**. You will find the label License Owner in some documents from the Paessler shop. License Owner is the same as License Name for which you will be asked while installing PRTG or when you change your license key 89.
License Key	Enter the license key you have received from us, the Paessler AG. To avoid typing errors, please copy and paste the **License Key**. It must exactly match your license key.
System ID	This field shows the system ID, a fixed value assigned to your PRTG installation. This setting is shown for your information only and cannot be changed here.

For offline activation, click **Save to File** to write your license information into a text file. You can then upload this file to request your activation data on the activation page and do not need to enter your license information manually.

STEP 3: ACTIVATE YOUR PRTG

If you select the automatic activation type, you can now update your license. Define if you need an HTTP proxy for the HTTPS connection to the activation server and click **Update License**.

PROXY CONFIGURATION

This option is not available in PRTG on demand.

Use Proxy Server	We recommend that you use PRTG with a direct internet connection. However, if you need to use a proxy, you can configure the relevant settings here. Choose between: ▪ **No, use direct connection to the Internet (default)**: Do not use a proxy. Use this setting if there is a direct internet connection available to the server running the PRTG core server.

PROXY CONFIGURATION

- **Yes, in our network a proxy is mandatory**: Define proxy settings below.

Proxy settings are valid for Auto-Update 3005, Activate the Product 91, obtaining Geo Maps 2824 tiles, and for sending out HTTP, push, and SMS text message Notifications 2921. The sensor types Cloud HTTP 571 and Cloud Ping 580 use these proxy settings as well.

Proxy Server	This setting is only visible if proxy usage is enabled above. Enter the address of the proxy server that you use for outbound connections. Please enter a valid address.
Port	This setting is only visible if proxy usage is enabled above. Enter the port number of the proxy server that you use for outbound connections. Please enter an integer value.
Use Proxy Credentials	This setting is only visible if proxy usage is enabled above. Determine whether the proxy server needs credentials or not. Choose between: ▪ **Yes, the proxy server requires credentials**: Define credentials (username and password) below. ▪ **No, there are no credentials necessary**: Do not use credentials for proxy connections.
User	This setting is only visible if proxy credentials are enabled above. Enter a username for proxy authentication. Please enter a string.
Password	This setting is only visible if proxy credentials are enabled above. Enter a password for proxy authentication. Please enter a string.

STEP 3: REQUEST ACTIVATION DATA

If you select the manual activation type, you have to request your activation data on https://www.paessler.com/activation using your license information. Open the activation page from a computer that can connect to https://www.paessler.com and provide your license information, or upload the license file that you can save above 3014.

Generate the key file for your license and provide this data below.

STEP 4: PROVIDE ACTIVATION DATA

This step is only necessary if you do an offline activation.

- Copy the content of the key file that you have generated on https://www.paessler.com/activation.
- Paste it into the **Activation Data** field. Alternatively, click **Load from File** if you have saved the key file with your activation data.
- Click **Update License** to complete the activation of your license.

8.12.17 Optional Downloads and Tools

To see optional downloads, select **Setup | Downloads** from the main menu. Click a tab to switch between different options.

Downloads Tabs

There are the following downloads available:

- Client App for Windows (Enterprise Console) 3018
- Client Apps for Mobile Devices 3018
- Remote Probe Installer 3018
- PRTG Tools 3019
- Desktop Notifications 3019

Client App for Windows (Enterprise Console)

Download the Windows Graphical User Interface (GUI) Enterprise Console to the current system. If you use the Enterprise Console, you can access the PRTG on premises web interface with a native Windows application. The version of the Enterprise Console must match the version of your PRTG server. For more information, please see **Install the Enterprise Console** 100.

This feature is not available in PRTG on demand.

Client Apps for Mobile Devices

To monitor your network while on the go, use our free apps for smartphones and tablets. They run on iOS, Android (including BlackBerry devices), and on Windows Phone.

For more information on **PRTG for iOS**, **PRTG for Android**, and **PRTG for Windows Phone**, see the Paessler Website: Mobile Network Monitoring with PRTG—Mobile Apps for Smartphones and Tablets

Remote Probe Installer

With remote probes you can extend your monitoring to distributed networks that are not directly reachable from your PRTG core installation. The version of the remote probe installer must match your version of PRTG.

For more information, see section **Install a PRTG Remote Probe** 93.

PRTG Tools

You can use several freeware tools directly from the Paessler labs which help you to manage your network and to diagnose and test network monitoring issues. Open the **PRTG Tools** tab and click the **More Information and Download** button to navigate to our freeware tools webpage. There you can find a collection of various tools for PRTG Network Monitor.

Find all tools on the Paessler Website: Freeware Network Tools

Desktop Notifications

This tab is only visible if you access the PRTG web interface with Google Chrome or Firefox browser.

For details, see section **Desktop Notifications** 3020.

More

Paessler Website: Mobile Network Monitoring with PRTG—Mobile Apps for Smartphones and Tablets

- https://www.paessler.com/apps

Paessler Website: Freeware Network Tools

- https://www.paessler.com/tools

8.12.18 Desktop Notifications

While you are logged in to the PRTG web interface with your Chrome or Firefox browser, PRTG can show notifications on your desktop whenever there are new alarms in your monitoring.

PRTG will show desktop notifications (by default, in the lower right corner of your desktop) whenever there are new alarms after a page refresh in the PRTG web interface. The notification displays the number of new alarms and the current number of each sensor status.

Example of a Chrome Desktop Notification

To enable desktop notifications in the PRTG web interface, choose **Setup | Downloads | Desktop Notifications** from the main menu bar 243. You have to initially allow the notifications for each installation/profile of Firefox or Google Chrome.

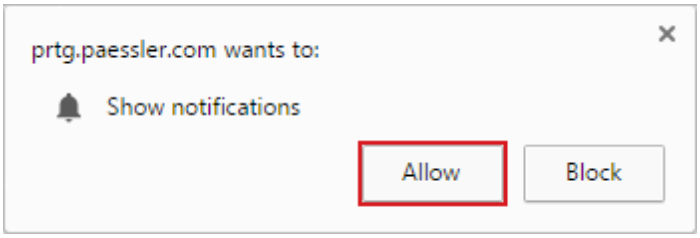
Desktop notifications are not available for Internet Explorer.

Desktop Notifications Settings

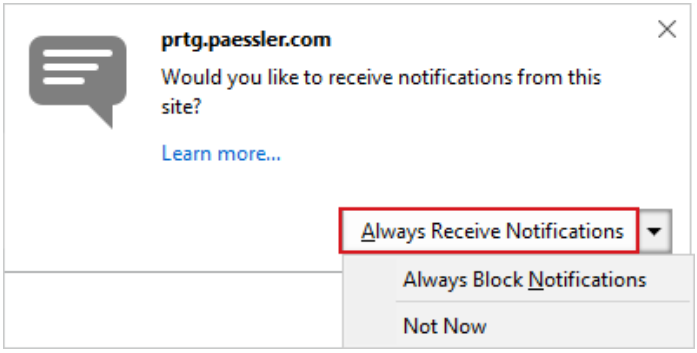
On the settings page, you see one of the following status messages.

Status: Click button below to enable Desktop Notifications

- Click the **Enable Desktop Notifications** button to add your PRTG URL to the list of allowed sites for desktop notifications in Chrome or Firefox.
- On top of your browser window a message appears, asking you to allow desktop notifications.
  - In Chrome, click **Allow** to add the URL of the PRTG web interface to the allowed sites.
  - In Firefox, click **Always Receive Notifications** to add the URL of the web interface to the allowed sites.



Click 'Allow' to enable Chrome Desktop Notifications



Click 'Always Receive Notifications' to enable Firefox Desktop Notifications

Status: Sorry, Desktop Notifications cannot be enabled or **Unknown**

- Desktop Notifications are explicitly blocked for the URL of the PRTG web interface in the browser options. Please see section Disabling or Re-Enabling Desktop Notifications 3021 below.

Status: Desktop Notifications enabled

- Desktop Notifications are successfully activated. To disable them, please see Disabling or Re-Enabling Desktop Notifications 3021 below.

Disabling or Re-Enabling Desktop Notifications

To disallow or re-allow desktop notifications for the PRTG web interface, edit your browser options:

- In **Google Chrome**: Click the **View site information** symbol in the address bar of the browser. You can block or re-allow notifications for the current URL in section **Permissions**.
- In **Firefox**: In the PRTG web interface, hold the Shift key and right-click to open the browser's context menu. Click **View Page Info** and select the **Permissions** tab. In section **Notifications**, select the desired option for the PRTG website, for example, block desktop notifications or enable them again.

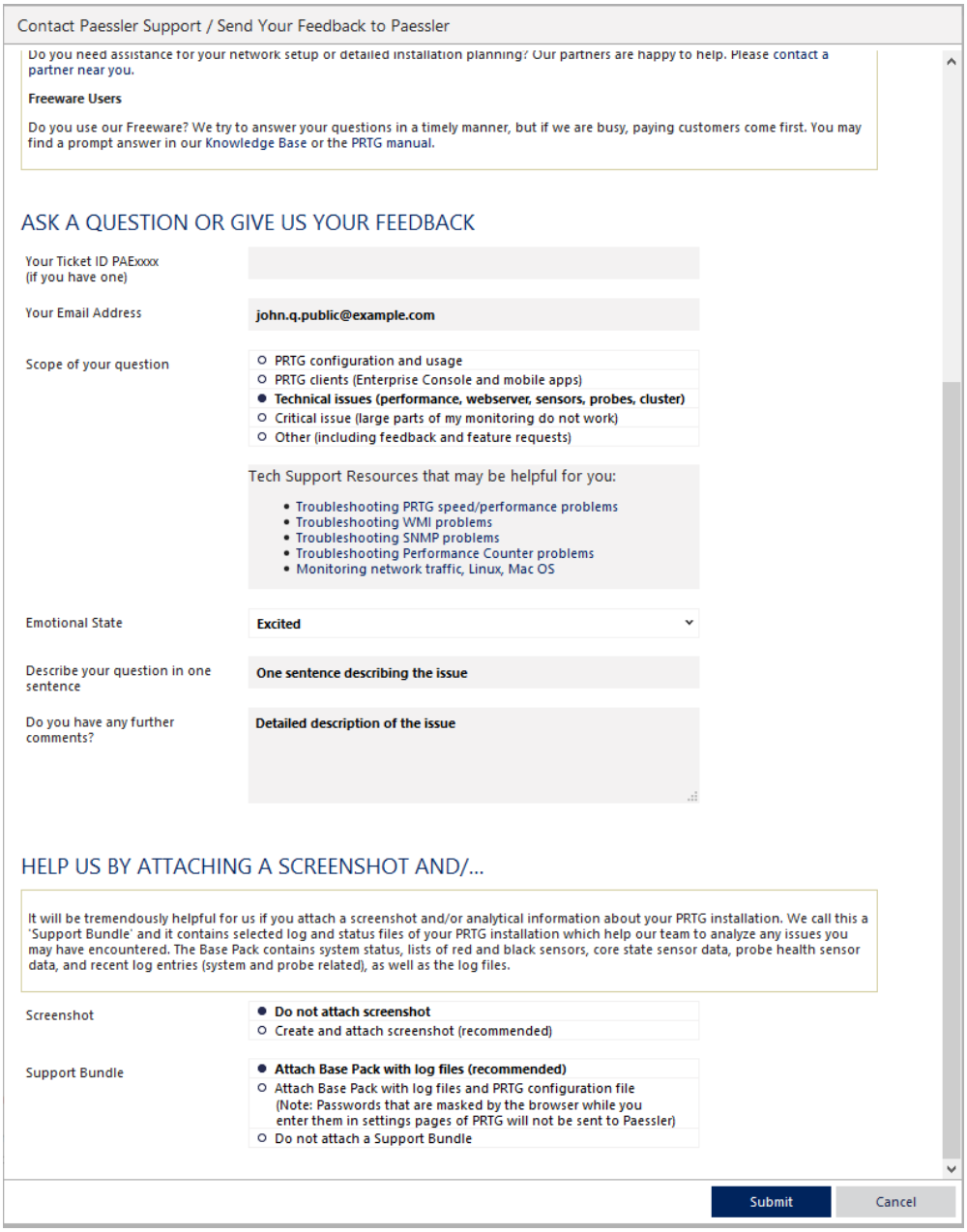
8.12.19 Support—Contact Support

To open the **Contact Paessler Support / Send Your Feedback to Paessler** window in PRTG, choose **Setup | Contact Support** from the main menu. You can open this form also via the footer **Contact Support** on any page in PRTG.

On the one hand, you can adapt this page as feedback form. Help improve PRTG by providing criticism, praise, bug reports, and feature requests. Any comments are welcome! Your feedback will be handled directly by the Paessler support team.

On the other hand, you can use this function to ask for support regarding technical issues. To make the support contact more comfortable, PRTG can automatically attach a screenshot in combination with a Support Bundle which contains several selected PRTG log and status files. This information will help our support team a lot to analyze any issues you may have with PRTG. Please also consider the suggested links to articles regarding the scope of your issue.

PRTG transmits your feedback or support question including the support bundle securely to Paessler via the PRTG Cloud. Please make sure your PRTG server has access to the internet and can reach the URL https://api.prtgcloud.com:443



Contact the Paessler Support or Send Feedback

Ask a Question or Give Us Your Feedback

Provide the following information in this section of the contact form:

- **Your Ticket ID PAExxx**: If you have already opened a new ticket (either directly via email to support@paessler.com, or via the Knowledge Base, or via the support form on paessler.com), enter its ID here. You can find it in your confirmation email regarding the request we received. You can provide the ID with "PAE" in front or just the number. If you leave this field empty, you will create a new ticket when you submit this form.

- **Your Email Address**: Enter your email address here. You can provide any of your addresses; however, recommended and default is the email address of your PRTG account to be able to associate you with your license.
- **Scope of Your Question**: Select a topic regarding your issue and consider the proposed links.
- **Emotional State**: If you want to, you can indicate your current feelings about PRTG.
- **Describe Your Question in One Sentence**: Provide short information with max. 60 characters to indicate the topic of your issue.
- **Do You Have Any Further Comments?**: Leave your comments here. It can be feedback or support questions. Please describe your issue as detailed as possible!

Attach a Screenshot and/or Support Bundle

To provide as helpful information as possible, you can attach a screenshot of the current page and a support bundle with useful analytical data about your PRTG installation.

In section **Screenshot**, choose between:

- **Do not attach screenshot**: Send the ticket without a screenshot.
  We recommend that you attach a screenshot of the affected PRTG webpage so that we can understand your request more easily.

- **Create and attach screenshot (recommended)**: Create a screenshot of the currently displayed page in PRTG to send it with your ticket. You can see a preview below the screenshot section.
  If you encounter issues on a specific page in PRTG, open the contact support form on this page to get a screenshot of it. This is not possible on error pages which are not meaningful enough for our support team to solve your issue.

In the section **Support Bundle**, you can choose between several packages that differ in coverage of information:

- **Attach Base Pack with log files (recommended)**: Contains log files of your PRTG installation and the following information:
  - System status
  - Lists of sensors regarding their current states
  - Core state data
  - Probe Health sensor data
  - Current log entries
- **Attach Base Pack with log files and PRTG configuration file**: Additionally contains the configuration file.
  Send this package only if our support team told you so! Encrypted passwords in the config.dat file and passwords that your browser masks while you enter them on settings pages will be removed before PRTG sends this package to Paessler Support.
- **Do not attach a Support Bundle**: The ticket will not contain files. Choose this option only when sending feedback.

Click the **Submit** button to send your request directly to our technical support team, or click **Cancel** to return to the page from which you opened the contact form. Usually you will receive an answer by our support team within one or two business days, no matter whether you provide feedback or you have a question.

If you have questions or feedback regarding your license purchase, upgrade, or maintenance extension, please contact our customer service 149.

More

Knowledge Base: How does Paessler handle user feedback and feature requests?

- https://kb.paessler.com/en/topic/33873

Part 9

Enterprise Console

9 Enterprise Console

The Enterprise Console (in old PRTG versions called "Windows GUI") is one alternative interface [111] that you can use to connect to the PRTG core server to configure your setup, view monitoring results, and keep an eye on your network. It is a native Windows application for fast access to data and monitoring management.

The Enterprise Console (EC) provides extended pop-up window functionalities, as well as a seamless link to the Ajax web interface [136] where you can change your monitoring configuration and access further functionalities such as reporting [3053], maps [3051], system setup [3059], tickets [3057], and libraries [3045]. The EC shows most of the functions with an embedded webkit browser, for a few options the EC opens an external browser window (using your default browser).

Remarks

The Enterprise Console runs under all supported Windows versions [25], but it is not fully compatible with Windows 10. Running the EC on Windows 10 results in several issues so please use another operating system. We will consider full Windows 10 support for future PRTG desktop clients.

The Enterprise Console does not support **System Information** [193] and does not show this tab on devices. Please use the PRTG web interface to access system information of a device.

PRTG on demand does not support connections from the Enterprise Console. If you want to use it, please connect the Enterprise Console to a PRTG on premises instance.

Access Several Core Servers in One Console

As an additional functionality, you can configure access to several PRTG core servers in the Enterprise Console. It can show data of all your independent core server installations at a glance (for example, the device tree [3038] and alarms list [3049]), so you can manage your monitoring centrally, also when it is spread across different servers.

Getting Started

Every installation of PRTG Network Monitor includes the Enterprise Console and installs it automatically on the computer running the PRTG core server. If you want to use the Enterprise Console on another computer, please download [3018] and install it there. For details, please see the **Install the Enterprise Console** [100] section.

The Enterprise Console is mainly designed to review and manage an existing installation of PRTG that you have already set up. If you just start monitoring, we recommend that you first run through the **Smart Setup** [50] in the PRTG web interface [136] and add your network devices there.

For detailed instructions, see section **Quick Start Guide** [44]. Once finished, you can seamlessly switch to the Enterprise Console.

Requirements for Connections to PRTG Web Server(s)

To show monitoring data of your PRTG setup, the Enterprise Console must be able to establish a connection to your PRTG web server(s). For this purpose, please ensure the following.

- The following server settings in the Enterprise Console have to match the following settings in the **PRTG Administration Tool** 3135.
  See section **PRTG Servers** 3062 for details.

ENTERPRISE CONSOLE SERVER SETTINGS	PRTG ADMINISTRATOR SETTINGS
Server IP / DNS name	**IP address for PRTG's Web Server** on the **Web Server** tab
Port	**TCP Port for PRTG's Web Server** on the **Web Server** tab PRTG switches to port **8080** as a fallback after a restart when port 80 is already used, and to port **8443** if port 443 is not available. PRTG keeps the SSL connection in this case. If this port is also not available, PRTG tries from port 32000 on until it finds an available port. Because the EC cannot recognize these ports (8080, 8443, 32000+) automatically, enter the currently used port manually here in the **Port** setting. If you do not get a connection to the PRTG web server, check the currently used port in the **Web Server** settings under **System Administration—User Interface** 2946 in the PRTG web interface.
Login Name	**Login Name** on the **Administrator** tab
Password	**Password** on the **Administrator** tab

- No local software firewall blocks the connection.
- No local virus protection program blocks the connection.
- The specified port is not used by another application.
- No (hardware) firewall blocks the connection when connecting through a network (LAN or WAN).
- The software versions of the Enterprise Console and the PRTG web server have to match at least in the third number (for example, EC version 3035 15.3.18.3590 can connect to server version 151 15.3.18.3796).

For common issues with the Enterprise Console and their solutions, see this Knowledge Base article: Problems with the Enterprise Console: What can I do?

More

Knowledge Base: Problems with the Enterprise Console: What can I do?

- https://kb.paessler.com/en/topic/60091

Enterprise Console—Topics

- First Start 3031
- General Layout 3033
- Menu Tabs and Page Content 3037
- PRTG Servers 3062
- Options 3065
- Windows Menu Structure 3071
- Context Menus 3079
- Shortcuts Overview 3080

Related Topics

- Ajax Web Interface—Basic Procedures 136
- Ajax Web Interface—Device and Sensor Setup 248
- Ajax Web Interface—Advanced Procedures 2804
- Other User Interfaces

9.1 First Start

This section helps you to start the Enterprise Console for the first time.

Open the Enterprise Console

Double click the **PRTG Enterprise Console** icon in the Windows start menu to open it. As soon as it opens, the Enterprise Console tries connecting to your PRTG installation, according to the defined PRTG server connection settings. In a fresh install of PRTG, the settings for the Enterprise Console installed on the computer running the PRTG core server are already predefined, so you can use the Enterprise Console right away. If you get an error message when opening the Enterprise Console, please check the connection settings 3029. For example, adjusting the settings is necessary if you changed the IP address of the server.

For detailed information, see section **PRTG Servers** 3062 (**PRTG Server Connection**).

Remarks

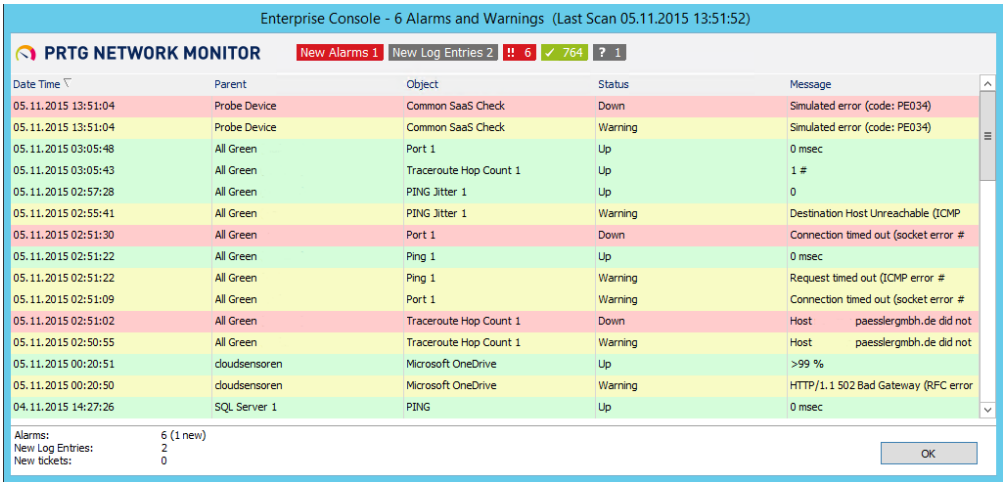
The Enterprise Console runs under all supported Windows versions 25, but it is not fully compatible with Windows 10. Running the EC on Windows 10 results in several issues so please use another operating system. We will consider full Windows 10 support for future PRTG desktop clients.

The Enterprise Console does not support **System Information** 193 and does not show this tab on devices. Please use the PRTG web interface to access system information of a device.

PRTG on demand does not support connections from the Enterprise Console. If you want to use it, please connect the Enterprise Console to a PRTG on premises instance.

Tray Window

By default, the Enterprise Console runs in background and shows a message box whenever there are new alerts, new messages, or new tickets for your monitoring. This window is one of the first things you see after opening the Enterprise Console.



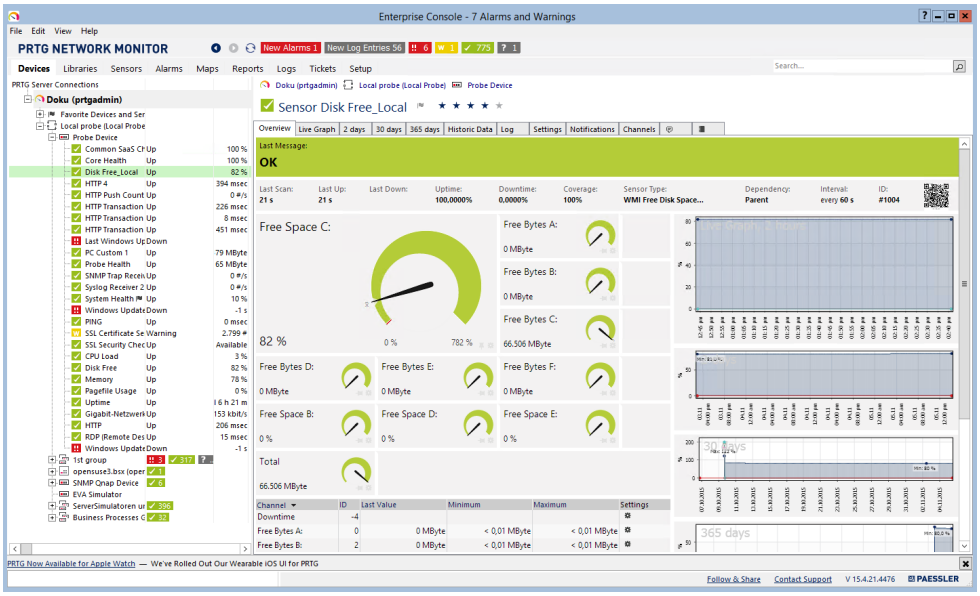
Example of the Tray Window

This window is always shown on top. Click the **OK** button to close it. You can change the tray behavior in the Enterprise Console settings.

For detailed information, see section **Options** 3067 (**System—Alerting**).

9.2 General Layout

The main layout of the Enterprise Console (EC in short form) program consists of different elements. See below for details.



PRTG Enterprise Console

From top to bottom, the main layout consists of:

- The Windows menu 3034.
- The page header bar 3034 with the PRTG logo, the viewpoint arrow symbols, the refresh icon, and the sensor states overview.
- The menu tabs bar and page content 3034 underneath.
- The server selection 3035 and search bar 3035 in the upper right corner.
- The news feed 3035 underneath the page content.
- The status bar 3035 at the bottom of the window.

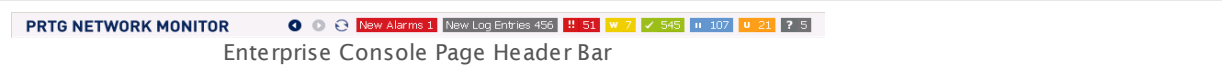
Often, the Enterprise Console displays data and settings directly. Some functionalities and extended setup additionally require a new window of the system's default browser and the web interface 136 shows up. In this case, you are logged in to the web interface automatically via username and hash value 2909. In your browser, it might be necessary to confirm the certificate that is used by the PRTG web server. For more information, please see **SSL Certificate Warning** 142 section.

If you configure your Enterprise Console for a connection with more than one PRTG core server, keep an eye on the server selection 3035 bar to choose which server's data you want to access.

Windows Menu

The Windows menu gives access to general configuration and settings. For details, please see section **Windows Menu Structure** 3071.

Page Header Bar



Enterprise Console Page Header Bar

The page header consists of the following parts:

- **PRTG Logo**
  Click the PRTG Network Monitor logo to open the Ajax web interface 136 in the browser which you define in the Enterprise Console **Options** 3065. If you configured several PRTG core servers, the browser loads the web interface of the server that you have currently selected in the **Devices** 3038 tab.

- **Previous Viewpoint / Next Viewpoint (Arrow Symbols)**
  The Enterprise Console stores the different views which you navigate to in the application. Using these arrows (or using the shortcuts Alt+Left and Alt+Right), you can step back and forth in the history, just as you know from your web browser.

- **Refresh (Arrow Circle Symbol)**
  Click the refresh symbol (F5) any time to refresh the current screen. This immediately queries data for the current screen from all active PRTG core servers just as the automatic refresh does. You can configure the update interval in the **Options** 3065 settings.

- **Global Sensor Status Symbols**
  This area shows the aggregated status of all sensors from all active PRTG core servers, divided into different sensor states. Depending on the particular sensor states, you see colored boxes with numbers which symbolize the sensors. For example, you can see how many sensors are in **Up**, **Down**, **Warning**, **Pause**, **Unusual**, or **Unknown** status 163. Click a status icon to view a list of all sensors in the respective status.
  Next to the global sensor status symbols you can also see the number of new alarms and new log entries, as well as the number of new tickets, if there are any. Click the respective icons to view **Alarms** 190, **Logs** 198, or **Tickets** 200.
  When you view sensor lists, you can only show the sensors of one server at once. So, the global sensor overview shows the total number of sensors in a certain status on all active servers, but viewing a list of all sensors in a certain status from all servers is not possible for performance reasons.

Menu Tabs Bar and Page Content

You can navigate through your setup using the menu tabs bar. Please take a few minutes to familiarize yourself with all menu items. The page content underneath varies depending on the selected menu tab. It shows various information about your monitored objects.

For a detailed description of all tabs, see section **Menu Tabs and Page Content** 3037.

Server Selection

Enterprise Console's Server Selection and Search Bar

In the server selection bar you see all active PRTG core server connections that are configured for the current Windows user account (saved in the registry).

The server you select here determines globally which information the EC shows in all **Menu Tabs** 3037 (except the **Devices** tab: the server selection does not apply for the devices tab). Depending on your selection, **Libraries**, **Sensors**, **Alarms**, **Maps**, **Reports**, **Logs**, **Tickets**, and **Setup** options are shown for the respective server only. Select **All PRTG Servers** to show consolidated information for all active PRTG core servers which appear in the list.

For technical reasons, you cannot show consolidated information from all servers in the **Sensors**, **Setup**, and **Search Results** tab. To use these tabs, please select one single PRTG core server from the server selection bar.

Select **File | Manage PRTG Server Connections** from the main menu 3071 to add or remove **PRTG Servers** 3062 from the list, or to edit an existing one.

Search Bar

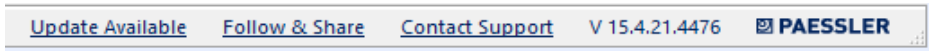
Select a single PRTG core server from the server selection 3035 bar and enter a key word to search the respective server. In the **Search Results** tab, the Enterprise Console displays matching monitoring objects, help topics, and related objects. If you click a monitoring object (for example, a sensor) in the search results, the Enterprise Console opens this object on the **Devices** 3038 tab with details in the device tree.

If you have configured a connection in the **PRTG Servers** 3062 options that uses a **Root ID** 3064 other than 0, the EC will ignore this setting while searching. In this case, the EC shows **Search Results** for the entire server (starting at Root ID 0).

News Feed Bar

The news feed bar shows latest news by Paessler. Click the bar to open a window with an overview about recent articles. You can open a specific article in the web browser by clicking the particular header. If you do not want to show the news feed in your Enterprise Console, click the X symbol besides the bar. You can enable it again via **View | Show News Feed** in the main menu 3076 (Ctrl+N).

Status Bar



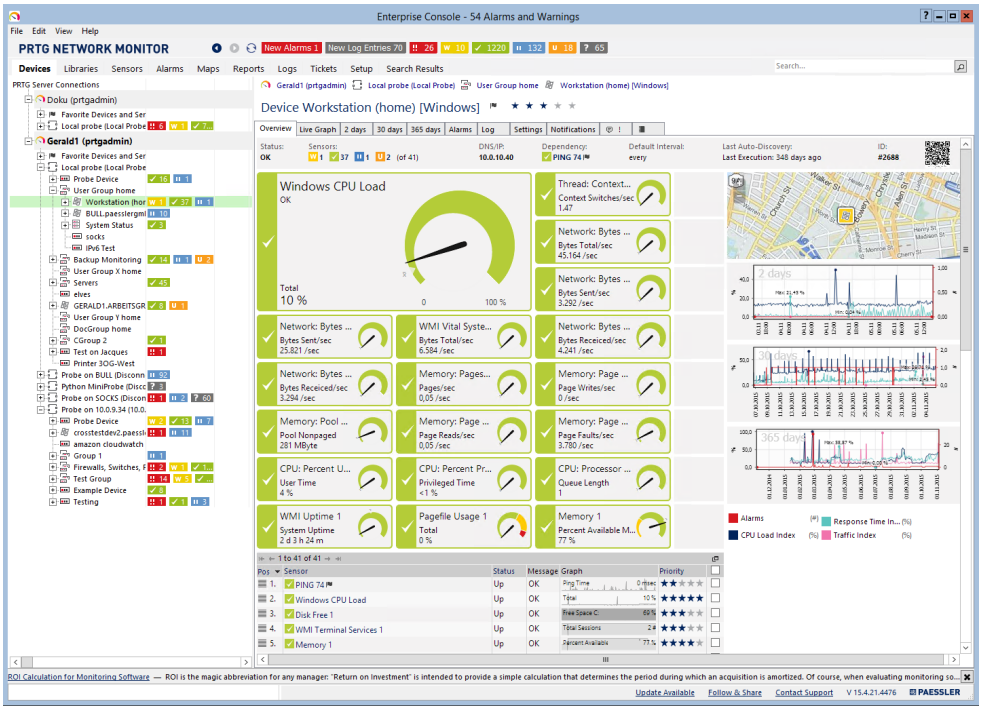
Enterprise Console Status Bar

The status bar shows the version number of your PRTG Enterprise Console and the Paessler logo which leads you to the Paessler website when you click it. Furthermore, the status bar contains a **Contact Support** 3022 link which opens a window to leave feedback or to ask for support, and a **Follow & Share** link which opens PRTG's social network contact information in the Ajax web interface.

You will also see a note if an update for one of connected servers is available. Click **Update Available** to open the **Auto-Update** 3005 page in the EC.

9.3 Menu Tabs and Page Content

Under the different menu tabs of the Enterprise Console, you can navigate through various pages with information about your monitored objects, such as your network status and monitoring results, for example.



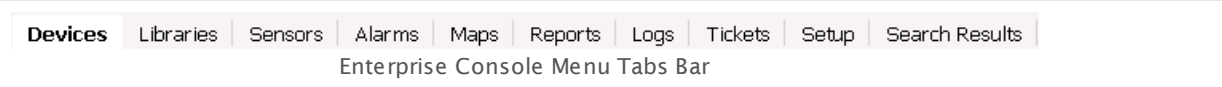
PRTG Enterprise Console — Device Details

The following sections introduce the available options within the different tabs:

- Devices 3038
- Libraries 3045
- Sensors 3047
- Alarms 3049
- Maps 3051
- Reports 3053
- Logs 3055
- Tickets 3057
- Setup 3059
- Search Results 3061

9.3.1 Devices

The Enterprise Console has a tab-like interface. Using the tabs you can navigate through various pages with information about your monitored objects, such as your network status and monitoring results, for example, as well as access maps, reports, tickets and settings.



Enterprise Console Menu Tabs Bar

There is documentation available for the following tabs:

- Devices 3038
- Libraries 3045
- Sensors 3047
- Alarms 3049
- Maps 3051
- Reports 3053
- Logs 3055
- Tickets 3057
- Setup 3059
- Search Results 3061

Devices Menu Tab

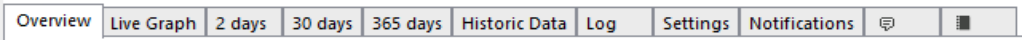
The **Devices** tab is your starting point for everyday use. The page is split into two parts. On the left hand side, it shows the tree-like device view which lists all configured PRTG core servers with their probes, groups, devices, and the sensors on the devices, in a hierarchical order. Next to each object you see an overview of the number of sensors, grouped by their current status.

The first child node of the tree is called **Favorite Devices and Sensors**. It contains all devices and sensors that you marked as favorites 211. To add an object to the favorites list, right-click the desired device or sensor and select the **Add to Favorites** entry from the context menu 215.

For more information about the hierarchical order of the different objects in the device tree, see section Object Hierarchy 118.

On the right side you see details about the object selected on the left. The information is spread over several tabs.

Over the object's name you see always a path which you can use to navigate through the device tree. It can also help you to orient yourself if you get lost. If you click a breadcrumb item, a drop-down menu opens that shows all available objects on the same level. For example, you can use this to directly access all other sensors or a device, other devices within a group, another group on the same probe, other probes in your root group, or another PRTG server.



Enterprise Console Sensor Sub-Tabs on the Device Tab

Edit Objects in the Device Tree

Use the **Edit** menu (or the object's context menu 3079) to access different important functions of the items you have currently selected in the device tree on the left hand side.

- Add devices or sensors to the favorites list (or remove them from the list)
- Sort all sub nodes of an object alphabetically
- Move objects up and down in the tree
- Check now
- Pause monitoring
- Access tools
- and many more

For details about the available options, see section **Windows Menu Structure** 3071.

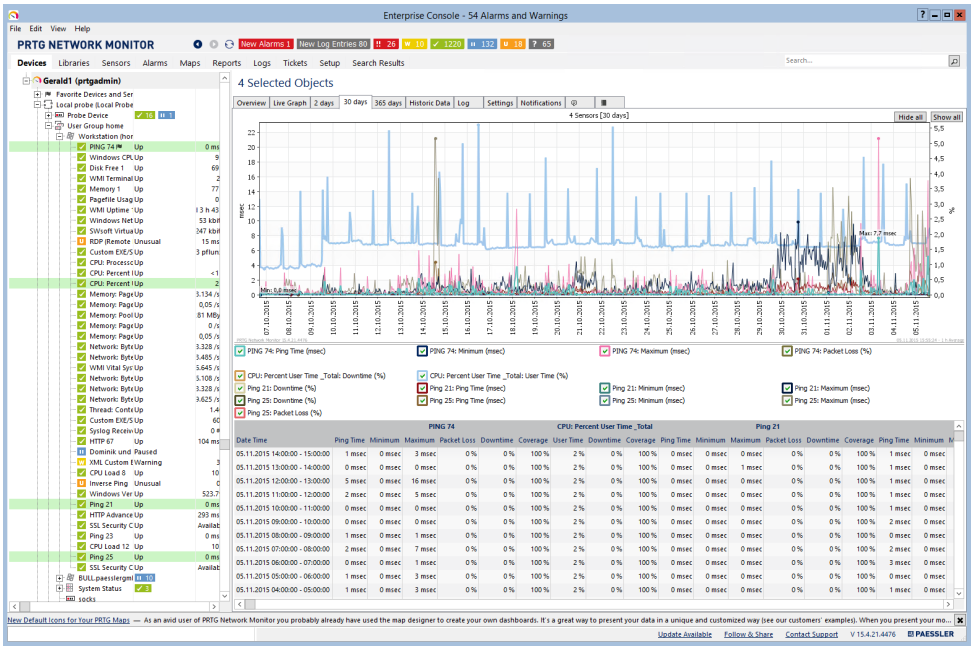
Select Multiple Items in Device Tree

In the device tree shown on the left, you can select one or more objects, even from different PRTG core servers. Hold down the Ctrl key to select more objects simultaneously with your mouse. Usually, you select more than one item to view combined graphs, or to apply a command from the **Windows Menu** 3071 (for example, **Check Now** or **Pause**) to several objects.

When you select multiple items, the sub-tabs on the right side show data for all selected items at a glance. For example, when if you select two sensors, you see their tables next to each other. Graphs will actually appear combined! This is a great way to instantly show one chart containing the graphs of all selected objects. Each sensor channel is represented as one line. This aggregated view works for all kind of objects.

The tab **Live Graph** shows data for sensors only.

Below each graph you see a key. Hover over an entry in the key to display the corresponding line in the graph above in **bold**.



Aggregated Graph View in Enterprise Console

You may need to enlarge the Enterprise Console's window to see all tables and graphs.

Devices—Overview

The **Overview** tab shows general information about the selected object. Depending on the selected object selected, you can see different information.

- For servers, probes, and groups the table shows information in the **Name** and **Status** section, such as priority, parent objects and number of sensors on this object. Additionally, the window shows a geographical map, if enabled in your PRTG configuration as well as in the Enterprise Console's **View** 3076 menu, and index graphs 168.
  For detailed information about geographical maps, see section **Geo Maps** 2824.

- For devices, the **Overview** tab shows device details and summary graphs for different time spans, gauges, as well as a list of all sensors on this device, recommended sensors 184, and a geo map.

- For sensors, the **Overview** tab shows sensor details, current status, and the last value of all sensor channels, as well as sensor graphs for different time spans. You can also edit channel settings in this tab by clicking on a channel's gear icon.
  For details, see section **Sensor Channels Settings** 2782.

Devices—Live Graph, 2 days, 30 days, 365 days

These tabs are only available if you enable the **Large Single Graph** (Ctrl+L) view in the **Windows Menu** 3076 (**View**).

For **Small Multiple Graphs** view, see section **Devices—Graph** 3041 below.

Select one of the tabs to display an object's monitoring results as **Live Graph** (content available for sensors only), or for different time spans in more or less detail (**2 days**, **30 days**, **365 days**). On every tab, you will see graphs as well as data tables.

While you view a sensor graph, you can hide single sensor channels individually. Remove the check mark symbol in front of a channel name underneath the graph, and the line of the according channel disappears. You can also **Show all** or **Hide all** channels by clicking these buttons in the graph. The graph view is reset immediately.

The days mentioned here are the default setting. You can change the detail of the different graphs any time under **System Administration—User Interface** 2950.

Below each graph you see a key. Hover over an entry in the key to display the corresponding line in the graph above in **bold**.

Devices—Graph

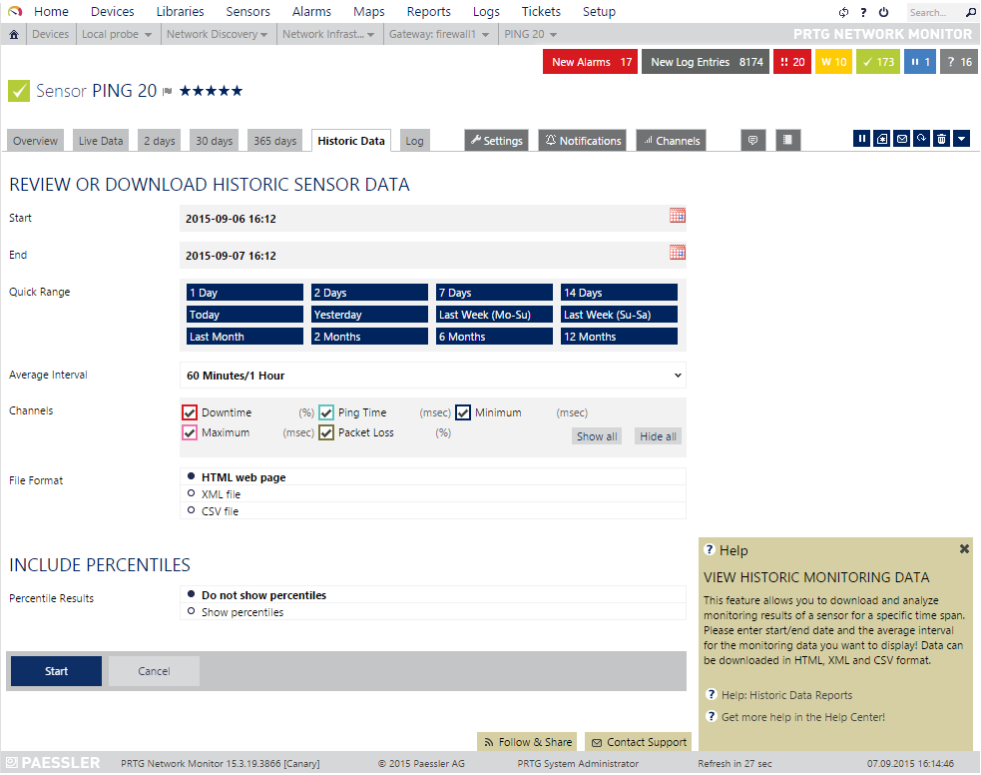
This tab is only available if you enable the **Small Multiple Graphs** (Ctrl+S) view in the **Windows Menu** 3071 (**View**). For **Large Single Graphs** view please see above 3040. This tab shows an overview with single graphs and data tables for live data, 2 days, 30 days, and 365 days. It might be necessary to enlarge the window to display all graphs.

The days mentioned here are the default setting. You can change the detail of the different graphs any time under **System Administration—User Interface** 2950.

Below each graph you see a key. Hover over an entry in the key to display the corresponding line in the graph above in **bold**.

Devices—Historic Data

The **Historic Data** tab is available for sensors only (not for probes, groups, or devices). When you open the historic data tab of a sensor, there is no sensor selection available. If you want to select a different sensor for the report, select **Sensors | View Historic Data** from the main menu in the PRTG web interface.



Historic Data Tab of Ping Sensor

Click here to enlarge: http://media.paessler.com/prtg-screenshots/historic_data_tab_ping_sensor.png

Select the **File Format** for the results:

- **HTML web page**: Opens a new browser window with the historic data report
- **XML file**: Opens a new browser window with the historic data report as XML file.
- **CSV file**: Opens a new browser window with the historic data report as CSV file.

When you click one of these items, a new window or tab of the external browser configured in the Enterprise Console's **Options** 3069 will open. PRTG automatically logs in and redirects you to the respective web page. If your browser displays a certificate warning, please find more information in section **SSL Certificate Warning** 142.

View and functionality are the same as in the web interface. For details about the available **Historic Data** report options, see section **Historic Data Reports** 175 of the Ajax Web Interface 136 documentation.

Devices—Log

Click the **Log** tab to show a table list with all log information on this object. This is a subset of the entries available via the **Logs** 3055 menu tab.

The list can show up to one hundred entries at a time. Use the arrow symbols above the list to show other items. You can jump to the beginning of the list, or browse through it hundred by hundred. If the list has more than one entry, you can also sort the items by the contents of a certain column. To sort, simply click the header of the column you want to sort by once or twice.

Devices—Settings

The **Settings** tab loads and displays the currently selected object's settings from the web interface. View and functionality are the same as in the web interface. For every type of object and for every sensor, different options are available. For detailed information, please see the following sections (depending on the selected object) in the Ajax Web Interface 136 documentation:

- **Probe Settings** 312
- **Group Settings** 334
- **Device Settings** 360
- **Sensor Settings** 384

Devices—Settings—Multi-Edit

If you select several objects on the left side, the **Settings** tab switches into multi-edit mode 2814. Using multi-edit, you can set a check mark for one or more settings. All changes apply to all selected objects. The multi-edit dialog displays settings which are common among the selected objects only.

If you select only sensors on the left side in the device tree, the **Settings** tab additionally displays a **Channel Settings** tab. Using this tab you can multi-edit the settings of any channels 2782 which are common among the selected sensors, as long as the channels have the same name. Set a check mark for one or more channel settings. All changes apply to all selected sensors.

You cannot use multi-edit for objects on different PRTG core servers.

Devices—Notifications

The **Notifications** tab loads and displays the currently selected object's settings from the web interface. View and functionality are the same as in the web interface. You can set different notification triggers.

For detailed information, see section **Sensor Notifications Settings** 2791 in the Ajax Web Interface 136 documentation.

You cannot change notification settings for multiple objects at a time. We recommend that you use the **Inheritance of Settings** 122 for easy configuration.

Devices—Comments

The **Comments** tab loads and displays the currently selected object's settings from the web interface. View and functionality are the same as in the web interface.

On the **Comments** tab you can enter free text for each object. You can use this function for documentation purposes or to leave information for other users.

Click **Save** to save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Devices—History

The **History** tab shows all changes to the settings of an object with a timestamp, the PRTG user which conducted the change, and a message.

Drag & Drop Sorting in Device Tree

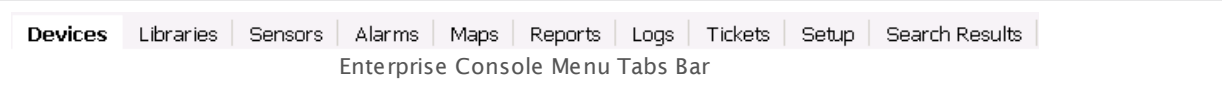
In the device tree, you can also move probes, groups, and devices simply via drag and drop. Activate it in the Windows menu 3071 under **Edit | Drag & Drop Sorting** and then drag your objects as you like: You can move devices and groups, or add groups or devices to other groups. You can also move objects via the context menu 3079.

You cannot move objects in the following cases:

- You cannot move any objects from one PRTG core server to another.
- You cannot move sensors from one device to another. To clone sensors to other devices using drag & drop, please use the Ajax Web Interface 136.
  For detailed information, see section **Manage Device Tree** 292.
- You cannot move devices from one group to another.
- You cannot move groups from one probe to another.
- You cannot move probes from one core server to another.

9.3.2 Libraries

The Enterprise Console has a tab-like interface. Using the tabs you can navigate through various pages with information about your monitored objects, such as your network status and monitoring results, for example, as well as access maps, reports, tickets and settings.



Enterprise Console Menu Tabs Bar

There is documentation available for the following tabs:

- Devices 3038
- Libraries 3045
- Sensors 3047
- Alarms 3049
- Maps 3051
- Reports 3053
- Logs 3055
- Tickets 3057
- Setup 3059
- Search Results 3061

Using Libraries is a great way to keep an eye on your network status because you can individually select which sensors you would like to see there.

For a general introduction to PRTG Libraries, see section Libraries 2845.

Libraries Menu Tab

The page is split into two parts. On the left hand side you see all available libraries from one or several servers, on the right hand side the actual libraries.

- Click a library's name to display it. In the tabs above the library, select from Overview 2845, Management 2852, Settings 2855, Notifications 2829, Comments 2859, and History 2860. Each of these tabs loads the respective functionality of the Ajax Web Interface 136. Click the **Save** button to apply changes to your settings.
- Underneath the tabs bar, there are different options available to change the current library view: You can set sensor filters (set or remove check marks to include or exclude sensors in a certain status) and change the device tree view.
  For details about the tree view, see section General Layout—Tree View Layout 151.
- Click a library node to edit the node settings 2855 in a new window.
- Double-click a library's name on the left to open the library in the configured external web browser. You can edit it or add new libraries to this PRTG server.

- Right-click a library's name to open its context menu 3079. The following options are available: **Add**, **Edit**, **Delete**, **Clone**, **Send link by email**, and **Open in Web Browser** in the libraries overview on the left, **Details...**, **Edit**, **Remove from Library...**, **Add Library Node...**, **Add Group...**, and **Send Link by Email** on the **Overview** tab of a specific library on the right.
- Use the button **Add Library** to create a new library and the button for object history 241 to view all changes to libraries.

For more details about PRTG Libraries, see section **Libraries** 2845.

Libraries Menu Tab—Add Library

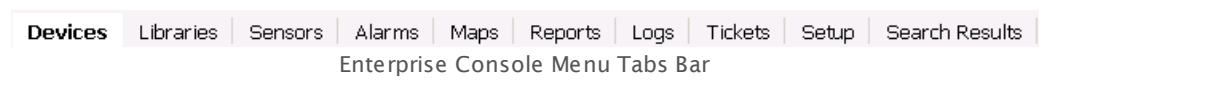
Click the **Add Library** button to add a new library to a PRTG server.

Depending on the current setting shown in the server selection 3035 bar in the upper right corner, an (embedded) window will open (if one specific server is selected), or you will see a selection window that asks you to choose the core server you want to add the new item to. Choose an installation to start.

For details about adding a library, see section **Libraries Step By Step** 2848.

9.3.3 Sensors

The Enterprise Console has a tab-like interface. Using the tabs you can navigate through various pages with information about your monitored objects, such as your network status and monitoring results, for example, as well as access maps, reports, tickets and settings.



Enterprise Console Menu Tabs Bar

There is documentation available for the following tabs:

- Devices 3038
- Libraries 3045
- Sensors 3047
- Alarms 3049
- Maps 3051
- Reports 3053
- Logs 3055
- Tickets 3057
- Setup 3059
- Search Results 3061

Viewing lists of sensors is a great way to keep an eye on your network status because you can select which kind of sensors you want to see. You can filter by various parameters like object or sensor type, for example, and current sensor status.

Sensors Menu Tab

For technical reasons, this function is available for one server at a time only. If you have configured more than one PRTG core server, choose one server from the server list in the upper right corner.

Click the **Sensors** entry in the menu tabs bar to show a table list of all sensors. You can enable a filter to only show certain sensors. To do so, choose from three different drop down menus to build a filter. With each filter you can further decrease the number of shown sensors.

- **By Type**
  The second drop down menu shows all sensor types 385 available in your monitoring setup. Select an entry to only show sensors of this type. The default value is **All Types**.

- **By Status**
  The third drop down menu shows all possible sensor states[163]. Select an entry to only show sensors that currently show this status. Choose between **All States**, **Down**, **Down (Acknowledged)**, **Down (Partial)**, **Warning**, **Up**, **Paused**, **Unusual**, and **Unknown**. The default value is **All States**.
  If you click a sensor symbol in the page header bar[3034], you can directly view a sensor list filtered by the selected sensor status for the selected server.

If you have filtered out all sensors and the list below shows no entries, remove some filters by reverting them to the default values.

In the column **Last Value**, the table only shows the last value of the sensor's **primary channel**.

The list can show up to one hundred entries at a time. Use the arrow symbols above the list to show other items. You can jump to the beginning of the list, or browse through it hundred by hundred. If the list has more than one entry, you can also sort the items by the contents of a certain column. To sort, simply click the header of the column you want to sort by once or twice.

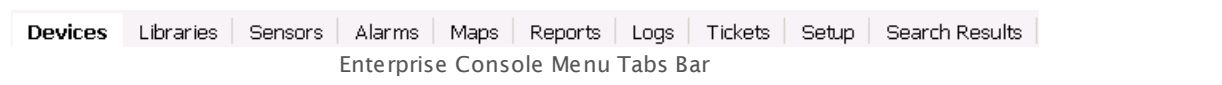
From this list view, you can select multiple items to apply the same action to them, for example, **Edit | Check Now**.

You can select multiple items by the following means (you can also combine them):

- Click and hold your left mouse key while pointing to the lines you want to select
- Hold the Ctrl key while clicking to toggle the selection status of a single line
- Click a line and hold the Shift key while clicking another line to select all lines in between.

9.3.4 Alarms

The Enterprise Console has a tab-like interface. Using the tabs you can navigate through various pages with information about your monitored objects, such as your network status and monitoring results, for example, as well as access maps, reports, tickets and settings.



Enterprise Console Menu Tabs Bar

There is documentation available for the following tabs:

- Devices 3038
- Libraries 3045
- Sensors 3047
- Alarms 3049
- Maps 3051
- Reports 3053
- Logs 3055
- Tickets 3057
- Setup 3059
- Search Results 3061

Alarms Menu Tab

In the **Alarms** tab you can show the alarms of all active PRTG core servers. To do so, select **All PRTG Servers** from the server selection in the upper right corner.

The alarms list shows all sensors that are currently in a **Down**, **Down (Partial)**, **Down (Acknowledged)**, **Warning**, or **Unusual** status. Sensors in other states (for example, **Up**, **Paused**, or **Unknown**) do not appear here. This is useful for keeping track of all irregularities in your network.

Using the options **Error**, **Warning**, and **Unusual**, you can hide and show sensors in the respective status by removing and adding a check mark. When choosing **Error**, this includes sensors in the states **Down**, **Down (Partial)**, and **Down (Acknowledged)**.

Click **Show as Gauges** to show the sensors on the **Alarms** tab represented with gauges 166.

If the list has more than one entry, you can also sort the items by the contents of a certain column. To sort, simply click once or twice on the header of the column you want to sort by.

From this list view, you can select multiple items to apply the same action to them, for example, **Edit | Check Now**.

You can select multiple items by the following means (you can also combine them):

- Click and hold your left mouse key while pointing to the lines you want to select
- Hold the Ctrl key while clicking to toggle the selection status of a single line
- Click a line and hold the Shift key while clicking another line to select all lines in between.

Acknowledge Alarm

An acknowledged alarm shows up in the alarms list as "acknowledged" (see **Sensor States** 163) and will not trigger 2791 any more notifications 2829.

If the alarm condition clears, the sensor usually returns to an **Up** status immediately with the next sensor scan.

To acknowledge an alarm, right-click a sensor entry and choose **Acknowledge Alarm...** from the context menu, enter a message and click the **OK** button. The message will appear in the last message value of the sensor. You can choose between: **Acknowledge Indefinitely...**, acknowledge **For 5 Minutes...**, **For 15 Minutes...**, **For 1 Hour...**, **For 3 Hours...**, **For 1 Day...**, or **Until...**.

If you choose **Until...** a dialog box appears:

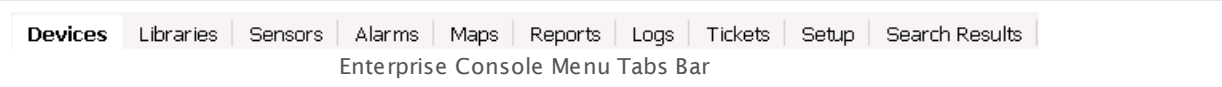
ACKNOWLEDGE ALARM UNTIL

Selected Objects	Shows the sensor(s) that you want to acknowledge the alarm for. You can acknowledge alarms for more than one sensor using multi-edit 2814.
Message	Enter a text, for example, the reason why you acknowledge the alarm. Please enter a string or leave the field empty.
Until	Enter the date when the acknowledge status will end. Use the date time picker to enter the date and time. If the alarm condition still persists after the specified date, the sensor will show a **Down** status again.

Only users 2975 with write access rights may acknowledge alarms. You can give read-only users the right to acknowledge alarms, too. See section **User Accounts Settings** 2976, section **Account Control**.

9.3.5 Maps

The Enterprise Console has a tab-like interface. Using the tabs you can navigate through various pages with information about your monitored objects, such as your network status and monitoring results, for example, as well as access maps, reports, tickets and settings.



Enterprise Console Menu Tabs Bar

There is documentation available for the following tabs:

- Devices 3038
- Libraries 3045
- Sensors 3047
- Alarms 3049
- Maps 3051
- Reports 3053
- Logs 3055
- Tickets 3057
- Setup 3059
- Search Results 3061

Maps Menu Tab

The page is split into two parts. On the left hand side you see all available maps from one or several servers, on the right hand side the details of the selected map.

- Click a map's name to display it. In the tabs above the map, select from **View Map**, Map Designer 2893, Settings 2902, Get HTML 2905, Comments 2906, and History 2906. Each of these tabs loads the respective functionality of the Ajax Web Interface 136. Remember to click the **Save** button to apply your settings.
- Double-click a map's name to open the map in the configured external web browser. You can edit it using the Map Designer 2893, or add new maps to this PRTG server.
- Right-click a map's name to open a context menu 3079. The following options are available: **Add**, **Edit**, **Delete**, **Clone**, **Send link by email**, and **Open in Web Browser**.
- Use the **Add Map** button to create a new map and the button for object history 241 to view all changes to maps.

For more details, see section Maps 2885.

Maps Menu Tab—Add Map

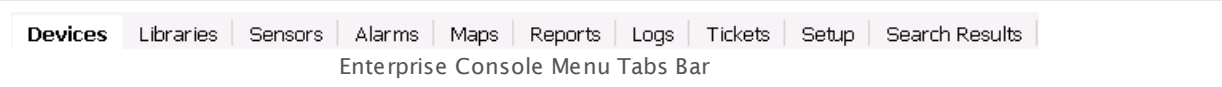
Click the **Add Map** button to add a new map to a PRTG server.

Depending on the current setting shown in the server selection 3035 bar in the upper right corner, an (embedded) window will open (if one specific server is selected), or you will see a selection window that asks you to choose the core server you want to add the new item to. Choose an installation to start.

For details about adding a map, see section **Maps Step By Step** 2890.

9.3.6 Reports

The Enterprise Console has a tab-like interface. Using the tabs you can navigate through various pages with information about your monitored objects, such as your network status and monitoring results, for example, as well as access maps, reports, tickets and settings.



Enterprise Console Menu Tabs Bar

There is documentation available for the following tabs:

- Devices 3038
- Libraries 3045
- Sensors 3047
- Alarms 3049
- Maps 3051
- Reports 3053
- Logs 3055
- Tickets 3057
- Setup 3059
- Search Results 3061

Reports Menu Tab

On the **Reports** tab you see all available reports from one or several servers in one list.

If the list has more than one entry, you can also sort the items by the contents of a certain column. To sort, simply click once or twice on the header of the column you want to sort by.

Choose one report and double click its name to open its details. The page will split into two parts. On the left hand side you see all available reports from one or several servers, on the right hand side the options for the currently selected report.

- Click a report's name in the list on the left to display its options. In the tabs above the report, select from Run Now 2870, Stored Reports 2872, Settings 2873, Select Sensors Manually 2882, Sensors Selected by Tag 2884, and Comments 2884. Each of these tabs loads the respective functionality of the Ajax web interface 136. Remember to click the **Save** button to apply your settings.
- Right-click a report's name to open its context menu 3079. The following options are available: **Add**, **Run Now**, **Edit**, **Delete**, **Clone**, **Send link by email**, and **Open in Web Browser**.
- Use the **Add Report** button to create a new report and the button for object history 241 to view all changes to reports.

For details, see section Reports 2862.

Reports Menu Tab—Add Report

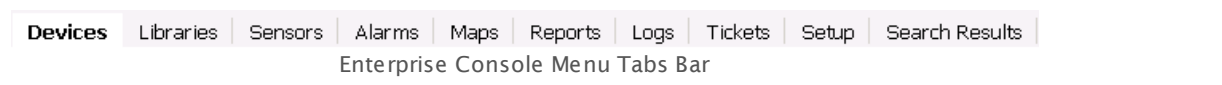
Click the **Add Report** button to add a new report to a PRTG server.

Depending on the current setting shown in the server selection 3035 bar in the upper right corner, an (embedded) window will open (if one specific server is selected), or you will see a selection window that asks you to choose the core server you want to add the new item to. Choose an installation to start.

For details about adding a report, see section **Reports Step By Step** 2866.

9.3.7 Logs

The Enterprise Console has a tab-like interface. Using the tabs you can navigate through various pages with information about your monitored objects, such as your network status and monitoring results, for example, as well as access maps, reports, tickets and settings.



Enterprise Console Menu Tabs Bar

There is documentation available for the following tabs:

- Devices 3038
- Libraries 3045
- Sensors 3047
- Alarms 3049
- Maps 3051
- Reports 3053
- Logs 3055
- Tickets 3057
- Setup 3059
- Search Results 3061

Logs show all past activities and events of your PRTG monitoring setup. This is useful for researching past user activities, system events, and, for example, to check whether messages were sent. In a typical setup, a huge amount of log data is produced. Because the activity of every single object is recorded, you can use this information to check if your setup works exactly as desired.

There are two options to call the logs list: Either you click the **Log** tab while you view an object's details on the Devices 3042 menu tab, or you choose the **Logs** entry from the menu tabs bar.

Logs Menu Tab

Click the **Logs** entry in the menu tabs bar to show a list of all log entries of a PRTG core server.

You can either view the entries of one or all servers. If you have configured more than one PRTG core server and you want to view entries from all servers in your PRTG Servers 3062 setup, simply select **All PRTG Servers** from the server selection in the upper right corner.

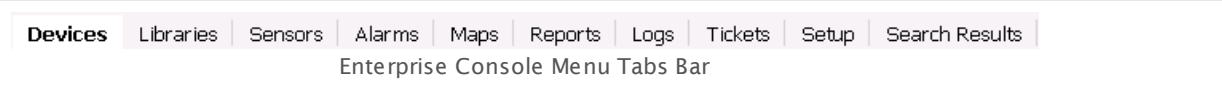
You can enable a filter to only show log entries of a certain event from the categories **Status Changes**, **System Events**, and **Object History**. Choose a category from the **Show** menu. The second drop down menu shows all possible event types for the selected category. Select an entry to only show events of the respective event type. Choose a sensor status 163 for status changes, **Probe Related**, **Auto Discovery**, **Notifications**, or **Status Messages** for system events, or a system object for object history 198.

You can also define the time span for which you want to show logs. Use the date time picker to enter the date and time.

The list can show up to one hundred entries at a time. Use the arrow symbols above the list to show other items. You can jump to the beginning of the list, or browse through it hundred by hundred. If the list has more than one entry, you can also sort the items by the contents of a certain column. To sort, simply click the header of the column you want to sort by once or twice.

9.3.8 Tickets

The Enterprise Console has a tab-like interface. Using the tabs you can navigate through various pages with information about your monitored objects, such as your network status and monitoring results, for example, as well as access maps, reports, tickets and settings.



Enterprise Console Menu Tabs Bar

There is documentation available for the following tabs:

- Devices 3038
- Libraries 3045
- Sensors 3047
- Alarms 3049
- Maps 3051
- Reports 3053
- Logs 3055
- Tickets 3057
- Setup 3059
- Search Results 3061

Tickets Menu Tab

For technical reasons, this function is available for one server at a time only. If you have configured more than one PRTG core server, choose one server from the server list in the upper right corner.

On the **Tickets** tab you can view all tickets on the currently selected PRTG core server.

You can only display tickets from one server at the same time, not from all PRTG servers.

In the header bar of the tickets list, you can choose several filters to find and display certain tickets: by status, type, concerned user or user group, related monitoring objects, and last edit. Click the X symbol to undo the date selection.

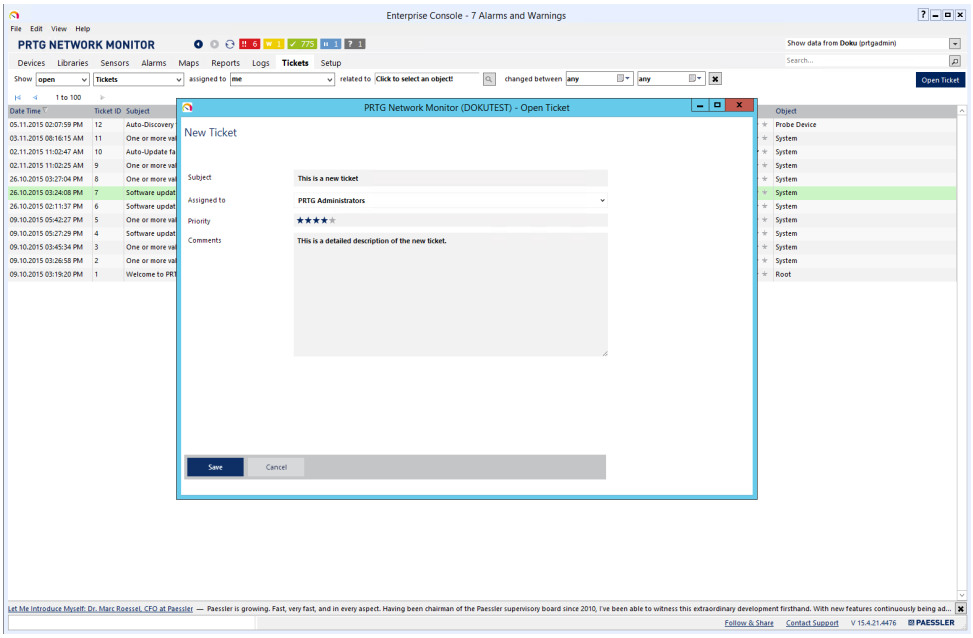
Double-click an entry in the tickets list to open a ticket in a new window and to conduct ticket related actions (edit, assign, resolve, close, or reopen). You can also multi-edit tickets via the context menu: mark several tickets by holding Ctrl or Shift and clicking on the corresponding tickets. Right-click a ticket to open the context menu.

The following actions are available: **Open Ticket**, **Edit Ticket**, **Assign Ticket**, **Resolve Ticket**, **Reopen Ticket**, **Close Ticket**, **Priority/Favorite**, **Open in Web Browser**.

The list can show up to one hundred entries at a time. Use the arrow symbols above the list to show other items. You can jump to the beginning of the list, or browse through it hundred by hundred. If the list has more than one entry, you can also sort the items by the contents of a certain column. To sort, simply click the header of the column you want to sort by once or twice.

Tickets Menu Tab—Open Ticket

To open a new ticket, click **Open Ticket** in the upper right corner or in the context menu. Select a related object, click **Continue**, and provide **Subject**, **Assigned to**, **Priority**, and **Comments**. Once finished, click **Save** to create the ticket.

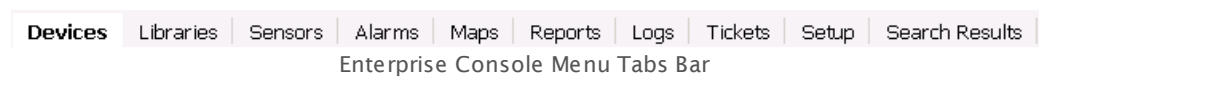


Open Ticket Dialog in PRTG Enterprise Console

For details about working with the PRTG ticket system, see section Tickets 200 for the PRTG web interface.

9.3.9 Setup

The Enterprise Console has a tab-like interface. Using the tabs you can navigate through various pages with information about your monitored objects, such as your network status and monitoring results, for example, as well as access maps, reports, tickets and settings.



Enterprise Console Menu Tabs Bar

There is documentation available for the following tabs:

- Devices 3038
- Libraries 3045
- Sensors 3047
- Alarms 3049
- Maps 3051
- Reports 3053
- Logs 3055
- Tickets 3057
- Setup 3059
- Search Results 3061

Setup Menu Tab

For technical reasons, this function is available for one server at a time only. If you have configured more than one PRTG core server, choose one server from the server list in the upper right corner.

On the **Setup** tab you can access all options available in the Setup 2907 menu of the Ajax web interface. You can collapse and expand the sections by clicking the – or + symbol.

For more information, please refer to the respective section in the documentation for the PRTG web interface.

Account Settings:

- My Account 2909
- Notifications 2916
- Notification Contacts 2934
- Schedules 2938

System Administration:

- User Interface 2943

- Monitoring 2955
- Notification Delivery 2961
- Core & Probes 2967
- Administrative Tools 2987
- Cluster 2992 (available in a cluster 116 setup only)

User Accounts:

- You see a list of configured user accounts. Select one to change settings. For details, please see User Accounts 2975 section.

User Groups:

- You see a list of configured user groups. Select one to change settings. For details, please see User Groups 2982 section.

PRTG Status:

- System Status 2994
- Cluster Status 3010 (available in a cluster 116 setup only)
- Licensing Status and Settings 3012
- Auto Update 3005

Optional Downloads and Add-Ons:

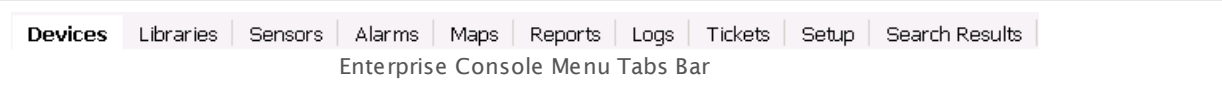
- Client App for Windows (Enterprise Console) 3018
- Client Apps for Mobile Devices 3018
- Remote Probe Installer 3018

Support:

- Contact Support 3022

9.3.10 Search Results

The Enterprise Console has a tab-like interface. Using the tabs you can navigate through various pages with information about your monitored objects, such as your network status and monitoring results, for example, as well as access maps, reports, tickets and settings.



Enterprise Console Menu Tabs Bar

There is documentation available for the following tabs:

- Devices 3038
- Libraries 3045
- Sensors 3047
- Alarms 3049
- Maps 3051
- Reports 3053
- Logs 3055
- Tickets 3057
- Setup 3059
- Search Results 3061

Search Results Menu Tab

For technical reasons, this function is available for one server at a time only. If you have configured more than one PRTG core server, choose one server from the server list in the upper right corner.

The **Search Results** tab is only visible if you do a search using the search box in the upper right corner. For your search, the Enterprise Console shows all matching objects on one PRTG core server. Click a monitoring object in the results to show it in the Enterprise Console's Devices 3038 tab.

Other objects, for example, manual sections, load in an external browser window.

When you click one of these items, a new window or tab of the external browser configured in the Enterprise Console's Options 3069 will open. PRTG automatically logs in and redirects you to the respective web page. If your browser displays a certificate warning, please find more information in section SSL Certificate Warning 142.

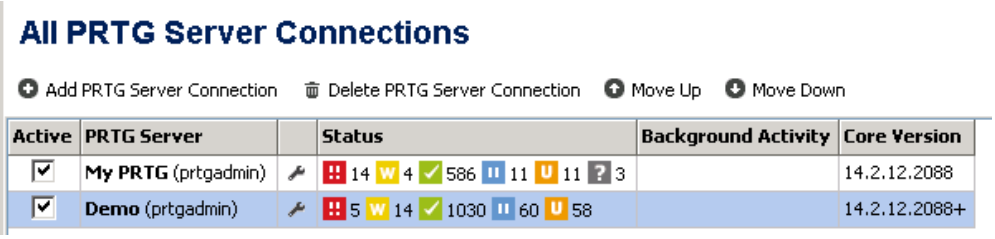
9.4 PRTG Servers

The Enterprise Console connects to the web server API running on every PRTG core server installation. It supports saving the configuration for a connection to one or more PRTG core servers. In a full PRTG installation, there is already a connection predefined.

For a successful connection, the program versions of Enterprise Console and PRTG core server have to match. When connecting to several servers, make sure they all run on the same software version. At least the third number of the whole version number has to be equal. For example, EC version 17.2.**31**.1917 can connect to server version 17.2.**31**.2018.

PRTG Servers List

From the main menu, select **File | Manage PRTG Server Connections** to view a list of all servers configured for the currently logged in Windows user account. You can also access this list by clicking the **PRTG Server Connections** entry above the device tree.



PRTG Servers List in the Enterprise Console

The list shows the server or display name, as well as login information used. In the **Status** column you see an overall sensor status for this server connection. You can also see if there is any **Background Activity** on the respective server (for example, a running Auto-Discovery 249), which can potentially affect performance and response times.

In the list, set a check mark for every PRTG server you want to poll with every update interval. If a server is not reachable, the Enterprise Console deactivates it automatically after several unsuccessful connection attempts. When opening the Enterprise Console, it automatically re-establishes the connection to all active servers.

Add or Edit a PRTG Server Connection

- Click **Add PRTG Server Connection** in the header bar above the server list to add a new server connection configuration.
- Click **Delete PRTG Server Connection** to remove an entry from the list.
- Click **Move Up** or **Move Down** to change the order of the servers on the Devices 3038 tab.

There is also a context menu 3079 available for each server connection with the following options.

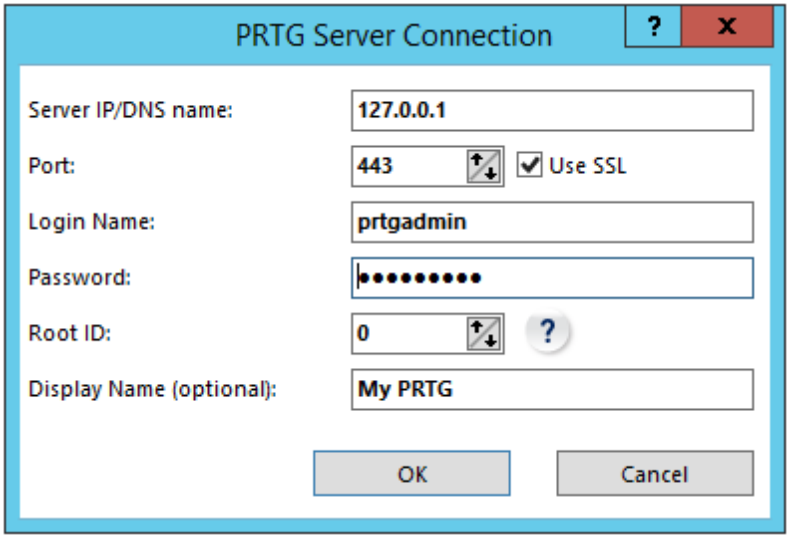
- Click **Deactivate PRTG Server Connection** to remove the server from the Devices 3038 tab but keep the server connection settings
- **Add** a server.

- Open and edit the **Settings** of the server.
- **Delete** the server.
- Open the server in the Ajax web interface (**Open in Web Browser**),
- **Move Up** and **Move Down** to change its position on the Devices 3038 tab.

To change the settings of an existing server in the list, open its context menu with right-click and click **Settings** or click the respective wrench symbol in the table. You can alternatively use the context menu of a server on the Devices 3038 tab. There you can choose between **Edit PRTG Server Connection** to open the edit dialog, **Deactivate PRTG Server Connection** to not show this server's monitoring data anymore (you can later reactivate it in the servers list 3062), or view Dependencies 126.

When adding or editing, a dialog box appears to enter connection information.

Connection settings are stored for each Windows user individually in the registry under the following node: HKEY_CURRENT_USER\Software\Paessler\PRTG Network Monitor\WinGUI



PRTG Server Connection Settings in Enterprise Console

Server IP/DNS name

- Enter the IP address or DNS name of the PRTG server the Enterprise Console connects to.
- This is the same address or name as defined in the web server settings for the core server. For detailed information please see PRTG Administration Tool 3136 (**Web Server**) section. Make sure the values match.
- Make sure the server is reachable (especially when using Network Address Translation (NAT)) and no firewall settings block the connection.

Port

- Enter the port on which the PRTG server runs.

- This is the same port as defined in the web server settings for the core server. For detailed information please see **PRTG Administration Tool** 3136 (**Web Server**) section. Make sure the values match.
- Make sure the server is reachable (especially when using Network Address Translation (NAT)) and no firewall settings block the connection.

Login Name

- Enter the login name that you use to login to the web server.
- This can be the administrator login or the login of another PRTG user.
- In a new installation, the login name is **prtgadmin** by default.
- For detailed information about user accounts, please see **System Administration—User Accounts** 2975 section.

Password

- Enter the password for the login name entered above.
- In a new installation, the password is **prtgadmin** by default.

Root ID

- Enter the ID of the object that is the root of the device tree 118.
- Default value is **0**, which is the **Root** group of your configuration.
- If you enter an other object's ID here, the device tree will start at this object, only showing all other objects below in the hierarchy.
- This is useful to only view a part of the device tree, which might load much faster.
- You can create several connections that only differ in the **Root ID** value to quickly switch between different views within your configuration, choosing different PRTG core server connections in the Enterprise Console's **Devices** 3038 tab.

Display Name (optional)

- Optionally enter a name that the EC displays in the **PRTG Server Connections** list.
- If you leave this field blank, the Enterprise Console displays the **Server IP/DNS name** setting there.

Click the **OK** button to save your settings or **Cancel** to discard them.

9.5 Options

From the Windows menu 3071 of the Enterprise Console, select **File | Options...** to open the options dialog.

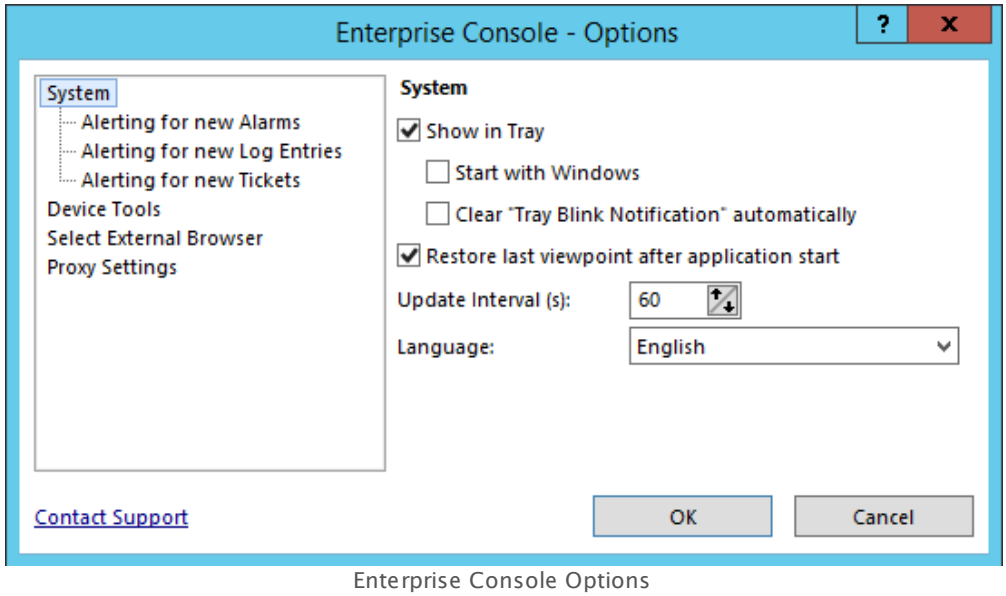
You can choose from these options on the left hand side:

- System 3065
- System—Alerting 3067
- Device Tools 3067
- Select External Browser 3069
- Proxy Settings 3070
- Contact Support 3022

System

From the Windows menu 3071 of the Enterprise Console, select **File | Options...** to open the settings dialog. Please select a setting on the left and change the respective values on the right side. Click the **OK** button to save your settings.

Change general system settings for the Enterprise Console.



Enterprise Console Options

ENTERPRISE CONSOLE – OPTIONS: SYSTEM

Show in Tray	By default this setting is enabled. With this setting enabled, a PRTG icon appears in the Windows tray 3031. When you point your mouse to it, it will show information with the most important status information about your monitoring. With a right-click you can access a menu with access to the most important functions. To use any alerting functionalities (see **System—Alerting** 3067 section), you must enable this option. If the tray icon is not shown, no alerting from the Enterprise Console is available.
Start with Windows	This setting is only available to change only if you enable the tray option above. By default this setting is enabled. With this setting enabled, the Enterprise Console will start up automatically when Windows starts.
Clear "Tray Blink Notification" automatically	This setting is only available to change only if you enable the tray option above. Whenever there are new entries in the **Alarms** 3049 list, the tray icon will start blinking. If you enable this option, the tray icon will stop blinking automatically as soon as there are no more alarms. With this option disabled, the icon will keep blinking, even if all alarms are cleared meanwhile.
Restore last viewpoint after application start	If this option is enabled, the Enterprise Console saves information about the currently shown view (for example, sensor details, a certain graph, or a map 2885). It is written to the registry 3070 when you close or exit the program. When you open the Enterprise Console again, it will try to restore the same view. Only if the object is not available any more (due to changes on the server, or due to unavailability of a server), the default view loads.
Update Interval (Sec.)	Define the number of seconds that the Enterprise Console waits before the screen refreshes. Please enter an integer value. Default value is **60** seconds. You can use the up and down arrows to go one second up or down.
Language	Choose the language for the Enterprise Console from the drop down menu. Default is **English**. Depending on your installation, you can choose other languages here. This setting only influences the language of the Enterprise Console.

System—Alerting

From the Windows menu 3071 of the Enterprise Console, select **File | Options...** to open the settings dialog. Please select a setting on the left and change the respective values on the right side. Click the **OK** button to save your settings.

You can define what the Enterprise Console will do in case of new **Alarms**, **Log Entries**, or **Tickets**. The settings are the same for all of these three cases, but you can individually define them for each case. On the left side, select either **Alerting for new Alarms**, **Alerting for new Log Entries**, or **Alerting for new Tickets** and define the settings as follows.

All alerting options only take effect if you enable the **Show in Tray** option in the system 3065 settings above. If the tray icon is disabled, there will be no alerting from the Enterprise Console.

ENTERPRISE CONSOLE – OPTIONS: ALERTING FOR NEW ALARMS

Blink Tray Icon	The tray icon will blink if there are new items to be alerted for. You can additionally set the **Clear Tray Blink Notification automatically** option in the system 3065 settings above.
Balloon Info in Tray	Show a balloon info next to the PRTG tray icon if there are new items to be alerted for.
Popup Message	Show a popup message window if there are new items to be alerted for. The popup window will be always on top until it is closed.
Play Sound	Play an audible notification if there are new items to be alerted for. There is a default sound defined. To change it, please click the folder icon and select any standard WAV file from your hard disk drive. PRTG already comes with a small set of sounds you can choose from. The sound file is only played on the computer running the Enterprise Console.
Open Enterprise Console	Open the Enterprise Console if there are new items to be alerted for.

Device Tools

From the Windows menu 3071 of the Enterprise Console, select **File | Options...** to open the settings dialog. Please select a setting on the left and change the respective values on the right side. Click the **OK** button to save your settings.

In the **Device Tools** settings you can define commands that will be available in the **Windows Menu** [3071] and context menu [3079] of groups, devices, and sensors. A command to initiate a remote desktop connection is already predefined.

You may need to run the Enterprise Console as administrator to make the tool function work with your Windows version.

Click the **Add** button to add a new command, or choose an existing one from the list and click the **Edit** button to change the settings. Use the **Delete** button to remove an entry from the list.

ENTERPRISE CONSOLE – OPTIONS: EDIT TOOL

Name	Enter a custom name for your command. The command will show up with this name in context menus. Please enter a string.
Command	Enter the command you want to execute on the local machine. This can be, for example the name of a program or script, with or without path, according to your system's configuration.
Parameters	Enter the parameters with which you want to execute the command. You can use the placeholders (variables) from section **Parameters—Available Placeholders** [3068]. Other placeholders are not possible. During runtime, these placeholders are replaced by the respective values set for the monitoring object you select to execute this device tool. For example, the %id placeholder will be replaced by the ID of a group, a device, or a sensor, depending on which object you execute the command for.
Shortcut	Select a key shortcut for the command. Choose an **F**-key from the list or select **None** to not use a key.

Parameters—Available Placeholders

The following placeholders (variables) are available in the Enterprise Console.

PLACEHOLDER	AVAILABLE FOR GROUPS	AVAILABLE FOR DEVICES	AVAILABLE FOR SENSORS	WILL BE RESOLVED TO
%id	☺	☺	☺	The object's **ID** as shown in the page header on the object's details page
%name	☺	☺	☺	The object's **Name**
%host	⊘	☺	☺	The sensor's or device's **IP Address/DNS Name**
%message	⊘	⊘	☺	The sensor's **Last Message**
%value	⊘	⊘	☺	The sensor's **Last Result** value
%type	⊘	⊘	☺	The sensor's **Type**

If you use a placeholder in combination with an object it is not available for, it will simply not be resolved but the placeholder itself will be returned.

To see the output of all placeholders for different objects you can create a simple test tool that displays the output in a command line window. Just create a tool with the command **cmd** and the following content in the **Parameters** field:

```
/K echo.id: %id && echo.name: %name
      && echo.host: %host && echo.message: %message
      && echo.value: %value && echo.type: %type
```

Right-click an object in the device tree and run the tool from the **Tools** option in the menu (either Windows 3071 or context menu 3075).

Select External Browser

From the Windows menu 3071 of the Enterprise Console, select **File | Options...** to open the settings dialog. Please select a setting on the left and change the respective values on the right side. Click the **OK** button to save your settings.

With these settings you can define which browser the Enterprise Console will use when you select a command that requires to open an external browser window, for example, when you select **View | Open in Web Browser** from the Windows menu of the EC. You can only select browsers installed on the system running the Enterprise Console, other browser options are disabled.

By default, the system's default browser is opened. To change the Enterprise Console's behavior, choose between:

- **Use system default browser (**browser.exe**)**
- **Use IE (Version:** x**)**
  Only Microsoft Internet Explorer 11 is supported by the Ajax web interface! Please do not use it with Internet Explorer 10 or earlier! We recommend that you use Google Chrome 57 or later (recommended) or Mozilla Firefox 52 or later as external browser.
- **Use Firefox (Version:** x**)**
- **Use Chrome (Version:** x**)**
- **Use Safari (Version:** x**)**

Proxy Settings

From the Windows menu 3071 of the Enterprise Console, select **File | Options...** to open the settings dialog. Please select a setting on the left and change the respective values on the right side. Click the **OK** button to save your settings.

If the connection to the PRTG core servers requires a proxy connection, you can set it here.

ENTERPRISE CONSOLE – OPTIONS: PROXY SETTINGS

No Proxy	Use a direct connection to the servers.
Use System Settings	Use your Windows default settings, configured in Internet Explorer. To view these settings, open the Internet Explorer on your system and select **Tools	Internet Options** from the menu. Select the **Connections** tab and click the **LAN settings** button.
Manual Proxy Configuration	Manually enter a proxy configuration. Enter the IP address or DNS name of the proxy, a port number, as well as username and password (if required by the proxy). Only basic authentication is available!

Settings Storage

For each individual Windows user account, the settings of the Enterprise Console are stored in the Windows registry.

For details, see section **Data Storage** 3226.

9.6 Windows Menu Structure

The Windows menu of the Enterprise Console has four main menu items:

- File 3071
- Edit 3072
- View 3076
- Help 3077

File

The **File** menu offers system related options for the Enterprise Console. The particular close and exit options depend on the enabling status of the tray option.

FILE	
Manage PRTG Server Connections	Show a list of all configured PRTG core server connections. For detailed instructions, see section **PRTG Servers** 3062 section.
Options...	Open the **Options** 3065 dialog to set EC system options and to configure one or more PRTG core server connections.
Close or Exit	This menu item appears as either **Close** or **Exit**, depending on whether the tray icon is enabled or disabled in the **Options** 3065 settings. ▪ Use **Close** to close the Enterprise Console window. Alerting is still available via the tray icon then. You can also double-click the tray icon to re-open the Enterprise Console. ▪ **Exit** shuts down the Enterprise Console completely. This option is only available if the tray icon is not running. Shortcut: Alt+X
Close and Exit	This menu item is only available if the **Show in Tray** option is enabled in the **Options** 3065 settings. It will completely shut down the Enterprise Console and tray icon, so no tray alerts are shown any more. Shortcut: Ctrl+Alt+X

Edit

The content of the **Edit** menu varies, depending on which menu tab [3037] you are and whether and which objects are selected within the **Devices** [3038], **Sensors** [3047], or **Alarms** [3049] tab.

Some of the options open the Ajax web interface when you select them.

When you click one of these items, a new window or tab of the external browser configured in the Enterprise Console's **Options** [3069] will open. PRTG automatically logs in and redirects you to the respective web page. If your browser displays a certificate warning, please find more information in section **SSL Certificate Warning** [142].

EDIT

Check Now	Perform an immediate scan for all selected objects (use the Ctrl key to select multiple objects). This option polls all selected devices and queries new data for all sensors on them. If you choose this option for a probe or a group, you query data for all sensors in the object hierarchy [118] underneath. Shortcut: Ctrl+K
Details	Open the overview tab for the selected object (probe, group, device, or sensor).
Edit	Access the pages for editing **Settings...** [188], **Notifications** [188], **Access Rights...** [129], and **Management** [188] (not for sensors) of the selected object. In addition, you can **Rename...** this object. Point on it to see available options.
Dependencies	This option is only available if you select a server (the **Root** group), a probe, or group. This function shows an overview of the dependencies [126] configured for the selected object. If you select a dependencies option, the Enterprise Console opens the respective dependencies overview in a new window. For details, see section **Show Dependencies** [2822].
Add Group...	This option is only available if you select a probe or group (not the **Root** group). This option opens an assistant in a new window which guides you through adding a new group to the selected probe or group. For detailed instructions, see section **Add a Group** [268].
Add Auto-Discovery Group...	This option is only available if you select a probe or group (not the **Root** group). This option opens an assistant in a new window which guides you through adding such a group.

EDIT

For detailed instruction, see section **Auto-Discovery** 249.

Add Device...	This option is only available if you select a probe or group (not the **Root** group). This option opens an assistant in a new window which guides you through adding a new device to the selected probe or group. For detailed instructions, see section **Add a Device** 275.
Add Sensor...	This option is only available if you select a device. This option opens an assistant in a new window which guides you through adding a new sensor to the selected device. For detailed instructions, see section **Add a Sensor** 288.
Auto-Discovery	This option is only available if you select a device. Hover over it to see available options. You can choose between: ▪ **Run Auto-Discovery**: This option starts an automatic search and adds new sensors to the selected device. The search is running in background. You will see new sensors after a few minutes automatically. If you have set the option **Manual (no auto-discovery)** in the device settings section 362 **Sensor Management** and start the auto-discovery, PRTG will not run it. Please note that the Ajax web interface 222 behaves differently in this case. ▪ **Run Auto-Discovery with Template**: With this option you can run an auto-discovery with a pre-defined device template. For more information, see section **Auto-Discovery** 250 (**Run Auto-Discovery Now**).
Create Device Template...	This option is only available if you select a device. This option opens an assistant in a new window which guides you through creating a device template. This template is then available for auto-discovery 249. For detailed instructions, please see **Create Device Template** 2818.
Sort Alphabetically	This option is only available if you select a probe, a single group, or a device. This will sort direct children of the selected node such as groups, devices, or sensors in alphabetical order. The ordering is stored in the monitoring configuration so you cannot revoke it!
Acknowledge Alarm...	This option is only available if you select a sensor in a **Down** or **Down (Partial)** status 163. Point on it to see available options.

EDIT

For details on how to acknowledge an alarm, see section Alarms 3050.

Delete	Delete the selected object(s). You will be asked for confirmation before anything is actually deleted.
Clone...	This option is only available if you select a single group, device, or sensor. This options opens an assistant in a new window which guides you through cloning the selected object. For detailed instructions, see section Clone Object 2812.
Move	Move the selected object(s) of the device tree (use the Ctrl or Shift key to select multiple objects). Hover over it to see available options. Choose between **Top**, **Up**, **Down**, and **Bottom** to move the object(s) to the top or bottom of the mother node, or one entry up or down. You can also move the selected group or device to another group with **To Other Group...** This option opens an assistant in a new window to guide you through the movement. For details about allowed movements, see section Devices 3044.
Pause	Pause and resume monitoring for the selected objects from the device tree (use the Ctrl key to select multiple objects). Hover over it to see available options. Choose between: ▪ **Indefinitely** ▪ **Resume** ▪ **For 5 Minutes** ▪ **For 15 Minutes** ▪ **For 1 Hour** ▪ **For 3 Hours** ▪ **For 1 Day** ▪ **Pause Until...**: This option will open an assistant in a new window where you can enter a message and a date. Use the date time picker to enter the date and time. PRTG will resume monitoring after this date.

EDIT

	You can also set up a **One-time maintenance window**: Enter a message and start and end date of the maintenance in the appearing window. Use the date time picker to enter the date and time.
Simulate Error Status	This option is only available if you select a sensor. Set the selected sensor to a simulated error status. As for the pause status, **Resume** will appear in the context menu if a the selected sensor is already in a simulated error state. **Simulate error status** does not work for sensors that run on a PRTG Mini Probe.
Priority/Favorite	Set the priority for the selected object. You can also add devices and sensors to favorites. For details, see section **Priority and Favorites** 211.
Historic Data	Open the historic data tab of the selected object. Hover over it to see available options. You can choose between **Last 2 days...**, **Last 30 days...**, and **Last 365 days...**, or when selected one sensor **Live Data...** and **View Historic Data...**. You can also create a report. For detailed instructions, please see **Historic Data Reports** 176 **(Menu)**. When you select one or more sensors (hold the Ctrl or Shift key to select multiple items), you can open the **Compare Sensors** 172 dialog. The graphs of all chosen sensors appear in the comparison dialog automatically. You can add additional sensors in the comparison dialog. For sensors, you can open the **Similar Sensors Overview** 180.
Device Tools	Call a tool command. All placeholders (variables) configured in a tool command will be resolved for the currently selected object. Hover over it to see all available tools configured in your **Options** 3067 settings (**Device Tools**). By default, a **Remote Desktop** tool is pre-configured that tries to initiate a remote desktop connection to the IP address or DNS name of the selected object. This will usually work for devices.

EDIT

	You can also add a device tool directly to the selected object: **Add Device Tool...** will open **Options—Device Tools** 3067. For devices, additional options are available. They allow you to connect to the **Service URL** value defined in the device's settings 3043, or open the **IP address/DNS name** of the device via the protocols HTTP, HTTPS, and FTP. For each of these functions, your system's default programs will be used. Usually, this is your browser. You can also install a remote probe on a device via **Remote Probe Quick Setup** 3199. You may need to run the Enterprise Console as administrator to make the tool function work with your Windows version.
Find Duplicates	This option is only available if you select a device. Search in your PRTG configuration for devices with the same IP address or DNS name as the selected device. A new window with the results will appear, either showing existing duplicates or a message indicating that there are no duplicates.
Drag & Drop Sorting	Enable this option to sort all objects in the device tree via drag and drop. By default, this option is disabled to avoid accidental moves of objects. For details, see section **Devices** 3044.
Send Link by Email	Send the link to the selected object by email. This option opens a new email using your system's standard email client. It contains a direct link to the details page of the selected object.
Open Ticket	Open a ticket that refers to the currently selected object. For details, please see section **Tickets** 3057.

View

The **View** menu provides settings related to what the Enterprise Console shows.

VIEW

Refresh	Query data for the current screen from the PRTG core server immediately, just as the automatic refresh does. You can configure the auto-refresh in the **Options** 3065 settings. Shortcut: F5

VIEW

Large Single Graph	Change the view in **Devices** 3038 menu tabs to large single graphs. This option displays live graphs and graphs for three other time spans in different tabs. Shortcut: Ctrl+L
Small Multiple Graphs	Change the view in **Devices** 3038 menu tab to multiple small graphs. This option displays live graphs and graphs for three other time spans in one tab.
Show Geo Maps	Choose if you want to show **Geo Maps** 2824 in the Enterprise Console. Shortcut: Ctrl+G
Show News Feed	Choose if you want to show the news feed in the Enterprise Console. Shortcut: Ctrl+N
Next Viewpoint	Go forward to the next viewpoint (only available if you went back to a previous viewpoint before). This is similar to a browser's function to go forth in history. Shortcut: Alt+Right
Previous Viewpoint	Go backwards to the previous viewpoint. This is similar to a browser's function to go back in history. Shortcut: Alt+Left
Open in Web Browser	Open the currently selected object in the Ajax web interface. This option is not available if multiple objects are selected. You can set the default browser in the **Options** 3069 settings.

Help

This menu provides links to help and information.

HELP

Help Center	Open the **Help and Support Center** in the Ajax web interface.

HELP

HTML Manual Enterprise Console...	Open the **Enterprise Console** 3028 sections of this manual in the Ajax web interface.
PRTG Network Monitor Homepage...	Open https://www.paessler.com/prtg in your browser for overall information about PRTG.
Follow & Share	Open PRTG's social network contact information in the Ajax web interface.
Contact Support	Open the **Contact Support** 3022 dialog box to leave feedback or to ask for support by sending a support bundle.
About...	Open an information window about the Enterprise Console application with version number and copyright information.

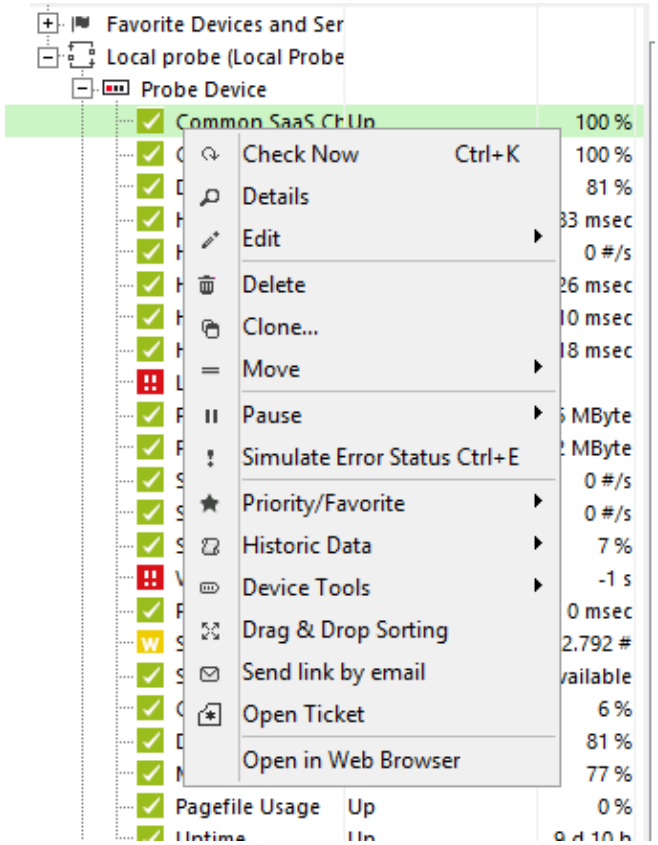
See Also

- **Shortcuts Overview** 3080

9.7 Context Menus

For every object in the Enterprise Console, there are context menus available which appear when you right-click an object in the device tree. These context menus vary depending on the selected object and always contain a sub-set of the options available in the Windows menu.

For detailed explanations, see section Windows Menu Structure 3071.



Context Menu of a Device in the Enterprise Console

9.8 Shortcuts Overview

The following shortcut keys are available in the Enterprise Console:

- **Alt+X**: File | Close or Exit
  With the **Show in Tray** option enabled in the **Options** 3065 settings, this is **Close**, otherwise **Exit**.
- **Ctrl+Alt+X**: File | Close and Exit
  This menu item is only shown if the **Show in Tray** option is enabled in the **Options** 3065 settings.
- **Alt+Right**: Next Viewpoint
- **Alt+Left**: Previous Viewpoint
- **Ctrl+K**: Edit | Check Now
- **Ctrl+P**: Edit | Pause | Indefinitely
- **Ctrl+R**: Edit | Pause | Resume
- **Ctrl+E**: Edit | Simulate Error Status
- **Ctrl+L**: View | Large Single Graph
- **Ctrl+S**: View | Small Multi Graphs
- **Ctrl+G**: View | Show Geo Maps
- **Ctrl+N**: View | Show News Feed
- **F5**: View | Refresh
- **F6**: [Context Menu] | Tools | Custom tool command, if available
- **F7**: [Context Menu] | Tools | Custom tool command, if available
- **F8**: [Context Menu] | Tools | Custom tool command, if available
- **F9**: [Context Menu] | Tools | Custom tool command (default: **Remote Desktop**)
- **F10**: [Context Menu] | Tools | Custom tool command, if available
- **F11**: [Context Menu] | Tools | Custom tool command, if available
- **F12**: [Context Menu] | Tools | Custom tool command, if available

See Also

- **Windows Menu Structure** 3071

Part 10

PRTG Apps for Mobile Network Monitoring

10 PRTG Apps for Mobile Network Monitoring

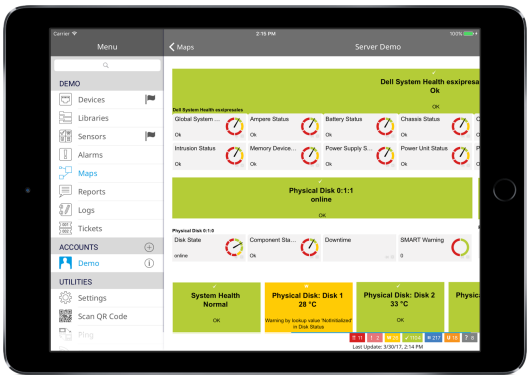
You can access your PRTG installation on your mobile devices with several PRTG apps. We provide apps for iOS devices, Android systems, and Windows Phone. You can download and use these apps for free. PRTG for iOS 3082, PRTG for Android 3082, and PRTG for Windows Phone 3083, and make it possible to monitor your network while on the go.

The basic requirements to use these free apps are a running PRTG core server which is accessible from the network your device is connected to (either directly or via a VPN connection) and a recent operating system version on your mobile device. For details about requirements, see below.

PRTG for iOS

PRTG for iOS is the iOS app for PRTG Network Monitor version 13 or later. You can use it on iPhone, iPad, and iPod touch with iOS version 8 or later. You can also use free push notifications 2923 with this app (required: PRTG for iOS 14.3.6 or later; PRTG 15.4.20 or later).

For more information and to download this app, see our website: **PRTG for iOS**.



Maps on iPad

PRTG for Android

PRTG for Android is the Android app for PRTG Network Monitor version 14 or later. Use it on your smartphone or tablet with Android version 4.0 or later, on a BlackBerry device or on a Kindle Fire. For full functionality, we recommend that you use at least Android 4.1. On your BlackBerry device you need version 10.3. You can also use free push notifications 2923 with the PRTG for Android app (required: PRTG for Android 14.3.2 or later; PRTG 15.4.20 or later).

For more information and to download this app, please see our website: **PRTG for Android**

You cannot deploy the app via BlackBerry Enterprise Service (BES).

Sensor List on PRTG for Android

PRTG for Windows Phone

PRTG for Windows Phone is the Windows Phone app for PRTG Network Monitor 13.3 or later. You can run it on Windows Phone 8.0 or later. You can also use free push notifications 2923 with the PRTG for Android app (required: PRTG for Windows Phone 15.1.1 or later; PRTG 15.4.20 or later).

For more information and in order to download this app, please see our website: **PRTG for Windows Phone**

PRTG for Windows Phone Menu

More

PRTG for iOS:

- https://www.paessler.com/apps/iosapp

PRTG for Android:

- https://www.paessler.com/apps/androidapp

PRTG for Windows Phone:

- https://www.paessler.com/apps/windowsphoneapp

Knowledge Base: Which features do the PRTG mobile apps support?

- https://kb.paessler.com/en/topic/60042

Knowledge Base: How can I use push notifications with PRTG?

- https://kb.paessler.com/en/topic/60892

Part 11

Sensor Technologies

11 Sensor Technologies

This section introduces different technologies that PRTG uses for monitoring to give you more background information. Please read more in the following sections.

Sensor Technologies—Topics

- Monitoring via SNMP 3087
- Monitoring via WMI 3092
- Monitoring via SSH 3095
- Monitoring Bandwidth via Packet Sniffing 3097
- Monitoring Bandwidth via Flows 3099
- Bandwidth Monitoring Comparison 3102
- Monitoring Quality of Service 3104
- Monitoring Email Round Trip 3109
- Monitoring Backups 3111
- Monitoring Virtual Environments 3112
- Monitoring Databases 3120
- Monitoring Syslogs and SNMP Traps 3125

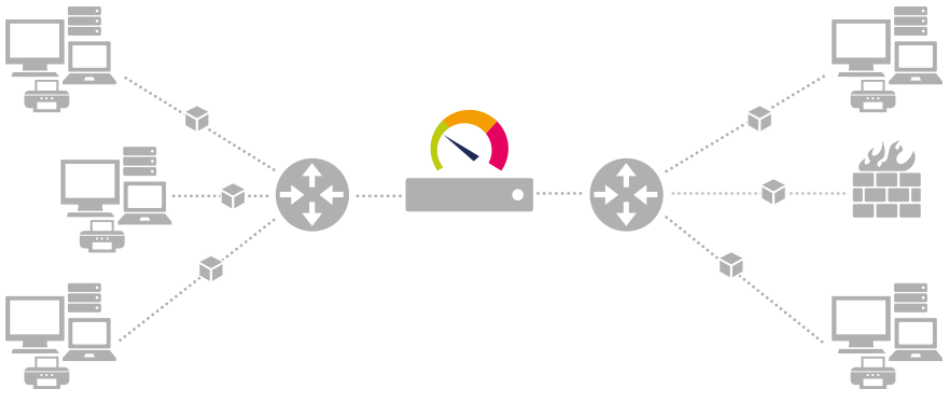
11.1 Monitoring via SNMP

Monitoring via Simple Network Management Protocol (SNMP) is the most basic method of gathering bandwidth and network usage data.

How SNMP Monitoring Works

SNMP is a set of standards for communication with devices in a TCP/IP network. SNMP monitoring is useful if you are responsible for servers and network devices such as hosts, routers, hubs, and switches. It enables you to keep an eye on network and bandwidth usage, and monitor important issues such as uptime and traffic levels.

You can use SNMP to monitor the bandwidth usage of routers and switches on a port-by-port basis, as well as device readings such as memory and CPU load. The target devices must support SNMP. Most devices with enabled SNMP require the same configuration like SNMP version and community string. To find out how to set up SNMP on a specific device, search in the internet for your device name or model and SNMP configuration. You will likely get plenty of information on how to configure SNMP.



Network Monitoring via SNMP

Click here to enlarge: http://media.paessler.com/prtg-screenshots/network-monitoring-via-snmp.png

When you use a sensor with this technology, PRTG sends small data packets to devices, for example, querying routers, switches, and servers for the traffic counters of each port. These queries trigger reply packets from the device. Compared to PRTG's other bandwidth monitoring technologies via flows, packet sniffing, or WMI, the SNMP option creates the least CPU and network load.

Reasons to Choose SNMP Monitoring

SNMP is the most commonly used method mainly because it is easy to set up and requires minimal bandwidth and CPU cycles. If your network devices support SNMP and/or if you want to monitor large networks with several hundred or thousands of sensors, we recommend that you start with SNMP.

Besides network usage monitoring, another well-known feature of SNMP is the ability to also watch other network parameters such as CPU load, disk usage, temperature, as well as monitoring many other readings, depending on the queried device.

SNMP Network Issues

To use Simple Network Management Protocol (SNMP) for monitoring purposes, it is imperative that UDP packets can travel from the machine running PRTG to the device you want to monitor and back. This is usually the case in LANs and intranets. For connections across the internet, to a Demilitarized Zone (DMZ), or for Wide Area Network (WAN) connections, some changes to the traversed firewalls may be necessary.

Keep in mind that SNMP V1 and V2c are not secure protocols so you should not use them across the internet or insecure data connections. Only SNMP version 3 supports encryption.

Understanding SNMP Sensors

To better understand and set up SNMP sensors, you may want to learn more about the principles of Object Identifiers (OID) and Management Information Base (MIB).

For more information about this topic, see this Knowledge Base article: How do SNMP, MIBs and OIDs work?

For an overview and details about all SNMP sensors, see section **List of Available Sensor Types** 387.

SNMP Versions

PRTG supports three versions of the SNMP protocol: Version 1, version 2c, and version 3.

SNMP Version 1

This is the oldest and most basic version of SNMP.

- Pro: Supported by most SNMP-compatible devices; simple to set up.
- Con: Limited security because it only uses a simple password (community string 3090) and sends data in clear text (unencrypted). Because of this, you should only use it inside LANs behind firewalls, but not in WANs. Version 1 only supports 32-bit counters which are not enough for high-load (gigabits/second) bandwidth monitoring.

SNMP Version 2c

This version adds 64-bit counters.

- Pro: Supports 64-bit counters to monitor bandwidth usage in networks with gigabits/second loads.
- Con: Limited security (same as with SNMP V1).

SNMP Version 3

This version adds authentication and encryption to SNMP.

- Pro: Offers user accounts and authentication for multiple users and optional data packet encryption, increasing available security; plus all advantages of Version 2c.
- Con: Difficult to configure and higher overhead for the probe, which will reduce the number of devices that you can monitor (see here 3089 for more information).

SNMP Traps

Various devices can send SNMP trap messages to notify you of system events.

- PRTG supports SNMP v1 and SNMP v2c traps.
- Destination for SNMP traps: IP address of the trap receiver, which is the IP of the PRTG probe system (server with either a local or remote probe running on it) to which you add the **SNMP Trap Receiver Sensor** 2143.

Which SNMP Version Should I Choose?

The SNMP version to choose depends on your environment, but as a guideline:

- If your network is publicly accessible, you may want to use SNMP v3, which has encryption and secure access. However security and encryption adds overhead, which results in less performance.
- If your network is isolated or well protected behind firewalls, the lower security of SNMP v1 or SNMP v2c may be sufficient.
- From the PRTG perspective, if you have a lot of devices to monitor, the SNMP v2c is preferable. It will allow you to monitor more devices on a shorter monitoring interval and supports 64-bit counters.

The most important thing is to set the same SNMP version in the PRTG settings (for example, on **Root** level) as you have configured in your target device. If you select an SNMP version that is not supported by the server or device you want to monitor, you receive an error message. Unfortunately, in most cases, these error messages do not explicitly point to the possibility that you use the incorrect SNMP version. These messages provide minimum information only, such as cannot connect or similar. Similar errors occur when community strings, usernames, or passwords do not match.

For basic requirements for SNMP monitoring, please see this Knowledge Base article: My SNMP sensors don't work. What can I do?

SNMP Overload and Limitations of the SNMP System

SNMP V1 and V2 scale directly with the performance of the hardware and the speed of the network. In our labs we are able to monitor 30,000 SNMP V1 sensors at a 60 second interval with one PRTG server (core and local probe) plus two remote probes with 10,000 sensors each.

However, SNMP V3 has performance limitations due to the SSL encryption. The main limiting factor is CPU power (as well as the other general limits for PRTG). Because of this limitation, you can monitor only a limited number of sensors per second using SNMP V3. Currently, PRTG is able to handle about 40 requests per second and computer core, depending on your system. This means that, on a common 1.x GHz computer with two cores, you can run about 5,000 SNMP v3 sensors with a 60 seconds scanning interval; on a system with four cores, you can monitor around 10,000 sensors with 60 seconds interval. The CPU load is at about 50% then. We do not recommend more.

Furthermore, the PRTG core server and probes should run on different computers. If you experience increased values in the Interval Delay SNMP or Open Requests channels of the **Probe Health Sensor** 1378 (values above 0 % indicate that the SNMP requests cannot be performed at the desired interval), you need to distribute the load over multiple probes. SNMP V1 and V2 do not have this limitation.

If you run into SNMP overload problems, you have three options:

- Increase the monitoring interval of the SNMP V3 sensors.
- Distribute the SNMP V3 sensors over two or more probes.
- Switch to SNMP V1 or V2 if you can go without encryption.

What is the SNMP Community String?

The SNMP Community String is similar to a user ID or password that allows access to the statistics of a router or another device. PRTG Network Monitor sends the community string along with all SNMP requests. If the correct community string is provided, the device responds with the requested information. If the community string is incorrect, the device simply discards the request and does not respond.

ⓘ SNMP community strings are only used by devices that support SNMP V1 and SNMP V2c protocols. SNMP V3 uses safer username/password authentication, along with an encryption key.

By convention, most SNMP V1/V2c equipment ships with a read-only community string set to the value **public**. It is standard practice for network managers to change all the community strings to customized values during device setup.

More

Tools: Paessler MIB Importer and SNMP Tester

- https://www.paessler.com/tools/

Knowledge Base: How do SNMP, MIBs and OIDs work?

- https://kb.paessler.com/en/topic/653

Paessler White Papers: Introducing SNMP and Putting SNMP into Practice

- https://www.paessler.com/press/whitepapers/introducing_snmp

German: Paessler White Paper: Einführung in SNMP und SNMP praktisch anwenden

- http://www.de.paessler.com/press/whitepapers/introducing_snmp

Video Tutorial: SNMP Basics

- https://www.paessler.com/support/videos/prtg-basics/snmp-basics

Video Tutorial: Debugging SNMP

- https://www.paessler.com/support/videos/prtg-basics/snmp-debugging

Knowledge Base: My SNMP sensors don't work. What can I do?

- https://kb.paessler.com/en/topic/46863

Knowledge Base: The interface numbers on my switch keep changing. What can I do?

- https://kb.paessler.com/en/topic/62217

Knowledge Base: What can I check if SNMP and SSH sensors throw timeout and auth errors?

- https://kb.paessler.com/en/topic/63794

Knowledge Base: What can I monitor with the SNMP Custom Table sensor?

- https://kb.paessler.com/en/topic/68539

11.2 Monitoring via WMI

You can monitor Windows systems via Windows Management Instrumentation (WMI) 3092 and Windows Performance Counters 3092. WMI is the Microsoft base technology for monitoring and managing Windows based systems. PRTG uses this technology to access data of various Windows configuration parameters and status values. However, sensors using the WMI protocol generally have a high impact on system performance. In addition to strict WMI sensors, there are sensors that can use Performance Counters to monitor Windows systems.

To monitor via WMI and Performance Counters it is usually sufficient to provide **Credentials for Windows Systems** in PRTG. However, monitoring via WMI is not always trivial and often causes issues.

Please see this article in our Knowledge Base if you run into issues: My WMI sensors don't work. What can I do?

It is also possible to use Simple Network Management Protocol (SNMP) for Windows devices. The same information is often available using any of these protocols. From a performance perspective, the preference would be SNMP, and then WMI or Performance Counters.

How WMI Works

WMI allows accessing data of many Windows configuration parameters, as well as current system status values. Access can be local or remote via a network connection. WMI is based on COM and DCOM and is integrated in Windows versions as of Windows Server 2000. (add-ons are available for Windows 9x and NT4). PRTG officially supports WMI for Windows 7 or later.

To monitor remote machines, PRTG WMI sensors need Active Directory account credentials to have access to the WMI interface. You can enter these credentials in PRTG for the parent device or group, or in the **Root** 294 group. The sensor will then inherit these settings.

Sensors using the Windows Management Instrumentation (WMI) protocol generally have high impact on the system performance! Try to stay below 200 WMI sensors per probe 111. Above this number, please consider using multiple **Remote Probes** 3196 for load balancing.

For an overview and details about all WMI sensors, please see the **List of Available Sensor Types** 389 section.

Monitoring Windows Systems: Performance Counters

Besides sensor types that can monitor Windows systems only via WMI, PRTG provides sensor types that can use a hybrid approach. If you choose the hybrid approach, these sensors will first try to query data via Windows Performance Counters using Remote Registry Service. These Windows sensors use WMI as a fallback if Performance Counters are not available or cannot be read out. When running in fallback mode, PRTG re-tries to connect to Performance Counters after 24 hours. You can change the **Preferred Data Source** in the **Windows Compatibility Options** in the **Device Settings** 360.

You can identify these hybrid sensors by looking at their categories, for example, in the add sensor dialog. **Search directly** for "windows" and select "Performance Counters" as **Technology Used**. Among them are various sensors with "Windows" in the name, as well as some Hyper-V sensors.

Limitations of WMI on Windows Server 2008 (R1)

You should be aware that performance of WMI based monitoring is drastically limited when the monitoring station or the monitored client runs on Windows Server 2008 (R1). When it comes to network monitoring via WMI, Windows Server 2008 R2 is many times faster than Windows Server 2008 (R1).

These are not limitations of PRTG, but arise from the WMI functionality built into the Windows operating systems mentioned.

These limitations also apply to Windows Vista, which is no longer officially supported. You can still monitor machines running Windows Vista, but PRTG core server and probes are no longer supported on this operating system.

The results of our tests are:

- On Windows Server 2008 R2 or Windows 7 (and on later Windows versions) you can run most WMI sensors if you provide optimal conditions, such as running the core and the target systems exclusively under Windows Server 2008 R2 and being located within the same LAN segment. Actual performance can be significantly less depending on network topology and WMI health of the target systems—we have seen configurations that could not go beyond 500 sensors (and even less).
- On Windows 2008 (R1) you can run about 300 WMI sensors with one minute interval.
- The more Windows 2008/Windows 7 client systems you have in your network, the more WMI monitoring performance will be affected.
- System performance (CPU, memory etc.) of virtualization does not strongly affect WMI monitoring performance.

If you want to use WMI for network monitoring of more than 20 or 30 systems, please consider the following rules:

- Do not use Windows 2008 (R1) as monitoring stations for WMI-based network monitoring.
- If possible use Windows Server 2008 R2 for WMI based network monitoring (or later Windows versions).
- Consider setting up remote probes for the WMI monitoring. You still get far better WMI monitoring performance with a remote probe on a virtual machine running Windows Server 2008 R2 than on any bare metal system running Windows 2008)
- Consider switching to SNMP-based monitoring for large networks. Using SNMP you can easily monitor 10 times as many nodes as with WMI on the same hardware.

More

Knowledge Base: General introduction to WMI and PRTG

- https://kb.paessler.com/en/topic/1043

Video Tutorial: Bandwidth Monitoring with SNMP and WMI

- https://www.paessler.com/support/videos/prtg-basics/bandwidth-monitoring-basic

Knowledge Base: Which WQL queries are used by PRTG's WMI sensors?

- https://kb.paessler.com/en/topic/8783

Tool: Paessler WMI Tester. A useful freeware tool to test WMI connections. Tests the accessibility of WMI (Windows Management Instrumentation) counters in a quick and easy manner.

- https://www.paessler.com/tools/wmitester

11.3 Monitoring via SSH

Monitoring via Secure Shell (SSH) enables you to gather performance and system data from many Linux and Unix distributions, as well as from certain Mac OS X systems. If your system is supported, this monitoring technology will work without any additional software on the target systems.

How Monitoring via SSH Works

To monitor remote machines via SSH, PRTG needs credentials (preferably root access) of the devices. If you use SSH sensors with PRTG, you can enter the necessary credentials in PRTG for the parent device or group, or in the **Root** 294 group, in the Credentials for Linux/Solaris/Mac OS (SSH/WBEM) Systems section on the **Settings** 188 tab. The sensors then inherit these settings by default.

With each scanning interval, PRTG logs in to your devices and queries data by executing specific commands.

For an overview and details about all SSH sensors, see the **List of Available Sensor Types** 390.

Limitations When Using SSH Monitoring

Due to the plurality of Linux/Unix derivatives, SSH sensors cannot support all distributions on the market. Also, only certain Mac OS systems are supported.

For a list of successfully tested distributions, see this Knowledge Base article: Which Linux or Mac OS distributions are supported by the Linux/Unix sensors (SSH, SNMP)?

Authentication via SSH Private Key

PRTG supports authentication via password or via private key.

When you use a private key, please ensure the following:

- Provide the key in OpenSSH RSA format.
- The key may not be encrypted! PRTG does not support password protected keys.
- The key must be provided as RSA key, you cannot use DSA keys with PRTG!

When you provide an unencrypted RSA private key in OpenSSH RSA format, please copy the entire key, including the

```
-----BEGIN RSA PRIVATE KEY-----
```

and

```
-----END RSA PRIVATE KEY-----
```

lines, into the designated text field in PRTG and **Save** your settings. Once you have pasted in and saved the private key, PRTG shows it as

```
**************************
```

Please make sure there exists a corresponding public key on the target device.

For a detailed description how to convert and use an existing SSH key, see this Knowledge Base article: How can I use private keys for my SSH sensors with PRTG?

More

Knowledge Base: Which Linux or Mac OS distributions are supported by the Linux/Unix sensors (SSH, SNMP)?

- https://kb.paessler.com/en/topic/6733

Knowledge Base: How can I use private keys for my SSH sensors with PRTG?

- https://kb.paessler.com/en/topic/32883

Knowledge Base: How do I enable SSH on my Mac OS X system?

- https://kb.paessler.com/en/topic/33113

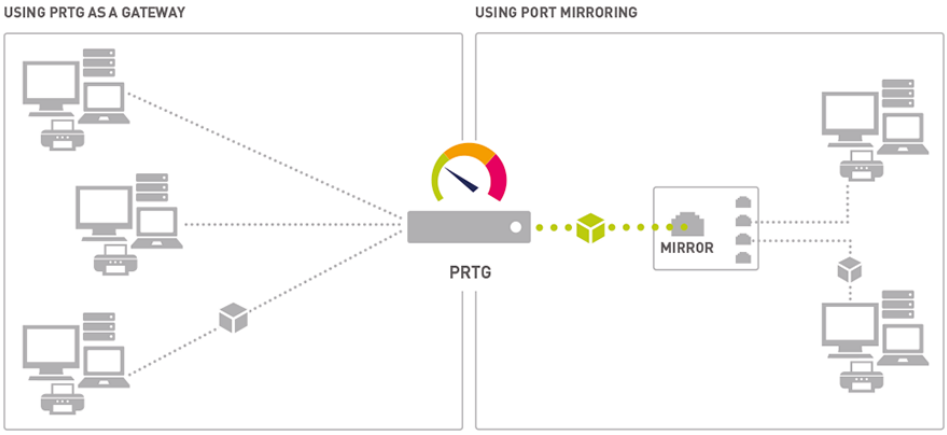
11.4 Monitoring Bandwidth via Packet Sniffing

Packet Sniffing comes into consideration if your network device(s) do not support SNMP or xFlow to measure bandwidth usage and if you need to differentiate the bandwidth usage by network protocol and/or IP addresses.

Packet Sniffer sensors support **Toplists** 2806 (Top Talkers, Top Connections, etc.).

How Packet Sniffing Works

If you need to know what applications or IP addresses cause the traffic in your network, you can use a packet sniffer. A packet sniffer looks at every single data package that travels through your network for accounting purposes.



Monitoring with PRTG via Packet Sniffer Sensors

Click here to enlarge: http://media.paessler.com/prtg-screenshots/data-acquisition-using-packet-sniffing-lan.png

PRTG can analyze the packets passing the network card of a PC or you can connect it to the monitoring port of a switch. To calculate bandwidth usage, PRTG inspects all network data packets either passing the PC's network card (shown on the left side in the schema above) or the data packages that a monitoring port of a switch (right side) sends with its built-in packet sniffer. Using remote probes, you can set up packet sniffers anywhere in your network (see **Add Remote Probe** 3195 section).

Comparing 3102 the four bandwidth monitoring technologies which PRTG provides (SNMP, WMI, xFlow, and packet sniffer) this one creates the most CPU and network load, so you should only use it in small to medium networks, on dedicated computers for larger networks or for individual computers.

Reasons to Choose Packet Sniffing

It is important to understand that the packet sniffer can only access and inspect data packages that actually flow through the network interface(s) of the machine running the PRTG probe software. This is fine if you only want to monitor the traffic of this machine (e.g., your web server). In switched networks, only the traffic for a specific machine is sent to each machine's network card, so PRTG can usually not discern the traffic of the other machines in the network.

If you also want to monitor the traffic of other devices in your network, you must use a switch that offers a monitoring port or port mirroring configuration (Cisco calls it SPAN). In this case, the switch sends a copy to the monitoring port of all data packages traveling through the switch. As soon as you connect one of the PRTG probe system's network cards to the switch's monitoring port, PRTG is able to analyze the complete traffic that passes through the switch.

Another option is to set up the PC running PRTG as the gateway for all other computers in the network.

Set Up Packet Sniffer Sensors

Find details on how to set up the different flow sensors in the following sections:

- **Packet Sniffer Sensor** 1278
- **Packet Sniffer (Custom) Sensor** 1289

Header Based Packet Sniffing

For packet sniffing, PRTG looks at the IP addresses and ports of source and destination to assess the protocol. This is a very fast method and saves system resources.

Sometimes, this method is not fully accurate. For example, it is not possible to identify HTTP traffic on ports other than 80, 8080 and 443 as HTTP. HTTP traffic on non-standard ports would not be accounted as such.

More

Video Tutorial: Bandwidth Monitoring With Flows and Packet Sniffing

- https://www.paessler.com/support/videos/prtg-advanced/bandwidth-monitoring-advanced

Knowledge Base: How can I change the default groups and channels for xFlow and Packet Sniffer sensors?

- https://kb.paessler.com/en/topic/60203

11.5 Monitoring Bandwidth via Flows

Using flow protocols, you can monitor the bandwidth usage of all packets going through a device. In PRTG, you can view **Toplists** 2806 for all xFlow (NetFlow, IPFIX, sFlow, jFlow) sensors.

Flows are a type of monitoring data pushed from network devices to PRTG. You can use it to monitor where data is traveling from and to, and how much. This way it determines which machine, protocol, and user is consuming bandwidth. PRTG currently supports the following flow types:

- NetFlow v5/v9 and IPFIX: Originally introduced by Cisco and supported by several vendors
- jFlow: Traffic sampling technology introduced by Juniper networks
- sFlow: Short for sampled flow, introduced by HP. sFlow uses statistical sampling of the traffic at defined intervals to achieve scalability for high volume interfaces.

You can also use packet sniffing 3097 for bandwidth monitoring if your hardware does not support any of these flow versions.

How xFlow Monitoring works

You can measure bandwidth usage by IP address or by application in a network, using one of the xFlow (including IPFIX) protocols. They are the best choice especially for networks with high traffic (connections with 100s of megabit or gigabits).

For xFlow monitoring, the router gathers bandwidth usage data (flows), aggregates them, and sends information about these flows to PRTG using UDP packets. When you use sampling (mandatory for sFlow), only information about every n-th packet is sent to PRTG which reduces CPU load a lot. Because the switch already performs a pre-aggregation of traffic data, the flow of data to PRTG is much smaller than the monitored traffic. This makes xFlow the ideal option for high traffic networks that need to differentiate the bandwidth usage by network protocol and/or IP addresses.

NetFlow and IPFIX Monitoring

The NetFlow (and IPFIX) protocol is mainly used by Cisco devices. Once configured, the router sends for each data flow a NetFlow or IPFIX packet to the monitoring system running on a PRTG probe. You can be filter and evaluate the data in PRTG. There are different NetFlow and IPFIX sensors available: The basic ones offer predefined channel definitions, the custom variants enable you to define your own channels.

The advantage of using NetFlow or IPFIX:

- Generates little CPU load on the router itself (according to Cisco 10,000 active flows create about 7% additional CPU load; 45,000 active flows account for about 20% additional CPU load).
- Generates less CPU load on the PRTG core system, compared to packet sniffer sensors.

You must enable NetFlow or IPFIX export on the device you want to monitor. The device must send a flow data stream to the IP address of the PRTG probe system on which you set up the NetFlow or IPFIX sensor.

You can monitor Juniper **jFlow** with the corresponding sensors as well. Basically they are adjusted NetFlow v5 sensors.

sFlow Monitoring

sFlow works similar to NetFlow monitoring. The router sends data flow packets to the monitoring system running on a PRTG probe. The most obvious difference between the two flow protocols: With sFlow, not all of the traffic is analyzed, but only every n-th packet. It is like having a river of traffic and you take a cup of water out of it ever so often and analyze it.

The advantage is clear: There is less data to analyze, there is less CPU load needed, and less monitoring traffic is generated. Nevertheless, you can get a good insight into your network bandwidth usage.

PRTG supports sFlow version 5.

Set Up Flow Sensors

Find details on how to set up the different flow sensors in the following sections:

- NetFlow V5 Sensor 1207
- NetFlow V5 (Custom) Sensor 1219
- NetFlow V9 Sensor 1230
- NetFlow V9 (Custom) Sensor 1242
- IPFIX Sensor 1063
- IPFIX (Custom) Sensor 1075
- sFlow Sensor 1457
- sFlow (Custom) Sensor 1469
- jFlow V5 Sensor 1095
- jFlow V5 (Custom) Sensor 1107

Limitations

On a powerful 2008 PC (Dual Core, 2.5 Ghz), you can process about 100,000 flows per second for one xFlow stream. Using sampling, the number of actual flows can be much higher. When using complex filters, the value can be much lower. For example, with a router sending about 2,000 flows/second (which corresponds to mixed traffic at gigabit/second level without sampling) you can expect to configure up to 50 NetFlow sensors operating properly.

PRTG internally monitors its own NetFlow processing. You can see decreased values in the **Health** channels of the Core Health 602 and Probe Health 1378 sensors as soon as NetFlow packets are not processed due to an overload (you find these sensors on the local probe device).

If you experience an overload, please consider using sampling or setting up multiple probes and distribute the NetFlow streams to them. We recommend that you do not add more than 50 NetFlow sensors per PRTG probe.

This sensor type cannot be used in cluster mode. You can set it up on a local probe or remote probe only, not on a cluster probe.

Flow sensors are not IPv6 compatible.

More

Video Tutorial: Bandwidth Monitoring With Flows and Packet Sniffing

- https://www.paessler.com/support/videos/prtg-advanced/bandwidth-monitoring-advanced

Knowledge Base: Can I add custom channels to standard Packet Sniffer and NetFlow sensors?

- https://kb.paessler.com/en/topic/2143

Knowledge Base: What filter rules can be used for custom Packet Sniffing or xFlow (NetFlow/sFlow) sensors?

- https://kb.paessler.com/en/topic/483

Knowledge Base: How do the channel definitions for custom Packet Sniffing or xFlow (NetFlow/sFlow) sensors work?

- https://kb.paessler.com/en/topic/473

Knowledge Base: Does my Cisco device (Router/Switch) support NetFlow Export?

- https://kb.paessler.com/en/topic/5333

Knowledge Base: Do you have any configuration tips for Cisco routers and PRTG?

- https://kb.paessler.com/en/topic/563

Knowledge Base: How to monitor Cisco ASA Firewalls using NetFlow 9 and PRTG?

- https://kb.paessler.com/en/topic/1423

Knowledge Base: How can I change the default groups and channels for xFlow and Packet Sniffer sensors?

- https://kb.paessler.com/en/topic/60203

Knowledge Base: What is the Active Flow Timeout in Flow sensors?

- https://kb.paessler.com/en/topic/66485

Tools: NetFlow Generator and NetFlow Tester

- https://www.paessler.com/tools/

11.6 Bandwidth Monitoring Comparison

The following table shows the differences between PRTG's four methods available for bandwidth monitoring:

	WMI 3092	SNMP 3087	Packet Sniffer 3097	xFlow (IPFIX, NetFlow, sFlow, jFlow) 3099
Setup	Medium	Easy	Easy to complex (depending on filter rules used)	Can be complex (e.g., the switch must be configured)
Traffic can be filtered	No	No	Yes	Yes
Differentiate bandwidth usage by protocol or IPs	No	No	Yes	Yes
PRTG can show Toplists (Top Talker, Top Connections, Top Protocols, custom)	No	No	Yes	Yes
Filter bandwidth usage by IP	No	No	Yes	Yes
Filter bandwidth usage by MAC address	No	No	Yes	No
Filter bandwidth usage by physical network port	Yes	Yes	No	No

	WMI 3092	SNMP 3087	Packet Sniffer 3097	xFlow (IPFIX, NetFlow, sFlow, jFlow) 3099
Monitor network parameters other than bandwidth usage	Yes	Yes	No	No
CPU load on the machine running PRTG	Low	Low	Higher, depends on the amount of traffic	Higher, depends on the amount of traffic
Excess bandwidth usage of monitoring	Small	Small	None (except when monitoring switch ports are used)	Depends on the traffic

More

Knowledge Base: Should I use SNMP, xFlow (IPFIX/NetFlow/sFlow) or Packet Sniffing for my monitoring?

- https://kb.paessler.com/en/topic/923

Knowledge Base: How do I discern excessive bandwidth usage with PRTG?

- https://kb.paessler.com/en/topic/2923

11.7 Monitoring Quality of Service and VoIP

PRTG can monitor the Quality of Service (QoS) in a network with dedicated QoS sensors, as well as Cisco IP Service Level Agreement (SLA) and Cisco Class Based Quality of Service (CBQoS). Slight variations of network parameters like jitter, packet loss, or packet delay variation (PDV) usually have only little effect on TCP based services (for example, HTTP, SMTP). But for UDP based services like Voice over IP (VoIP) and video streaming, a steady stream of data packets is crucial. The sound quality of a VoIP call drops dramatically when UDP packets are not received in a timely fashion, or if packets are lost or out-of-order.

As a rule of thumb for good quality of service (in a VoIP perspective), you want low measurements for jitter (less than 20 to 50 ms) and PDV (less than 100 ms), and preferably zero measurements for packet loss, duplicated packets, or packets in wrong order.

For Quality of Service measurements, four sensor types are available:

- **QoS (Quality of Service) Sensor** 1395
  Monitors VoIP relevant network parameters by testing network connection quality between two probes.
- **QoS (Quality of Service) Round Trip Sensor** 1403
  Monitors VoIP relevant network parameters by testing network connection quality between a probe and a target device at the endpoint of the connection. Traffic is measured bidirectional.
- **Cisco IP SLA Sensor** 540
  Monitors VoIP relevant network parameters through IP SLA results from Cisco devices (via SNMP).
- **SNMP Cisco CBQoS Sensor** 1587
  Monitors VoIP relevant network parameters by using Cisco's CBQoS (via SNMP).

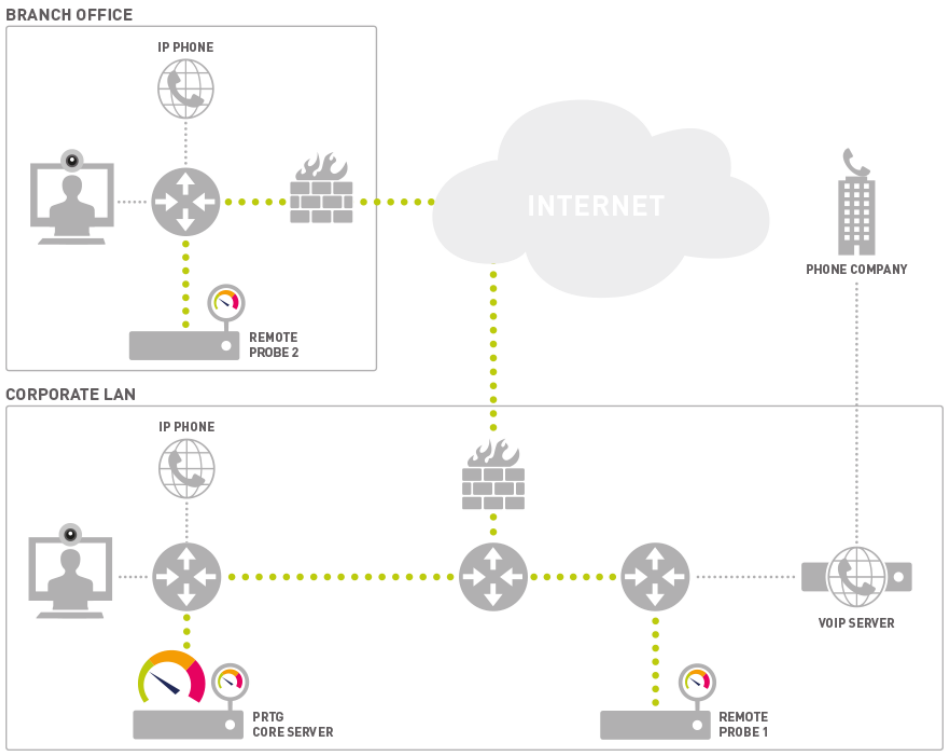
QoS (Quality of Service) Sensors

The QoS Sensors monitor the quality of a network connection by measuring the following parameters:

- Jitter in ms according to RFC 3550
- Packet delay variation (PDV) in ms according to RFC 3393
- Lost packets in %
- Out-of-order packets in %
- Duplicated packets in %

The QoS sensors measure quality of service by sending UDP packets between two probes. This means that you can test any network connection in your network by simply placing a remote probe 3195 on (or near) each 'end' of the connection and measuring the connection quality between them. This is the perfect tool to find network issues that can affect VoIP sound quality or video streaming 'hiccups'.

You can use the QoS Round Trip sensor also without installing a remote probe at the connection endpoint. See this Knowledge Base article for details about the PRTG QoS Reflector: How can I monitor QoS roundtrips without using remote probes?



Monitoring Quality of Service with PRTG

Click here to enlarge: http://media.paessler.com/prtg-screenshots/voip-monitoring-1.png

The measurements for QoS monitoring are taken between two probes. So the first step is to place two PCs running a remote probe on (or near) both ends of the connection that you want to monitor. As an alternative, the local probe on the PC running the PRTG core can also be used as one end, or you can use the PRTG QoS Reflector (see the Knowledge Base) to bounce the packets when monitoring QoS roundtrips. If any firewalls, packet filters, or Network Address Translation (NAT) systems are en route, you must configure them as necessary so that the UDP packets can reach the target probe.

In PRTG, create a new QoS sensor on a **Probe Device**, or, if you use the roundtrip sensor, on any device. With the settings for number and for size of the packets, you can configure the test data stream. 1,000 packets of 172 bytes each is a good start, but if your applications use larger packets you may want to enter other values here. Try to configure the test streams with parameters similar to that of the UDP services you are using across this connection.

Find details about settings in the manual sections **QoS (Quality of Service) One Way Sensor** 1395 and **QoS (Quality of Service) Round Trip Sensor** 1403.

Cisco IP SLA Sensor

Wikipedia describes IP SLA as a feature included in the Cisco IOS Software that can allow administrators the ability to Analyze IP Service Levels for IP applications and services. IP SLA uses active traffic-monitoring technology to monitor continuous traffic on the network. This is a reliable method in measuring over head network performance. IP-SLA is mostly used to monitor the sound quality of VoIP traffic.

If you have not done so already, add a device in PRTG for the Cisco device that you want to monitor. Then create a new **Cisco IP SLA** sensor on this device.

Find details about settings in the **Cisco IP SLA Sensor** 540 section.

This feature is only available in the more expensive Cisco devices. If you do not have IP SLA capable routers and switches, you can still get similar information with PRTG QoS sensors (see above 3104) that do not require any special hardware—just two PCs running Windows. If you own hardware that supports IP SLA, then PRTG brings you probably the least-cost monitoring solution for IP SLA. Most vendors charge extra for IP SLA support (a thousand bucks and more). Following Paessler's long term policy, we simply include this as one of our sensor types. With PRTG you can even use the PRTG on premises Freeware Edition to monitor IP SLA!

PRTG monitors the following parameters: Calculated Planning Impairment Factor (ICPIF), Mean Opinion Score (MOS), Average Jitter, Packets Lost, Packets Out Of Sequence, Packets Late, Average Round Trip Time (RTT), DNS RTT, TCP RTT, Transaction RTT.

Especially two of these parameters are interesting for VoIP: Mean Opinion Score (MOS) and Calculated Planning Impairment Factor (ICPIF).

SNMP Cisco CBQoS Sensor

Cisco Class Based Quality of Service (CBQoS) provides information about QoS of Cisco network devices which support the Modular QoS command line interface (MQC). With Classed Based QoS, you can obtain monitoring data that includes summary counts and rates by traffic class before and after the enforcement of QoS policies, according to Cisco's CBQoS Management Information Base (MIB) definition.

PRTG determines CBQoS data via Simple Network Management Protocol (SNMP). The corresponding sensor type is available out-of-the-box in PRTG version 13.x.5 or later. CBQoS is available in Cisco IOS by default as of version 12.4(4)T.

To monitor CBQoS, add a device to PRTG for the Cisco device that you want to monitor. Then create a new SNMP Cisco CBQoS sensor on this device.

See section **SNMP Cisco CBQoS Sensor** 1587 for more details.

This sensor type supports the following CBQoS classes:

- **Class Map**: statistical data about class maps, such as pre- and post-policy packets and sizes, drop packets and size, as well as no-buffer drop packets

- **Match Statement**: statistical data about match statement specific information, such as pre-policy packets and size
- **Queueing**: statistical data about queuing actions, such as current and maximum queue depth, drop packets, and drop size

You can select the desired CBQoS entries which you want to monitor while creating the sensor in PRTG. The available entries are given with their particular connections, their descriptions, and class types.

Voice over IP

For Mean Opinion Score (MOS) measurements, Cisco conducted a panel test where a wide range of listeners judged the quality of voice samples sent using particular codecs, on a scale of 1 (poor quality) to 5 (excellent quality). The Cisco device calculates the corresponding value for the current network connection based on the network parameter measurements like jitter and packet loss.

The Cisco IP SLA sensor reads out the MOS directly from the Cisco device. For the QoS and the QoS Round Trip sensor, PRTG calculates the MOS by itself. For details, see this Knowledge Base article: How does PRTG calculate the MOS score for QoS sensors?

The values and their meanings are:

MOS	Quality	Expected Quality Impairment
5	Excellent	Imperceptible
4	Good	Perceptible, but not annoying
3	Fair	Slightly annoying
2	Poor	Annoying
1	Bad	Very annoying

The second interesting parameter ICPIF is the sum of measured impairment factors minus a user-defined access Advantage Factor that is intended to represent the user's expectations, based on how the call was placed (for example, a mobile call versus a land-line call) (quoted from Cisco's website).

Upper Limit for ICPIF	VoIP Call Communication Quality
5	Very good

Upper Limit for ICPIF	VoIP Call Communication Quality
10	Good
20	Adequate
30	Limiting case
45	Exceptional limiting case
55	Customers likely to react strongly (complaints, change of network operator)

More

Knowledge Base: Where can I find more information about Cisco IP SLAs, VoIP, and QoS?

- https://kb.paessler.com/en/topic/11093

Knowledge Base: How does PRTG calculate the MOS score for QoS sensors?

- https://kb.paessler.com/en/topic/59491

Knowledge Base: How can I monitor QoS roundtrips without using remote probes?

- https://kb.paessler.com/en/topic/61176

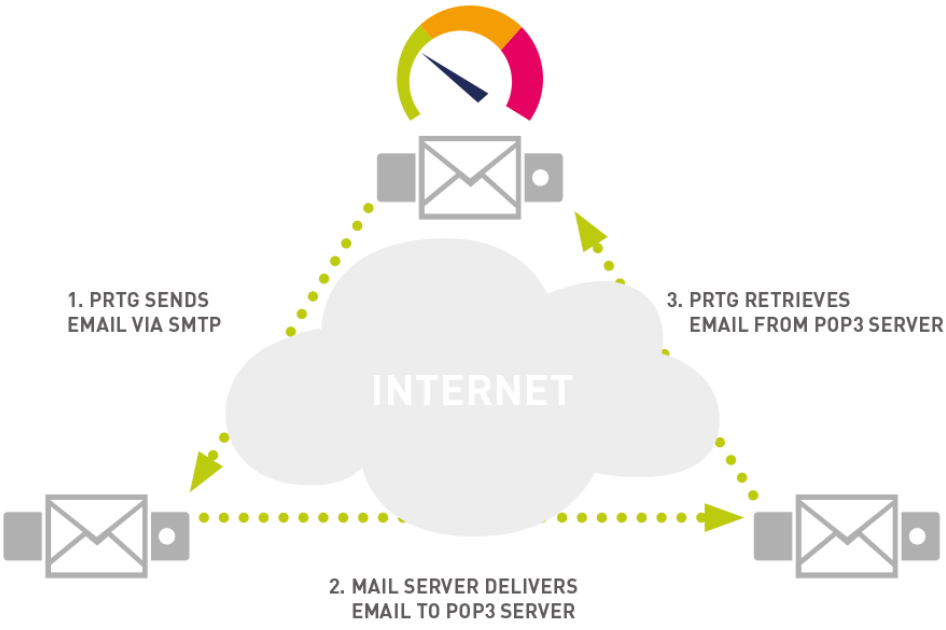
11.8 Monitoring Email Round Trip

Email Round Trip sensors ensure the end-to-end delivery of emails and make it possible to monitor availability and performance of a complete email delivery process. There are two sensor types for this task:

- SMTP&POP3 Round Trip Sensor 1519
- SMTP&IMAP Round Trip Sensor 1508

Both initially deliver an email to a mail server using SMTP. Afterwards the receiving mailbox is scanned using Post Office Protocol version 3 (POP3) or Internet Message Access Protocol (IMAP) until the email arrives. The test email contains a unique code in the topic which is used to identify the email, such as PRTG Roundtrip Mail: {6D136420-5A3E-46CF-871A-1DAF0C4F3D5D}

When PRTG successfully received an email in this email round trip cycle, it marks the respective message for deletion on the mail server. Usually, a mail server will then delete this email. For best performance, we recommend using a dedicated email accounts for email round trip sensors.



Monitoring an Email Round Trip

Click here to enlarge: http://media.paessler.com/prtg-screenshots/monitoring-an-email-round-trip.png

In the scenario shown above, there are three steps in the round trip:

- **Step 1**
  PRTG delivers an email via the SMTP protocol to a mail server (just like an email client).
- **Step 2**
  The SMTP server delivers the email to a POP3/IMAP server (which can be located at a remote site, in your local LAN or on the same server as well).

- **Step 3**
  Every few seconds PRTG connects to the POP3/IMAP server until the test email arrives.

Recommended Configuration

Here is a simple concept to check delivery of email out of and into your organization:

1. Create a dedicated email account for this test in your mail system.
2. Set up an external email account (hosted mail server, free mail service, etc.) and configure it to send all emails back to this dedicated email account in your organization (which you created in Step 1).
3. Set up a PRTG round trip sensor to send an email to the external email account (which you created in Step 2) using your network's mail server and then check for the email account on your mail system (which you created in Step 1) for arrival of the email.

With this technique you are testing multiple aspects of your email server setup. As long as the sensor shows a green light, this means:

- Your email server accepts emails via SMTP.
- Emails are being sent to the outside world (internet connection works, MX lookups work etc.).
- Emails from external mail server can be delivered into your mail system (this includes aspects like the fact that the MX records for your domain are correct, your mail server can be reached from the outside world, your email filtering is working etc.).
- Emails can be retrieved using POP3 (or IMAP).

Please use dedicated email accounts with this sensor type. If you use more sensors of this type, please make sure that each sensor uses its own email accounts.

Conclusion

These two sensor types are a great tool to ensure delivery of email from and to your mail servers. Compared to the standard SMTP, POP3, and IMAP sensors, which only check the availability of these services, the two roundtrip sensor types actually monitor the complete transaction from accepting the email on the first email server to delivery of the email on the final POP3/IMAP server.

11.9 Monitoring Backups

Monitoring your backup software enables you to be sure that your recent backups succeeded. With PRTG you can check the email notifications of various backup jobs. You only need two things for backup monitoring:

1. Configure your backup software to send emails to a dedicated email account.
2. Configure the PRTG **IMAP Sensor** for backup monitoring.

PRTG will analyze the backup emails for you and set the status of the IMAP sensor accordingly. This way you will see the states of all your backup jobs at a glance.

Backup Monitoring via Email

Click here to enlarge: http://media.paessler.com/prtg-screenshots/backup-monitoring-via-email_en.png

Setting up Backup Monitoring

Please refer to our Knowledge Base for a step-by-step tutorial to monitor your backup jobs: Monitoring Backup Solutions via Email

More

Knowledge Base: Monitoring Backup Solutions via Email

- https://kb.paessler.com/en/topic/47023

Knowledge Base: Can I analyze multipart emails using the PRTG IMAP sensor?

- https://kb.paessler.com/en/topic/63532

11.10 Monitoring Virtual Environments

A highly flexible IT infrastructure is a common need nowadays and virtualization has become an important pillar of the IT all over the world. Applications in your network might be distributed over many different servers, networks, and locations. They might also be in the cloud, and your computations can take place in data centers spread over the whole world. So, if your network connection or any other corresponding hardware fails, hundreds of applications might be unavailable—an impact to your daily business processes which should be avoided at any costs.

Because of this, monitoring the physical infrastructure of your data center is still a must in times of virtual environments. With the layer of virtualization in addition to your physical equipment, your logical infrastructure also needs a close treatment. PRTG assists you to deal with these advanced requirements and enables you to react proactively to issues before they affect your whole system. With PRTG you can monitor all layers of your IT infrastructure in a comprehensible way so you will reduce issues related to dynamic IT environments significantly.

Monitoring All Layers of Your IT Infrastructure

In general, you can assume that with the layer of virtualization you have to monitor a total of four layers in your IT infrastructure:

- **Hardware (Server Racks):** Usually you will set up your monitoring in the common way and monitor most of the hardware components in your network with PRTG's SNMP sensors 387. You are able to gain monitoring data about many different device readings such as CPU load, memory, disk space with this monitoring technology 3087, as well as information about network traffic and bandwidth usage of your routers and switches. It is absolutely mandatory for a working IT environment to monitor all hardware components in order to be alerted if something fails or hardware resources are running out. In addition, you can identify potential bottlenecks affecting your virtualized infrastructure. You can set this monitoring up in the usual way.

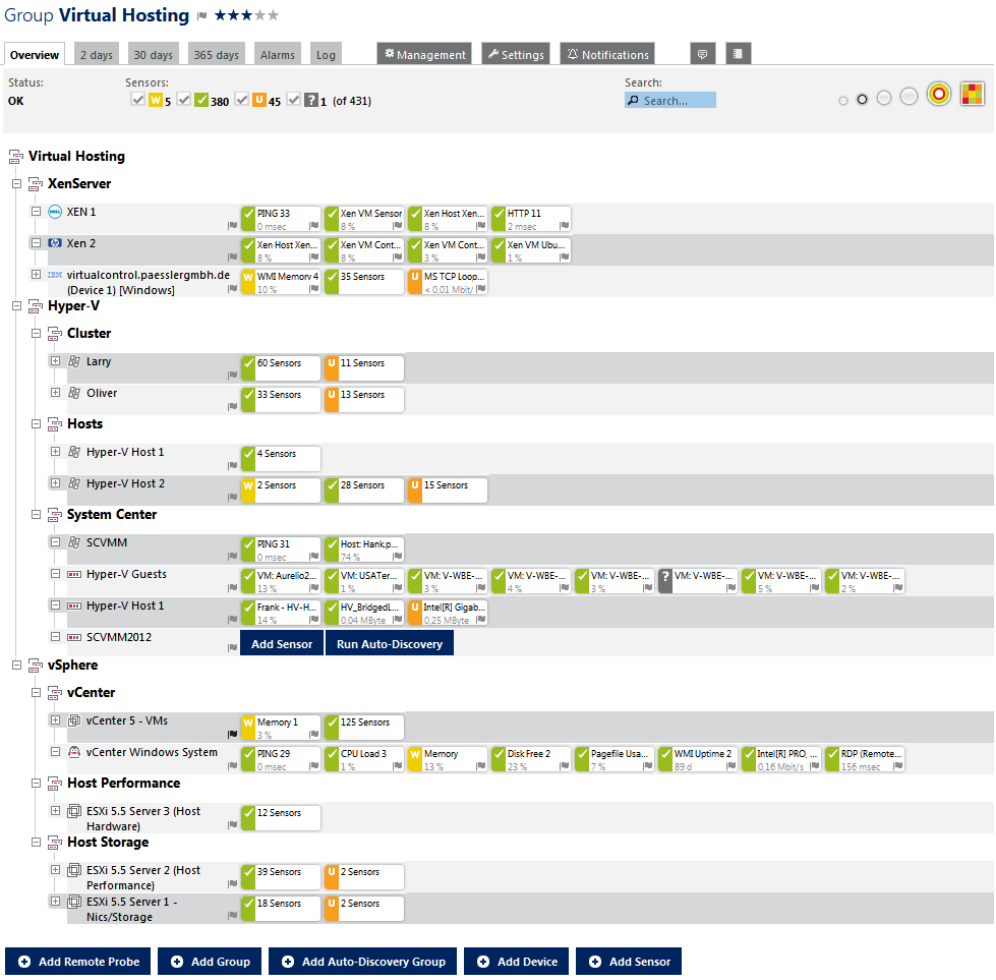
- **Host Server Hardware:** It is essential to explicitly monitor the host hardware of your virtualization solution. If you have issues with your virtual machines (VMs), the origin might be a host hardware failure. You should closely monitor your VM host servers to get alerted if the status is other than "normal". Besides the out of the box hardware sensors, PRTG provides specific sensors for various virtualization host servers; the following monitoring data of your host servers will help you prevent issues in virtualized environments:
  - VMware: current reading and health status (via WBEM), a general status as shown in vSphere (via SOAP), and disk space of a VMware data store (via SOAP)
  - Hyper-V: host health critical values, deposited pages, network traffic, CPU usage of guests, hypervisor, and in total
  - Citrix XenServer: CPU, memory, and network usage, the number of running virtual machines on the host server, and load average

- **VMs from the "Outside":** The virtual machines run on their particular host servers. PRTG can show you the status of single virtual machines and several of their performance counters. It might be helpful to know which resources a single VM uses and needs, but monitoring single VMs is not advisable in every case because it has a noticeable influence on the overall performance. Often it will be sufficient to monitor only VMs which are critical for your network. If a VM reaches its capacity limits, PRTG can alert you and you can conduct the corresponding resolution steps like enhancing this VM's resources. Indicators for a healthy virtual machine which you can monitor with PRTG out of the box are:
  - VMware: CPU and memory usage, disk read and write speed, read and write latency, and network usage
  - Hyper-V: CPU usage, disk read and write speed
  - Citrix XenServer: CPU usage and free memory

- **VMs from the "Inside" (Operating Systems):** You can monitor the Windows operating system of a single VM with PRTG's standard WMI sensors 389, for example. With this technology 3092 you can access data of various Windows parameters. Other operating systems like Linux/MacOS can make data available via SSH 3095 and SNMP 3087. The status of the operating systems on your VMs can indicate potential issues of the same, just like the operating systems on your physical machines which are important for a reliably working IT infrastructure: You can monitor these with the same attention, depending on your application scenario, but be careful due to performance considerations. Especially many WMI sensors can result in load problems, so monitor only really important systems "from the inside". Furthermore, you do not need to monitor every item multiple times. For example, it might be sufficient to monitor free disk space only from the outside of the actual VM.

Monitoring the Virtual Infrastructure

To monitor your IT infrastructure, best practice is to set up the monitoring of the hardware layer of your data center first in PRTG, especially in order to find potential bottlenecks which might have an impact on your virtual servers. Then you can start monitoring your virtual environment itself. If you use several solutions for virtual hosting, it is also a good idea to group related host servers, their virtual machines, and the operating systems together. The screenshot below will give you an idea about how to organize this.



Grouped Virtual Components

The screenshot above shows you the particular group "Virtual Hosting" of an entire PRTG setup. This is an example how monitoring of virtual environments can look like. The sample group contains several subgroups for the virtualization solutions Citrix "XenServer", Microsoft "Hyper-V", and VMware "vSphere". The vSphere group, for example, has three subgroups: we monitor the vCenter VMs and the vCenter Windows system, the performance of the host server, and the storage system of the host.

Devices for Physical Hosts

In PRTG, set up devices which represent the physical hosts of your virtual machines. For example, for your VMware hosts, add devices which represent the ESXi servers, for Hyper-V add devices which represent your Hyper-V host servers, for Citrix add devices which represent your Xen servers.

Then you can add suitable and expressive sensors to the host server devices. Running PRTG's auto-discovery [249], many useful sensors will be created automatically. There are several pre-configured host hardware sensors available out of the box in PRTG:

- VMware Host Hardware (WBEM) Sensor 2354: monitors an ESXi server via Web-Based Enterprise Management (WBEM)
- VMware Host Hardware Status (SOAP) Sensor 2362: monitors a VMware host server via Simple Object Access Protocol (SOAP)
- VMware Host Performance (SOAP) Sensor 2372: monitors a VMware host server via Simple Object Access Protocol (SOAP)
- Hyper-V Host Sensor 1001: monitors via Windows Management Instrumentation (WMI) or Windows Performance Counters, as configured in the "Windows Compatibility Options" of the parent device
- Citrix XenServer Host Sensor 550: monitors via Hypertext Transfer Protocol (HTTP)

These sensor types monitor hardware specific counters to ensure that no hardware issues affect your actual virtual machines. Additional sensor types can monitor the host hardware via SNMP (for example, traffic and custom requests), data storage on ESXi servers via SOAP, as well as there are sensors for network adapters and storage devices which are connected to a Hyper-V host server. You can also monitor Virtuozzo host servers with sensors for network usage and disk space for each container.

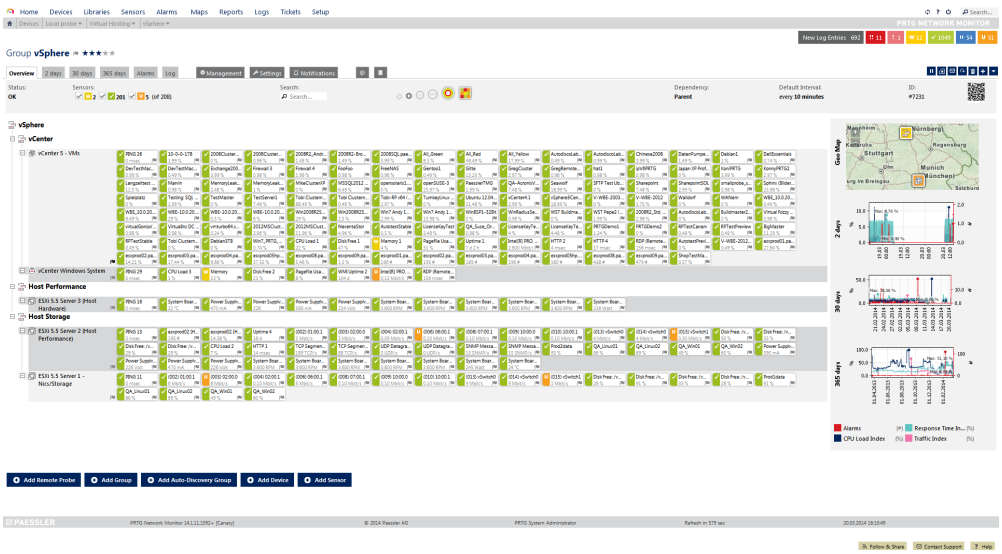
Devices for Virtual Machines

To monitor your actual virtual machines, add them to your host servers in PRTG. For a better overview, you might want to add another device to PRTG which represents your host server and add sensors for your VM to there. The according sensors for virtual machines will show you the performance of single VMs as well as their usage of resources. This will help you identify VMs with poor performance and react proactively before one or more VMs crash. As mentioned above, you can additionally monitor your particular VMs from the inside (which means the operating systems on your VMs) if necessary. See the sections below for details about particular virtualization solutions.

VMware Virtual Machine

PRTG's VMware Virtual Machine (SOAP) Sensor 2382 monitors VMs on a VMware host server via Simple Object Access Protocol (SOAP). With the VMware system, the general idea is to add a vCenter server as a device to PRTG and use the vCenter as parent device where you add the sensors to for your virtual machines. So, in the case of vMotion when your VMs change their host server, PRTG will be able to follow these movements and will never lose the monitored VMs.

For this sensor type, you need the Microsoft .NET Framework with the latest update of version 4.0 running on the probe machine. If you use many VMware sensors, we also recommend adjusting the settings on your VMware host server to accept more incoming connections.

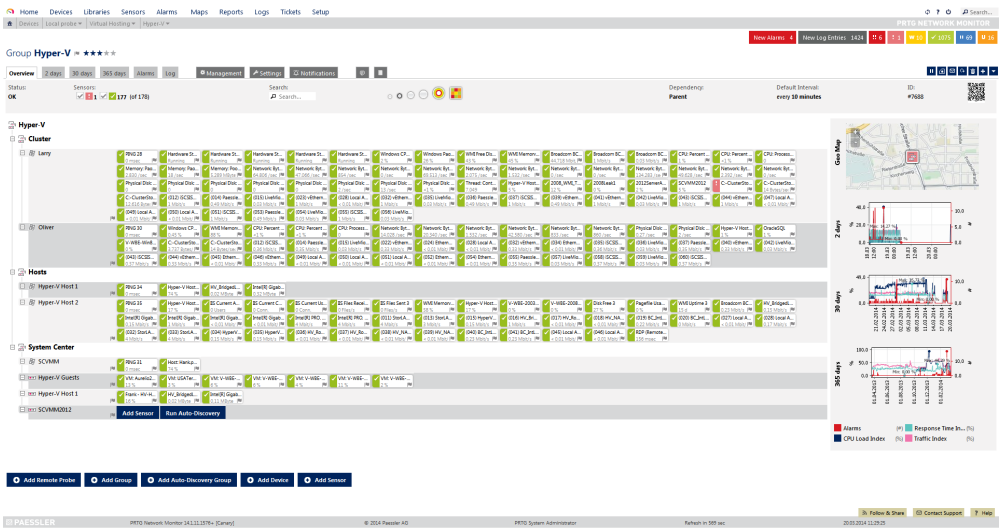


vSphere Group

This screenshot a sample vSphere group in PRTG. As recommended, the VMware virtual machines are added to the vCenter device. There is also a dedicated device for the vCenter Windows operating system with common WMI sensors for CPU, memory, disk, and network usage. The ESXi host servers are organized in their own groups regarding performance and storage. In this example, PRTG monitors the hosts with the standard SNMP hardware sensors as well as with the specific VMware ESXi host sensors.

Microsoft Hyper-V Virtual Machine

PRTG's Hyper-V Virtual Machine Sensor 1009 monitors VMs via Windows Management Instrumentation (WMI) or Windows Performance Counters, as configured in the "Windows Compatibility Options" of the parent device. With this hybrid approach, the sensor first tries to query data via performance counters and uses WMI as a fallback if there are no performance counters available. Performance counters in general need less system resources than WMI. We recommend using System Center Virtual Machine Manager (SCVMM) as parent device for this sensor type, because when your VMs change their physical host with Live Migration, this sensor will still be able to continue monitoring. You should also disable User Account Control (UAC) in the Windows operating system of the VM.



Hyper-V Group

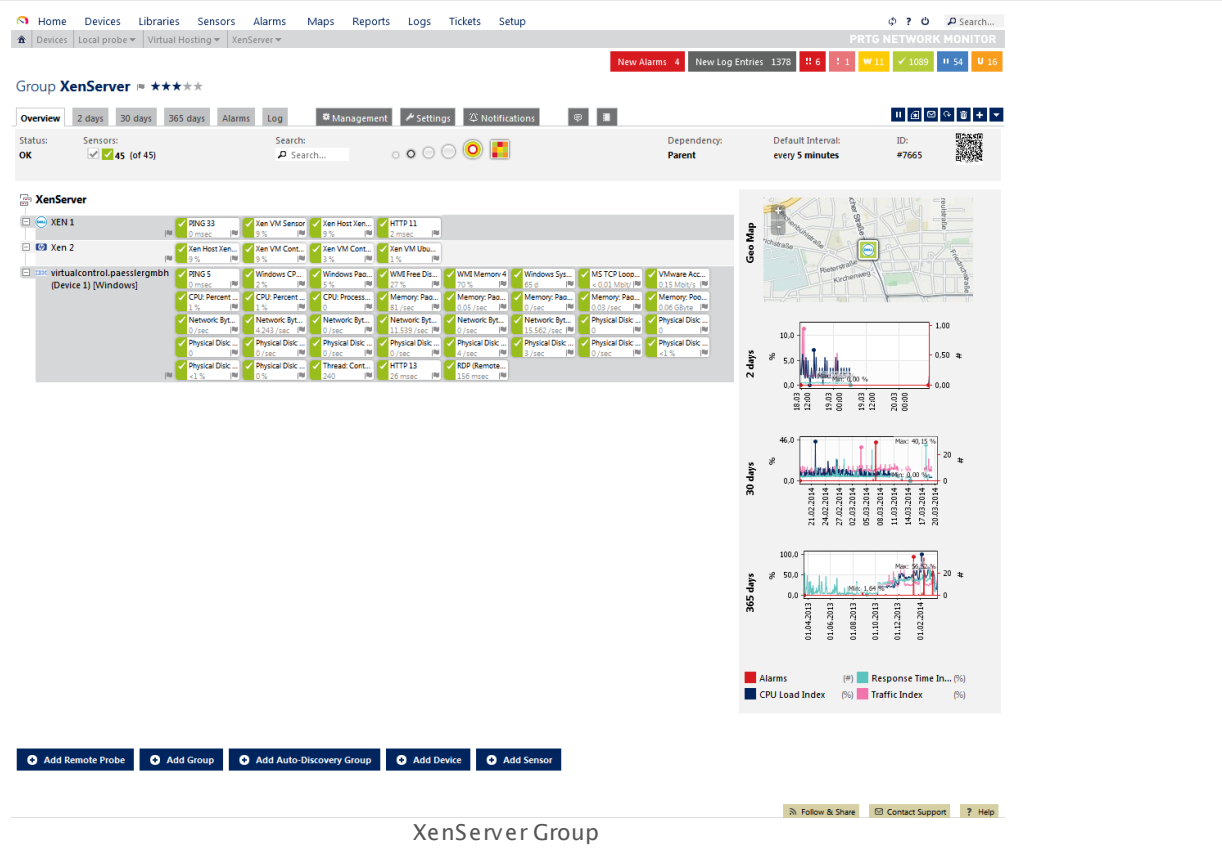
This screenshot shows a sample Hyper-V group in PRTG. There is a dedicated group for failover clustering where two nodes are monitored with several SNMP and WMI sensors, as well as Hyper-V Host Server sensors 1001 and sensors for the Hyper-V virtual machines. This ensures that Hyper-V and failover clustering works without any issues. The Hyper-V hosts are monitored the same way, organized in a dedicated group for hosts.

Note that we recommend adding the particular virtual machines to the SCVMM server if possible! We pointed out above that you should add the VMs to an SCVMM server to avoid issues with Live Migration. You can see this in the group "System Center". The particular VMs are added to the dedicated device "Hyper-V Guests".

Citrix XenServer Virtual Machine

PRTG's Citrix XenServer Virtual Machine Sensor 561 monitors VMs via Hypertext Transfer Protocol (HTTP). For this sensor type, you have to add a device to PRTG which represents a Citrix XenServer with version 5.0 or later. Another requirement is the Microsoft .NET Framework: You have to run the latest update of version 4.0 on the probe machine where you add this sensor to.

In a XenServer pool, every host knows each running VM. Because of this, there is no central instance which provides all available data so it does not matter on which host you query your VMs. All queries on any host are automatically forwarded to the pool master which manages the XenServer pool. So it is sufficient to create the desired sensors for your XenServer VMs on a device that represents one host server of your pool. PRTG's XenServer sensors can figure out by themselves which host is running and retrieve the according data.



XenServer Group

This screenshot shows a sample XenServer group in PRTG. There are two devices for XenServer hosts (Xen 1 and Xen 2), each with a Citrix XenServer Host sensor [550] and several Citrix XenServer Virtual Machine sensors [561] for the particular VMs on this host. Furthermore, the Windows operating system is represented as a dedicated device ("virtualcontrol") which is monitored with several WMI sensors regrading CPU, disk, memory, and network usage.

Conclusion

The sensor types described in this section monitor virtual machine specific counters to ensure that all your VMs have enough resources available. If a VM is overloaded, PRTG can notify you immediately and you can proactively take care of issues before a particular VM has an outage or other failures. Additionally, we have shown an idea for a structured virtual monitoring with several recommendations.

You can find all available sensors for virtual servers and the according virtual machines in section List of Available Sensor Types—Virtual Servers Sensors [391].

Performance Considerations

For best performance when monitoring virtual environments, we strongly recommend that you use a computer with **Windows Server 2012 R2** to run the PRTG probe with the according sensors. So for example, you can run up to 300 VMware sensors in a 60 seconds scanning interval on Windows 2012 R2, while you can only use 30 VMware sensors with the same interval on Windows 2008 R2.

More

Knowledge Base: I run PRTG on VMware. How can I obtain best performance?

- https://kb.paessler.com/en/topic/49193

Sensor Technologies—Topics

- Monitoring via SNMP 3087
- Monitoring via WMI 3092
- Monitoring via SSH 3095
- Monitoring Bandwidth via Packet Sniffing 3097
- Monitoring Bandwidth via Flows 3099
- Bandwidth Monitoring Comparison 3102
- Monitoring Quality of Service 3104
- Monitoring Email Round Trip 3109
- Monitoring Backups 3111
- Monitoring Virtual Environments 3112
- Monitoring Databases 3120
- Monitoring Syslogs and SNMP Traps 3125

11.11 Monitoring Databases

Monitoring your databases enables you to ensure that, on the one hand, database queries are processed in time, and, on the other hand, that the database itself performs within the defined parameters. Furthermore, database monitoring with PRTG makes it possible to be alerted via a corresponding sensor status if database queries return an unexpected result value.

PRTG comes with built-in native sensors for the most common databases:

- Microsoft SQL servers
- MySQL servers
- PostgreSQL servers
- Oracle SQL servers

It is also possible to monitor many other database servers. For this concern, PRTG uses the ActiveX Data Objects (ADO) interface.

There are two types of database sensors:

- **Sensors monitoring databases directly** 3120: Monitor databases from the user perspective. These sensors send a request to the database server and receive corresponding values. You can optionally process data tables and show values in individual channels or monitor transactions.
- **Sensors monitoring database performance** 3123: Monitor databases with a more abstract view on the servers. Usually, these sensors monitor performance counters via Windows Management Instrumentation (WMI).

Sensors Monitoring Databases Directly

PRTG provides several sensors which can "look into" the content of databases. Sensors of this type connect to the database server, execute a defined query, and show the execution time of the whole request and the query. You can use these sensors to process the data table and show requested values in individual channels.

The following sensor types are available for this kind of monitoring:

- **Microsoft SQL v2 Sensor** 1135: Monitor your Microsoft SQL server 2005 or later.
- **MySQL v2 Sensor** 1151: Monitor your MySQL server version 5.0 or later.
- **Oracle SQL v2 Sensor** 1253: Monitor your Oracle database server version 10.2 or later.
- **PostgreSQL Sensor** 1363: Monitor your PostgreSQL database version 7.x or later.

For these sensor types, you can define valid SQL statements that the sensors send to the database server. Define the queries in an SQL script file and store it into the respective **\Custom Sensors\sql** subfolder of your PRTG installation (see section **Data Storage** 3226 for details).

You can select this SQL script when you add the sensor to PRTG. With every scanning interval [307], the sensor executes this script with the defined query against the database and the database returns corresponding values in individual channels (see the example [3121] below for sample channel value selections). Use the **Sensor Channels Settings** [2783] to define limits for specific values.

These sensor types need .NET 4.0 or later installed on the computer running the PRTG probe.

Alternatively, you can monitor almost all available database servers with the **ADO SQL v2 Sensor** [418] via an ActiveX Data Objects (ADO) connection.

Example: SQL Channel Value Selection

The SQL (v2) sensors determine their channel values by using column numbers, column names, row numbers, or key value pairs. This section shows which option you can choose to get the desired value from an SQL data table.

Consider the following data table that an SQL query might return from a database:

article_id	articles_available	first_listing	orders
00	12	2001	4
01	345	2005	56
02	678	2008	290
03	90	2012	32

This data table has four columns with the following numbering:

- Column 0 has the name "article_id"
- Column 1 has the name "articles_available"
- Column 2 has the name "first_listing"
- Column 3 has the name "orders"

The numbering of columns starts with 0, as well as the numbering for rows starts with 0. The table has four rows, each row contains the properties of one "article". The "articles" have the IDs 00, 01, 02, 03. This also illustrates the proper row numbering (0, 1, 2, 3).

With the options for channel value selection in SQL sensors, you can read out the following values:

- All values that are in row 0 (here: 00, 12, 2001, 4)
- All values that are in column 0 (here: 00, 01, 02, 03)

- All values that are in column 1 (here: 12, 345, 678, 90)

It is not possible to get values from any other cell in a data table. If you need this, you have to re-construct your data table.

The following samples show possible results for channel value selections regarding this data table:

SAMPLE CHANNEL VALUE SELECTIONS

Channel Value Selection by Column Number	This channel will show the value in row 0 of the column you specify. Consider you define "1" as column number. Then the sensor channel value is "12" because it is the cell in column 1 and row 0. Possible return values for this option are: ▪ Column number "0" returns "00" ▪ Column number "1" returns "12" ▪ Column number "2" returns "2001" ▪ Column number "3" returns "4"
Channel Value Selection by Column Name	This channel will show the value in row 0 of the column you specify. Consider you define "orders" as column name. Then the channel value is "4" because it is the cell in column "orders" and row 0. Possible return values for this option are: ▪ Column name "article_id" returns "00" ▪ Column name "articles_available" returns "12" ▪ Column name "first_listing" returns "2001" ▪ Column name "orders" returns "4"
Channel Value Selection by Row Number	This channel will show the value in column 0 of the row you specify. Consider you define "1" as row number. Then the sensor channel value is "01" because it is the cell in row 1 and column 0. Possible return values for this option are: ▪ Row number "0" returns "00" ▪ Row number "1" returns "01" ▪ Row number "2" returns "02" ▪ Row number "3" returns "03"

SAMPLE CHANNEL VALUE SELECTIONS

Channel Value Selection by Key Value Pair	This channel will show the value in column 1 of the same row where the key in column 0 was found. Consider you define "02" as key. Then the sensor channel value is "678" because it is the cell in the same row in column 1 as the the key in column 0. Possible return values for this option are: ▪ Key "00" returns "12" ▪ Key "01" returns "345" ▪ Key "02" returns "678" ▪ Key "03" returns "90"

This sample channel value selection illustrates how to choose the correct option to get needed values from an SQL data table and shows which cells the SQL sensors can address.

UDF: Counting Returned Rows

If you execute a UDF (User Defined Function) on the SQL server and want to know how many rows this UDF returns, follow these steps:

- A command to execute your UDF on the SQL server may look like this, for example:

```
exec myUDF
```

- To get the information how many rows this UDF returns, extend the query in your SQL script:

```
exec myUDF;
select @@rowcount as row_count
```

- Create a new SQL v2 sensor and enable **Data Processing** while sensor creation.
- In the settings of your SQL sensor, choose the option **Select Channel Value by Column name**
- Enter **row_count** into the **Column Name** field of the channel to show the value from this column in the channel.
- To count table rows returned by a SELECT statement, choose the option **Count table rows** in the sensor settings section **Data Processing**.

Sensors Monitoring Database Performance

Performance sensors for database servers have a more "abstract" view on databases and regard performance "from the outside". They do not read out any values of the database, neither do they send SQL queries to databases. This sensor type is only available for Microsoft SQL.

The Microsoft SQL server sensors monitor performance via Windows Management Instrumentation (WMI). You can manually set up different performance counters for your server instances, for example, general statistics, access methods, buffer and memory manager, locks, and SQL statistics.

Microsoft SQL Server performance sensors are available for Microsoft SQL Server 2008, 2012, 2014, and 2016:

- **WMI Microsoft SQL Server 2008 Sensor** 2628
- **WMI Microsoft SQL Server 2012 Sensor** 2640
- **WMI Microsoft SQL Server 2014 Sensor** 2652
- **WMI Microsoft SQL Server 2016 Sensor** 2664

11.12 Monitoring Syslogs and SNMP Traps

PRTG is utilizable as a full scale syslog server and SNMP trap receiver. Every PRTG installation includes this functionality so no additional software is needed. This manual section describes a sample configuration for PRTG's syslog and SNMP trap receiver and gives you an idea about how to use these features.

Syslog is a well-established standard for computer message logging. Many network devices support sending syslogs to communicate informational, analysis, and debugging messages that are intended for network management and security auditing. SNMP traps are asynchronous notifications from SNMP-enabled devices and can be used to report important incidents and data, just like syslog messages. Devices trigger these messages for various reasons, such as system events, outages, critical conditions, and many more.

PRTG provides two dedicated sensor types that work as full scale syslog and SNMP trap receivers:

- **SNMP Trap Receiver Sensor** 2143
- **Syslog Receiver Sensor** 2309

Because both the syslog and the trap receiver are implemented as common sensor types, you do not need to install software in addition to PRTG (for example, you do not need an extra syslog server but only the PRTG web server). You can create the Syslog Receiver as well as the SNMP Trap Receiver sensors in the usual PRTG way via the add sensor 288 dialog. Then configure your syslog or SNMP trap-enabled device(s) to send messages to PRTG.

Under lab conditions, PRTG could handle about 10,000 syslog and trap messages per second on a quad core desktop machine when using a single sensor without filters.

The number of messages PRTG can process actually depends on your configuration and system setup. It might be significantly fewer messages.

You can filter the incoming messages by various parameters so that PRTG will process only specific messages and purge other data right away. Processed messages are stored in an internal high-performance database on the particular probe machine and are available for review and analysis via the PRTG web interface. The main limiting factor for storing syslog and trap messages is the hard disk space on the machine running the PRTG probe with these sensors.

Sample Configuration

Follow the steps below for a sample configuration of Syslog and SNMP Trap Receiver sensors. You can apply these instructions to both the SNMP Trap Receiver as well as the Syslog Receiver because the setup works in a similar way for both.

1. Adding the Receivers 3126
2. Configure the Source Devices 3127
3. Collect Messages 3127
4. Review and Analyze Messages 3128

5. Refine the Filters 3129

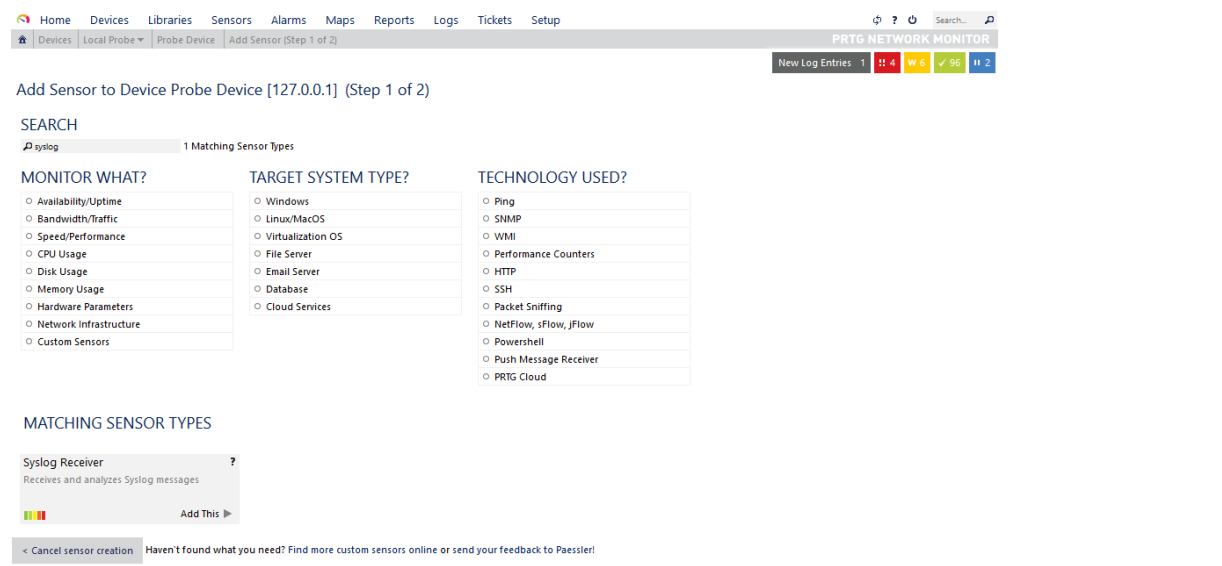
6. Create Notification Triggers 3130

Step 1: Add a Syslog Receiver or SNMP Trap Receiver sensor to PRTG.
Both sensor types inherit an implicit filter from the IP address of the parent device. So, on the one hand, it is possible to add these sensors to a probe device 120. Then you will receive all messages from the system running the probe and can optionally filter for specific sources later. On the other hand, you can add these sensors directly to the source device. Then only messages from this device will be processed.

Add the receiver sensors to the desired device in the common way, for example, via the device's context menu 222. We recommend leaving the sensor's default settings unchanged for the first configuration (port, include and exclude filter, warning and error filter) to see what data actually comes in.

Adding the sensor to a network device directly will increase its speed in comparison to a filter definition in the sensor settings. Distributing Syslog and SNMP Trap Receiver sensors over different probes will make the overall performance scalable and gives you flexibility with the data storage 3226 location.

If you do not add the sensor to a probe device but to another device in PRTG, be careful with the configuration: Ensure that the IP address or DNS name of the parent device matches the proper sender. For example, if you want to receive syslog or trap messages from a Storage Area Network (SAN), you might have to add a device to PRTG using the IP address of a specific array member that sends the messages. Providing a DNS name that points to the IP address of a whole group might not work for SANs.

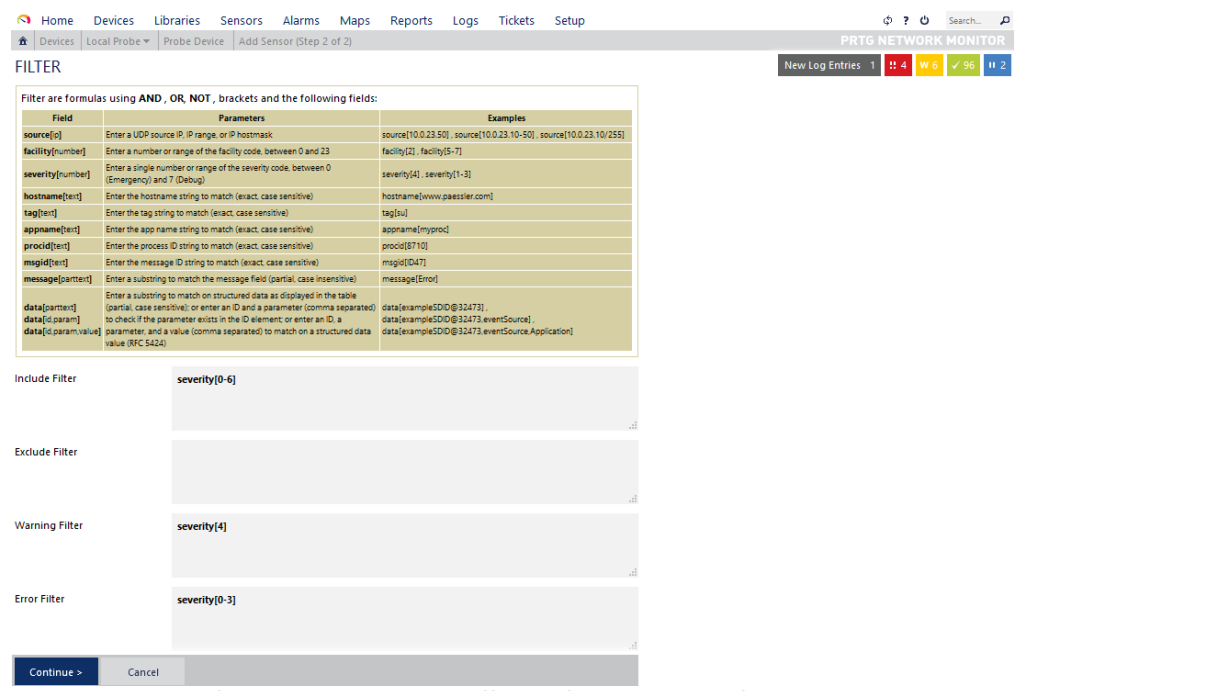


Syslog Receiver Sensor in the Add Sensor Dialog

Step 2: Configure your network device(s) that support sending syslogs or SNMP traps appropriately.
Configure your syslog or SNMP trap ready devices to send syslogs or traps (see the documentation of the respective device vendors). They have to address the PRTG probe where your Syslog or SNMP Trap Receiver sensor runs. So specify the IP address of the machine with the respective PRTG probe. If you keep your syslog or trap receiver's default settings, use the port 514.

The protocol is User Datagram Protocol (UDP).

The SNMP Trap Receiver does not support **SNMP v3** traps. Please use SNMP v1 or v2c instead.

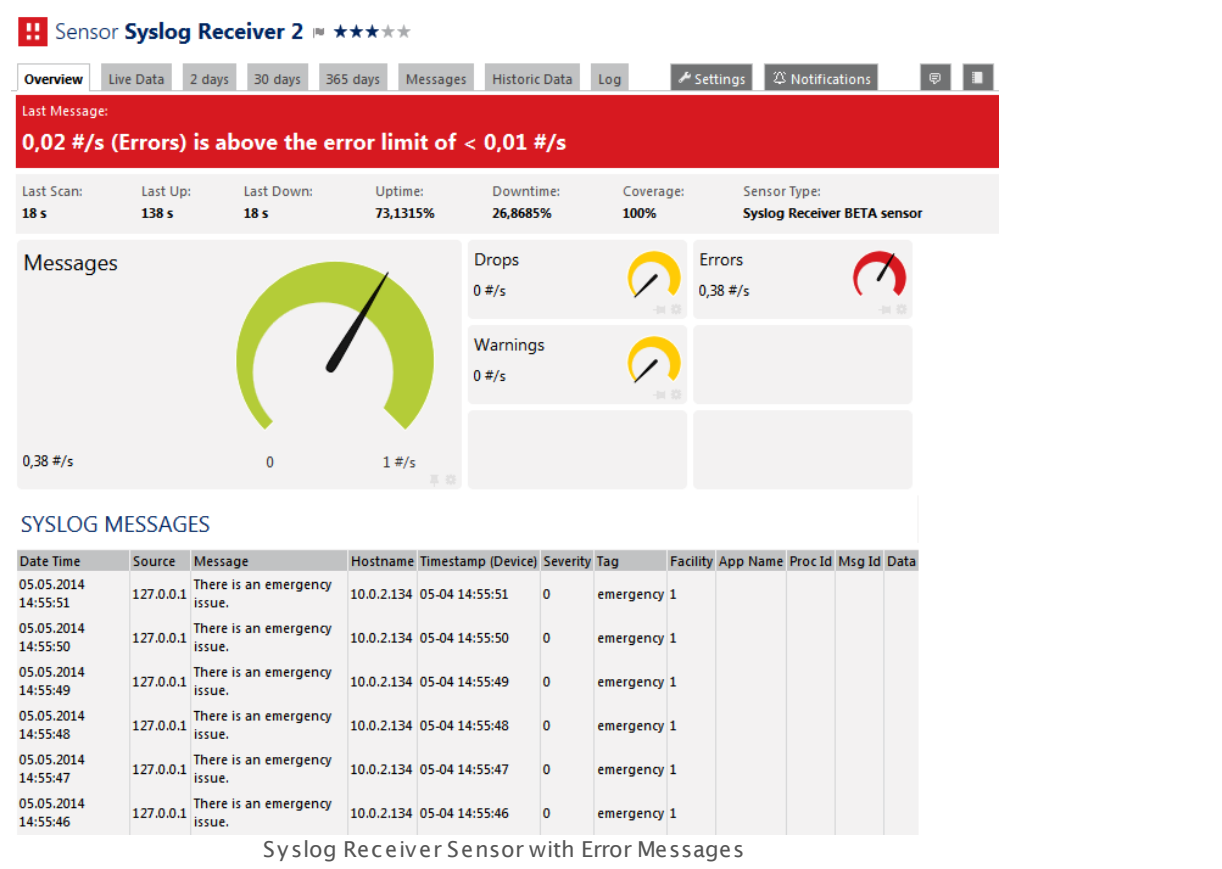


Default Sensor Settings: Sufficient for the First Configuration

Step 3: Start collecting syslog or SNMP trap messages from your devices.
You do not have to complete any further configuration steps to use PRTG as a syslog server or SNMP trap receiver. When your device(s) send syslogs or SNMP traps to the specified PRTG probe machine, the messages appear automatically in the PRTG web interface. After each sensor scan (by default, the scanning interval is inherited from the parent device), PRTG will count the received syslogs or traps in the according channels (total number of messages during the last interval, error and warning messages, or dropped packets).

Let the syslog receiver or the SNMP trap receiver collect data for a while to see what comes in. By default, the respective sensor will go into a **Warning** status if there was at least one message with severity 4 and into an **Error** status if there was at least one message with severity 3 or lower during the last sensor scan.

Incoming messages are counted per scanning interval, so it might take a few moments to see the received syslogs and traps, depending on the remaining time until the next sensor scan. Of course, you can use **Check Now** via the sensor's context buttons [155] to perform an immediate scan and see corresponding data. The sensor states are also defined per scan. So, for example, a message that is classified as an error will count for the error channel only for one scanning interval. If there is no new error message in the following scanning interval, no message is shown in the error channel and the error status will disappear after the next sensor scan. The syslog or trap itself will still be accessible on the **Messages** tab.

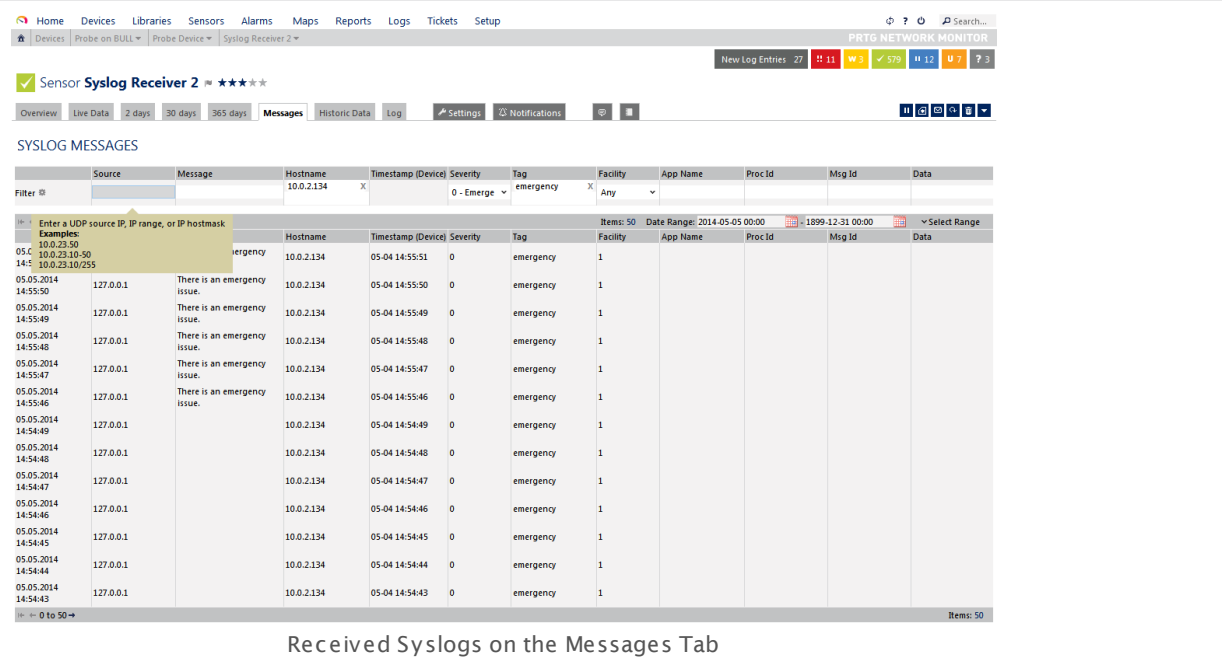


Syslog Receiver Sensor with Error Messages

Step 4: Review and analyze the collected data.
All incoming messages that match the include filter are processed and stored in PRTG's internal high-performance database. Review and analyze the received syslogs and traps via PRTG's web interface. For details, see the respective manual sections of **SNMP Trap Receiver Sensor** [2153] and **Syslog Receiver Sensor** [2319]. Then you can decide about further filtering of the incoming messages.

The received data is also available in PRTG's data folder [3226] as common files. One data file is created per hour.

In PRTG on premises you can add the Management Information Base (MIB) files of your devices to the **\MIB** subfolder to use them with the SNMP Trap Receiver sensor. This will result in Object Identifier (OID) resolution and makes trap messages more comprehensible. For example, instead of the OID 1.3.6.1.4.1.32446.1.1.2 you would see SNMPv2-SMI-v1::enterprises.32446.1.1.2 = 0 (example from the PRTG MIB).



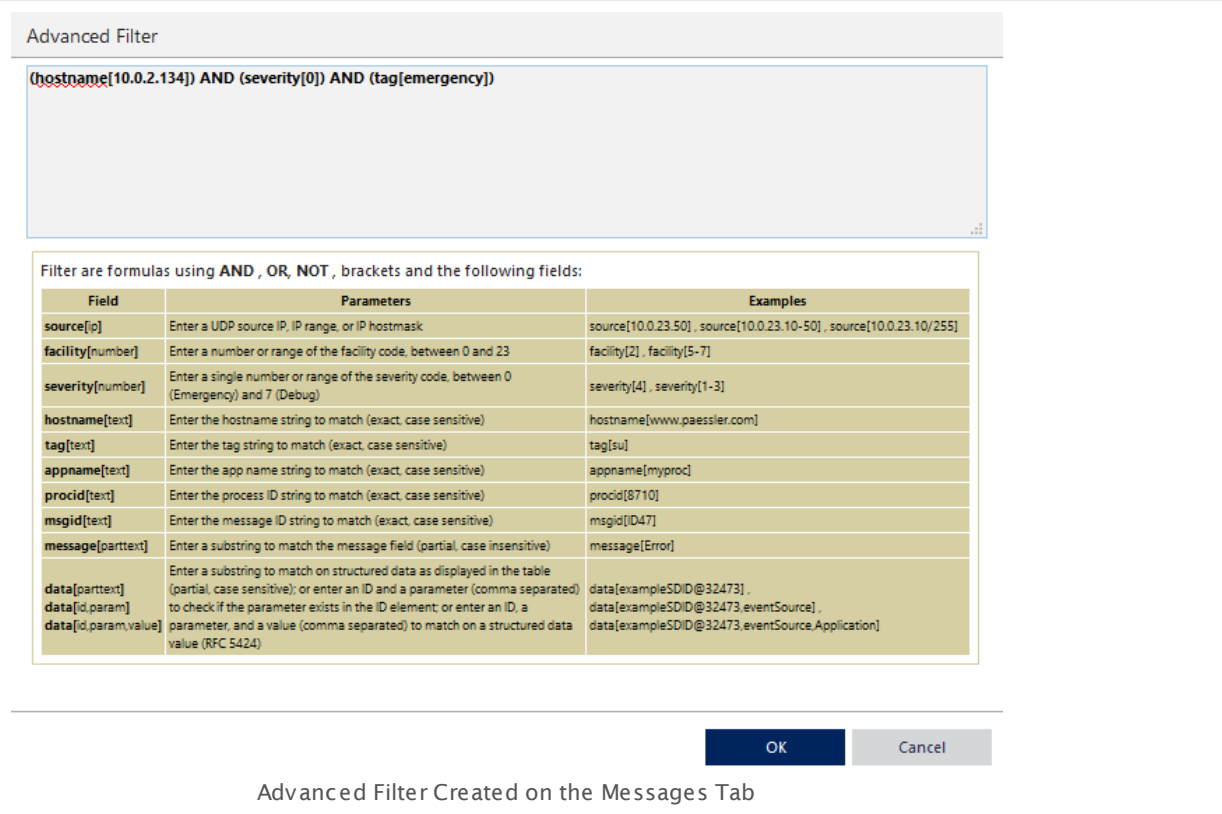
Received Syslogs on the Messages Tab

Step 5: (Optionally) refine the filters.
In order to increase productivity with your PRTG syslog servers and trap receivers, you can adjust the default filter settings. PRTG provides you a comprehensible formula system that you can use to describe what kind of messages you want to process and which of them will count as error or warning messages. You can configure the following filters for received messages in the settings of the respective receiver:

- **Include** filter: Process and store specific types of messages only.
- **Exclude** filter: Do not process specific types of messages and discard them.
- **Warning** filter: Define rules to categorize received messages as warnings.
- **Error** filter: Define rules to categorize received messages as errors.

Use the syntax that is provided in the corresponding manual sections to define your individual filter rules: SNMP Trap Receiver Sensor 2152 and Syslog Receiver Sensor 2318.

You can create filter rules with a few mouse clicks in the **Advanced Filter** on the **Messages** tab of a specific sensor and copy these rules into the sensor settings to apply them.



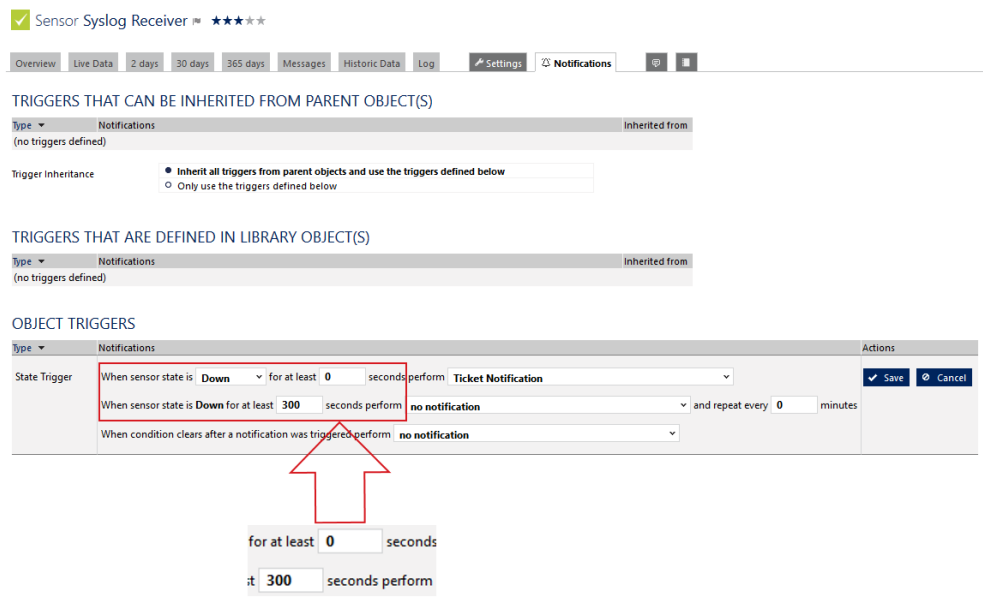
Advanced Filter Created on the Messages Tab

Step 6: (Optionally) create notification triggers.
By default, the warning and error channels of the Syslog and SNMP Trap Receiver sensors have a very low upper warning or error limit (0.00000001). The reason for this is that even when only one syslog or trap has been counted in the respective channel during a scanning interval, the overall status of the sensor will show this with the corresponding status. This way, you always recognize if there is something wrong on the monitored system.

Because of this sensor behavior, best practice would be to add a **State Trigger** on the **Notifications** 2829 tab of the sensor if you want to get a notification 128 when a warning or error message type comes in. Define 0 seconds **Down** or **Warning** time condition to not miss any warnings, errors, or any other messages. Another option would be a **Speed Trigger** for notifications regarding messages per second.

See also this Knowledge Base article: How can I configure sensors using speed limits to keep the status for more than one interval?

You can use syslog and trap specific placeholders in notification templates in order to see the messages when you receive a notification. See the **More** 3131 section below for more information.



State Trigger for a Syslog Receiver

Click here to enlarge: https://media-s3.paessler.com/prtg-screenshots/syslog_howto7_notification.png

More

Knowledge Base: How can I configure sensors using speed limits to keep the status for more than one interval?

- https://kb.paessler.com/en/topic/73212

Knowledge Base: What placeholders can I use with PRTG?

- https://kb.paessler.com/en/topic/373

Part 12

PRTG Administration Tool

12 PRTG Administration Tool

The **PRTG Administration Tool** is part of your PRTG installation and helps you edit administrative settings of your local probe and your remote probe installations.

You can launch the PRTG Administration Tool from the Windows start menu, on your core server, or on your remote probe server. If you start the PRTG Administration Tool on the PRTG core server, you can change settings that affect your whole PRTG installation and your local probe. If you run the PRTG Administration Tool on a system on which a remote probe runs, you can only change settings that are related to this probe.

All settings that you change will require a restart of the affected PRTG Windows services to apply any changes on the configuration. Please see the following sections for details.

You can also change many administrative settings via the **Setup** 2907 in the PRTG web interface 136. For probes, settings are also available on the corresponding tab 330 in the web interface.

You can review the history of all changes to the settings of the PRTG Administration Tool in the **Logs (Debug)** directory. The name of the corresponding logfile is **PRTG Administration Tool Changelog.log**. For information on how to find the folder used for storage, please see section **Data Storage** 3226.

More

Video Tutorial: The PRTG Administration Tool

- https://www.paessler.com/support/videos/prtg-basics/administration-tool

PRTG Administration Tool—Topics

- **PRTG Administration Tool on Core Server System** 3135
- **PRTG Administration Tool on Remote Probe System** 3157

Related Topics

- **Setup** 2907
- **Failover Cluster Step by Step** 3219

12.1 PRTG Administration Tool on Core Server System

With the **PRTG Administration Tool** you can define various system-oriented settings that affect your PRTG installation, as well as restart services and view log information. You can also change many of these settings via the system administration 2907 in the PRTG web interface 136.

This section describes the available settings in the PRTG Administration Tool when you open the tool on the PRTG core server system. This means that you can edit settings that regard your PRTG core or web server and the local probe, which is the probe on your core server. If you open the PRTG Administration Tool on a remote probe machine, only probe related settings 3157 are available.

All settings you define are only valid for the local installation that is running on the computer on which you start the Administration Tool. In order to change settings for another installation, for example, another cluster node installation, please log in to that computer and open the program there.

Do you want to know how the PRTG Administration Tool relates to all other major parts of PRTG Network Monitor? To get familiar with the different components of PRTG, we recommend that you read the **Architecture** 111 section. If you prefer a video introduction to the **PRTG Administration Tool**, see the **More** 3156 section below for more information.

This feature is not available in PRTG on demand.

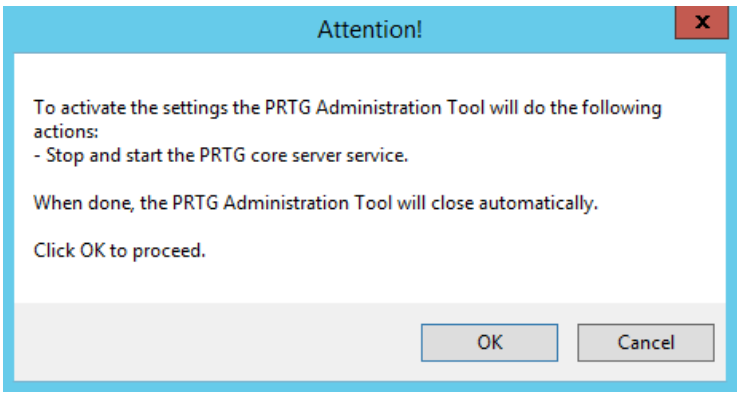
Start the PRTG Administration Tool

From the Windows start menu, select the **PRTG Network Monitor** group and click **PRTG Administration Tool** to open the application.

You can choose from these options in different tabs:

- Web Server 3136
- Core Server 3139
- Cluster 3141
- Administrator 3146
- Probe Settings for Core Connection 3148
- Probe Settings for Monitoring 3150
- Service Start/Stop 3151
- Logs and Infos 3154

After you change settings, click the **Save & Close** button. A new window opens where PRTG asks you to agree to restart the PRTG core server service. Click **OK** if you do not want your changes to be ignored.

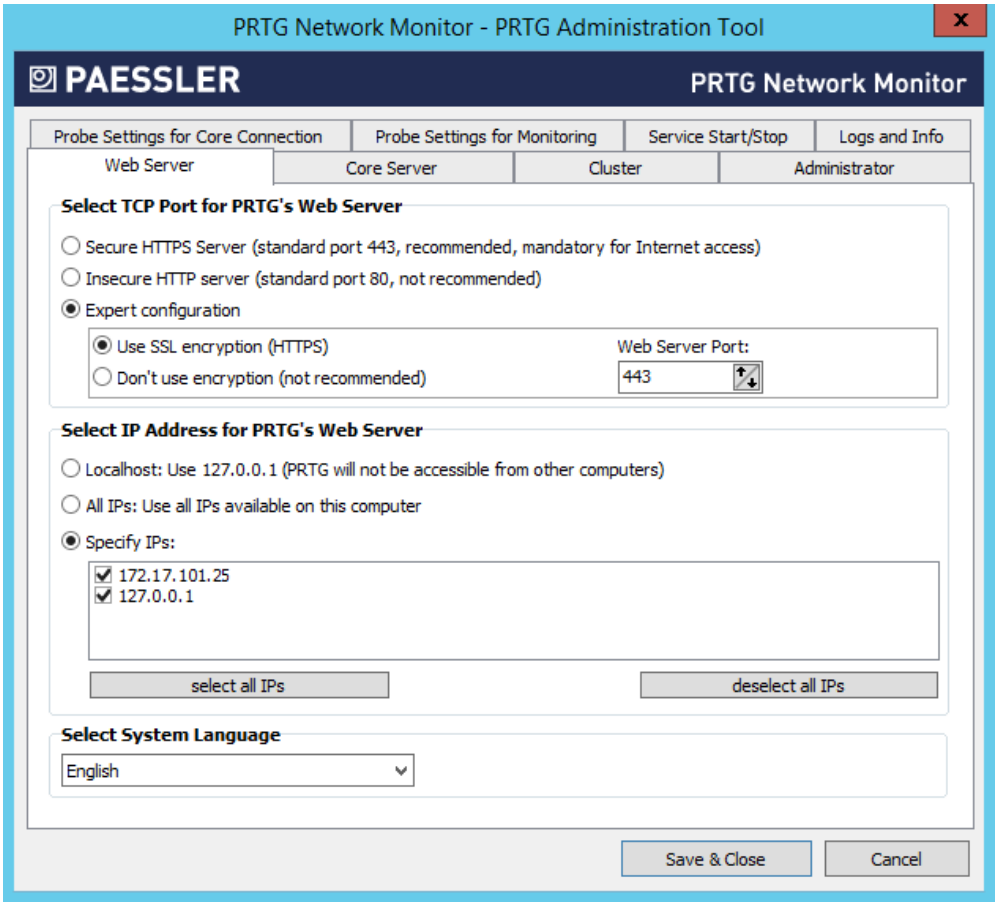


PRTG Administration Tool: Restart Services

Web Server

Edit IPs, ports, access methods, and language for the PRTG web interface 136.

You can also change all settings on the **Web Server** tab via the PRTG web interface in the User Interface 2943 settings.



PRTG Administration Tool

WEB SERVER

Select TCP Port for PRTG's Web Server

PRTG runs a web server in order to provide access via the web interface and the Enterprise Console. Please specify on which port this web server will run. Choose between:

- **Secure HTTPS server (recommended, mandatory for internet access)**: We recommend this setting and you need it to access the PRTG server via the internet. Use a secure HTTPS connection that is encrypted via SSL on port 443.
  Although the connection is secure, you will see an **SSL Certificate Warning** 142 in your browser when logging in to the PRTG web interface, because the default certificate is unknown to your browser. You can install another SSL certificate for PRTG later. Please see **Using Your Own SSL Certificate** 3228.

  If port 80 is free, PRTG will reserve it as well. When users try to connect on port 80 via HTTP, they will then be redirected to port 443 via HTTPS. You can change this behavior by using a registry setting.
  If port 443 is not available, PRTG will try port 8443 as fallback. If this port is also not available, PRTG searches from port 32000 upwards for a free port. PRTG will send a ticket 200 that shows you the currently used port number and will switch back to 443 as soon as it is available again.
- **Insecure HTTP server (standard port 80, not recommended)**: Use a standard web server without SSL encryption on port 80. This setting is not recommended for WAN connections.
  If you use an insecure web server on the internet, attackers could potentially spy on credentials you enter into PRTG. We strongly recommend that you use this option in a LAN only.
- **Expert configuration**: This setting allows you to specify a custom web server port and the security of the connection. This option is intended for systems with an existing web server on the standard port. Define port and encryption below.
  If PRTG always uses a fallback port after a server restart, check for other programs that use the same port as PRTG. For example, the Microsoft IIS web server also uses the port 80 (443 for SSL) by default and blocks it. Please disable such programs and services on startup.

Expert Configuration: SSL Encryption

You will see this setting only if you select **Expert configuration** above. Specify if you want to use an SSL encryption. Choose between:

WEB SERVER

- **Use SSL encryption (HTTPS)**: Use a secure HTTPS connection that is encrypted via SSL on a custom port as defined above.
  Although the connection is secure, you will see an SSL Certificate Warning 142 in your browser when you log in to the PRTG web interface, because the default certificate is unknown to your browser. You can install another SSL certificate for PRTG later. Please see Using Your Own SSL Certificate 3228.
- **Don't use encryption (not recommended)**: This setting is not recommended for WAN connections. Use a standard web server without SSL encryption on a custom port as defined above.

If you use a web server without encryption on the internet, attackers could potentially spy on credentials you enter into PRTG. We strongly recommend that you use this option in a LAN only.

Expert Configuration: Web Server Port

You will see this setting only if you select **Expert configuration** above. Enter the TCP port number you want the PRTG web server to run on. Please enter an integer value.

If you use a secure connection and port 80 is free, PRTG will reserve it as well. When users try to connect on port 80 via HTTP, they will be redirected to the custom port via HTTPS. You can change this behavior by using a registry setting.

If the defined port for a secure connection is not available, PRTG will try port 8443 as fallback. If this port is also not available, PRTG searches from port 32000 upwards for a free port. PRTG sends a ticket 200 that shows you the currently used port number and will switch back to the original port as soon as it is available again.

Select IP Address for PRTG's Web Server

PRTG is running a web server in order to provide access via the web and Windows interface. Please specify the IP address this web server will run on. Later, you can log in to PRTG by simply pointing your browser to the specified IP address.

Choose between:

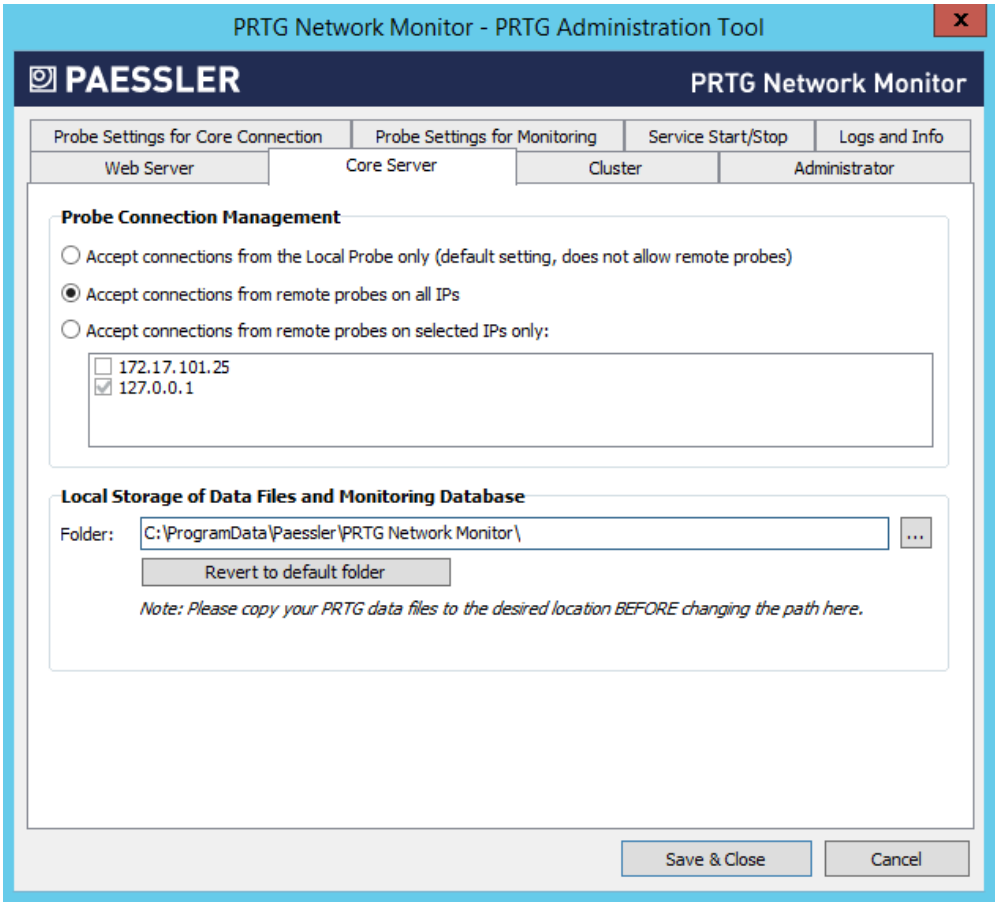
- **Localhost, 127.0.0.1 (PRTG will not be accessible from other computers)**: Use 127.0.0.1 only. The PRTG web interface and the Enterprise Console will only be accessible from the computer PRTG is installed on. Either the selected port or at least one port in the range from **8080** to **8089** has to be available on 127.0.0.1.

If you run PRTG on localhost, please do not use the DNS name http://localhost to log in to the web server, as this may considerably slow down the PRTG web interface. Please use your local IP address or http://127.0.0.1 instead.

WEB SERVER	
	▪ **All IPs available on this computer**: Use all IP addresses available on this computer and enable access to the web server for all of these addresses. The TCP port selected below must be free on every available IP address. ▪ **Specify IPs**: Select specific IP addresses on which the PRTG Web server will run. A list specific to your system is shown. Add a check mark in front of every IP address you want the PRTG web server to be available at. You can also select and deselect all addresses by clicking on the check box in the table header. Either the selected port or at least one port in the range from **8080** to **8089** has to be available on the specified IP address. Regardless of the selected setting above, one port in the range from **8080** to **8180** has to be available on the specified IP address so PRTG can create reports. The report engine will try to connect to the core server on one of these ports. If PRTG does not find a network card on startup it will switch the IP setting to **Localhost**. This setting will remain, even if a network card is available later on. If you disabled or removed the network card on the machine running the PRTG core server, please re-check this setting.
Select System Language	Choose the system language from the dropdown list. Default is **English**. Depending on your installation, you may be able to choose other languages here. This setting defines the language of the PRTG web interface 136, as well as of the **PRTG Administration Tool** 3134.

Core Server

Define settings for the core server.



PRTG Administration Tool: Core Server

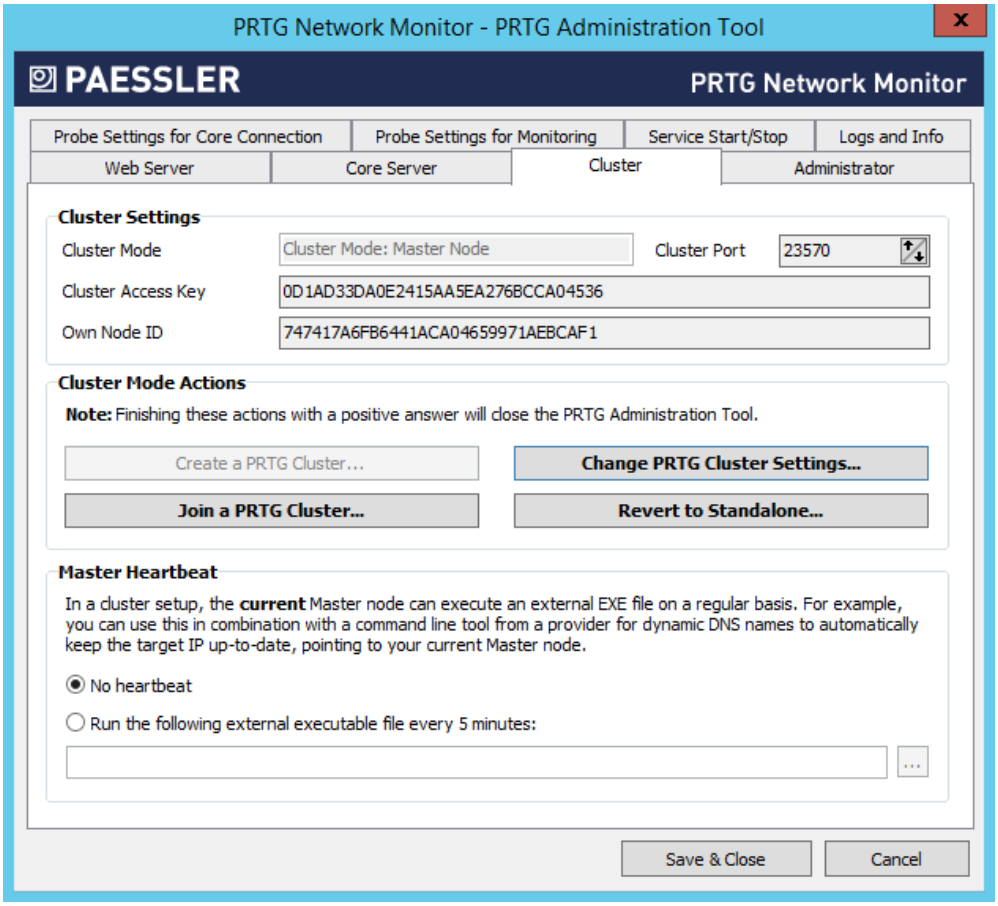
CORE SERVER

Probe Connection Management	Define how PRTG will handle incoming connections from probes. Choose between the following options: ▪ **Accept connections from the Local Probe only (default setting, does not allow remote probes)**: This is the default setting. Only local probe connections will be accepted by the PRTG core server. You cannot use remote probes 3195 with this setting enabled. ▪ **Accept connections from remote probes on all IPs**: Incoming connections from remote probes will always be accepted, no matter on which IP address of the core server they come in. ▪ **Accept connections from remote probes on selected IPs only**: Incoming connections from remote probes 3206 will only be accepted on the selected IP address(es) of the core server. In the list, select the IP addresses by adding a check mark in front of the desired IPs.

CORE SERVER	
	You can also change this setting in the PRTG web interface under **System Administration—Core & Probes** 2968.
Local Storage of Data Files and Monitoring Database	Define the data folder to which PRTG will store configuration and monitoring data. Click the **...** button to choose another folder on your system. Before you change the path, make sure you stop both the core server and the probe services and copy all data to the new location. Click **Revert to default folder** to reset to default.

Cluster

On the **Cluster** tab, you can manually change how the current core installation will behave in a cluster. Before changing settings here, please read the **Failover Cluster Configuration** 3212 section.



PRTG Administration Tool: Cluster

CLUSTER

Cluster Settings

Depending on the current cluster settings, you will see different information here.

- **Cluster Mode**: Shows which cluster mode the current installation is running. This setting is shown for your information only and cannot be changed here. Possible values are **Standalone** (no cluster mode), **Cluster Mode: Master Node**, or **Cluster Mode: Failover Node**.
- **Cluster Port**: This field is only shown when PRTG is running in a cluster mode. This setting is shown for your information only and cannot be changed here.
- **Cluster Access Key**: This field is only shown when PRTG is running in a cluster mode. This setting is shown for your information only and cannot be changed here.

CLUSTER

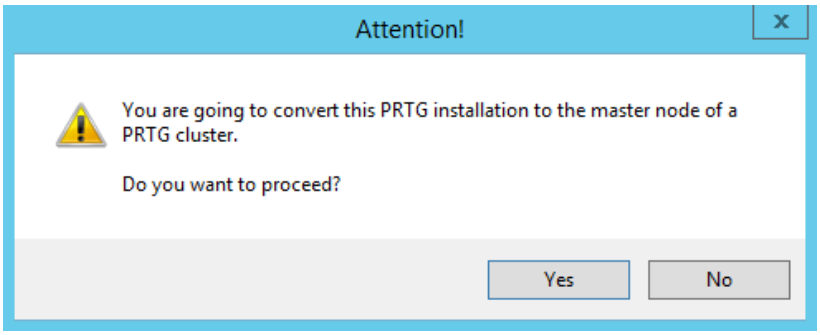
	▪ **Own Node ID**: This field is only shown when PRTG is running in a cluster mode. This setting is shown for your information only and cannot be changed here.
Cluster Mode Actions	Depending on the current cluster settings, you see different active buttons here. ▪ **Create a PRTG Cluster...** ▪ **Join a PRTG Cluster...** ▪ **Change PRTG Cluster Settings...** ▪ **Revert to Standalone...** For details on these options, please see below this table 3143.
Master Heartbeat	This section is only visible if you are running your PRTG installation in cluster mode. The current master can execute an external executable file on a regular basis. We call this a "heartbeat". You can use this, for example, to report the IP address of the current master node to a dynamic DNS provider, so a DNS name is always redirected to the current PRTG master node in case the original master node fails and a failover node (running at a different IP address) takes over the master role. Choose between: ▪ **No heartbeat:** Do not execute a file on a regular basis. ▪ **Run the following external executable file every 5 minutes:** Click the **...** button to choose a file you want to execute. This can be, for example, a command line tool, or a batch file. It will be executed on the current master node only, with a fixed interval of five minutes. The interval cannot be changed. Please make sure that the selected file is available under the same (local) path on all failover nodes. In case one of your failover nodes becomes current master, the heartbeat can only be executed reliably if the executable file exists on all of your failover nodes.

Cluster Mode Actions

Follow these instructions to create or join a cluster, to change a cluster's settings, or to revert a cluster node to a standalone PRTG installation:

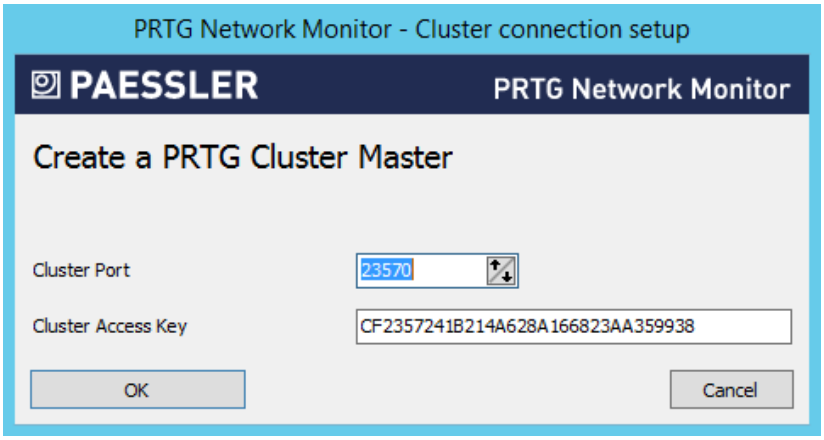
Create a PRTG Cluster...

- Click this button to start creating a cluster. The current PRTG core server will then be the **Master Node** of your cluster.
- Click **Yes** to confirm the conversion of this installation into a cluster master node.



Converting an Installation into a Cluster Master Node

- A new dialog box will appear.



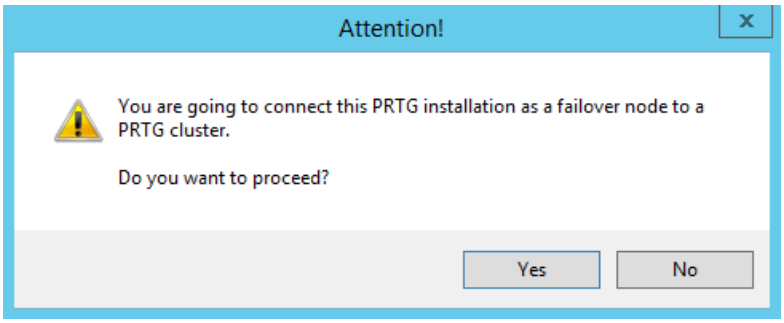
PRTG Administrator: Creating a Cluster Master

- Enter a **Cluster Port**. This is the port on which the internal communication between the different cluster nodes is sent. Make sure connections between cluster nodes are possible on the selected port.
- Enter or paste a **Cluster Access Key**. This is a unique access key. All nodes in a cluster have to be configured with the same cluster access key in order to join the cluster. Connection attempts with the wrong access key will be rejected.
- We recommend that you use the default value.
- Save the **Cluster Access Key** so you have it at hand when configuring your **Failover Node (s)**.
- After confirming your settings you will be asked to restart Windows services. Please do so in order for your changes to take effect.

Join a PRTG Cluster...

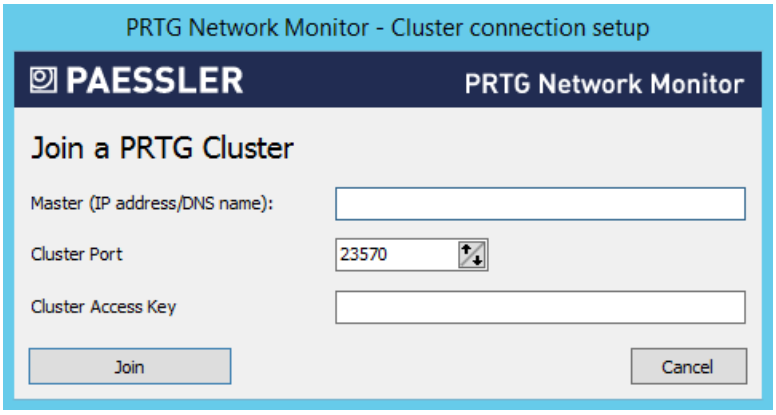
- Click this button to add this installation to an existing cluster that already has a **Master Node**. The current PRTG core server will then be a **Failover Node** in the cluster.

- This button is also available if you are currently running your PRTG installation in **Cluster Mode: Master Node**. This option will then change your master node to a failover node!
- Click **Yes** to confirm the conversion of this installation into a failover node.



Converting an Installation into a Cluster Failover Node

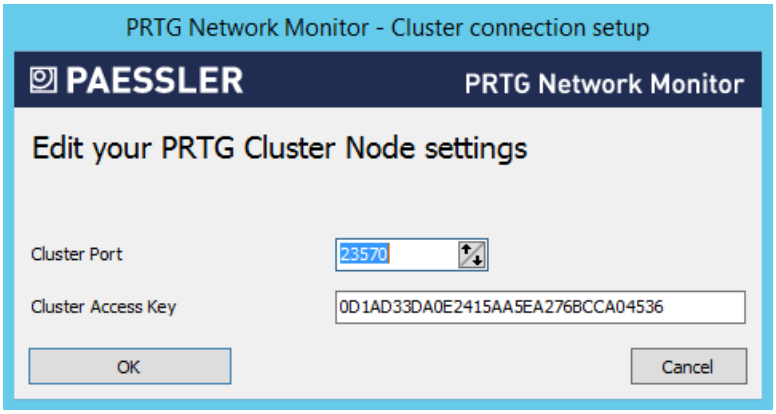
- A dialog box will appear.



PRTG Server Administrator

- Enter a **Master IP address/DNS name** for your cluster. It must be reachable from the machine running the failover node.
- Enter the other settings as defined in the settings of your **Master Node.** Please make sure you use the same settings on all nodes in your cluster.
- Enter a **Cluster Port**. This is the port on which the internal communication between the different cluster nodes is sent. Make sure connections between cluster nodes are possible on the selected port.
- Enter or paste a **Cluster Access Key**. This is a unique access key. All nodes in a cluster have to be configured with the same cluster access key in order to join the cluster. Connection attempts with the wrong access key will be rejected.
- After confirming your settings you will be asked to restart Windows services. Please do so in order for your changes to take effect.

Change PRTG Cluster Settings...



PRTG Server Administrator

- If you are running your PRTG installation in cluster mode, you can change the settings here. A new window will appear.
- Enter a **Cluster Port**. This is the port on which the internal communication between the different cluster nodes is sent. Make sure connections between cluster nodes are possible on the selected port.
- Enter or paste a **Cluster Access Key**. This is a unique access key. All nodes in a cluster have to be configured with the same cluster access key in order to join the cluster. Connection attempts with the wrong access key will be rejected.
- Please make sure you use the same settings on all nodes in your cluster.
- After confirming your settings you will be asked to restart Windows services. Please do so in order for your changes to take effect.

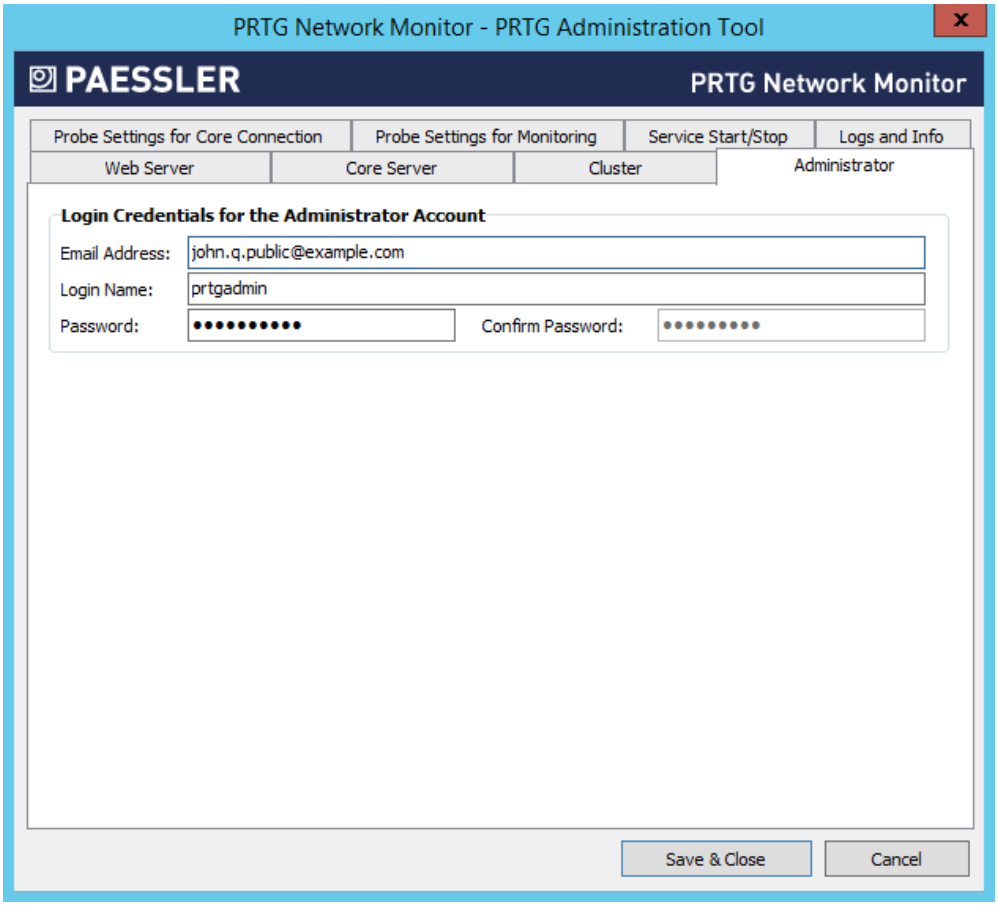
Revert to Standalone...

- If you are currently running your PRTG installation in cluster mode, you can change it to **Standalone** mode. If you do so, this node will no longer be part of a cluster.
- After confirming your settings you will be asked to restart Windows services. Please do so in order for your changes to take effect.

Administrator

Change PRTG System Administrator specific settings.

You can also change these settings in the account settings 2976 of the **PRTG System Administrator** user in the PRTG web interface.



PRTG Administration Tool: Administrator

LOGIN CREDENTIALS FOR THE ADMINISTRATOR ACCOUNT

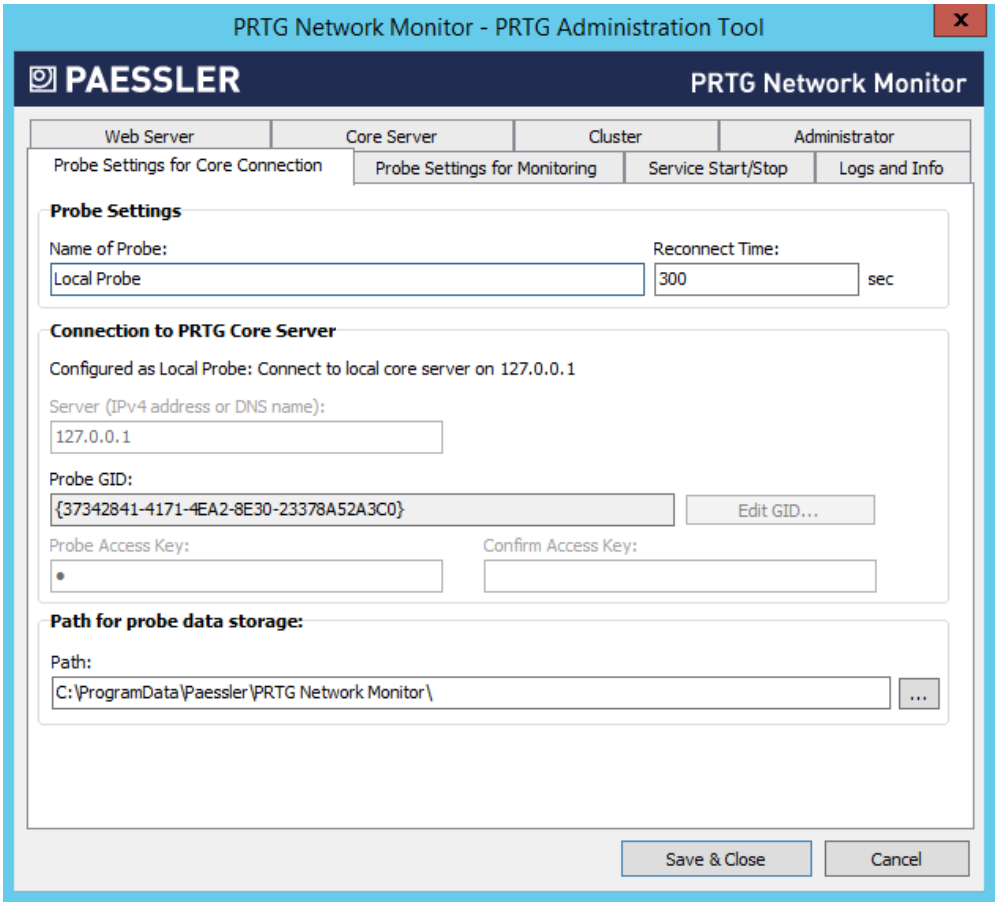
Email Address	Enter a valid email address for the administrator. By default, PRTG will send notifications and important messages to this address.
Login Name	Enter a name for the **PRTG System Administrator** login. This is your default login! You use it when you log in to the PRTG web interface or Enterprise Console. ⓘ The default login name is **prtgadmin.**
Password	Enter a password for the **PRTG System Administrator** login. This is your default login! You use it when you log in to the PRTG web interface or Enterprise Console. ⓘ The default password is **prtgadmin.**

LOGIN CREDENTIALS FOR THE ADMINISTRATOR ACCOUNT

Confirm Password	If you change your password, re-enter the password for the **PRTG System Administrator** login to confirm it.

Probe Settings for Core Connection

Define general settings regarding the probe and probe connections.



PRTG Administration Tool: Probe Settings for Core Connection

PROBE SETTINGS

Name of Probe	Enter a meaningful name to identify the probe. PRTG shows this name, for example, in the device tree, and in all alarms by default. Please enter a string.

PROBE SETTINGS

Reconnect Time	Define the time that PRTG will wait until the probe tries to reconnect to the core server if the connection fails. Please enter an integer value.

CONNECTION TO PRTG CORE SERVER

These settings affect the way the probe will connect to the core server. A probe is either a local probe or a remote probe. PRTG will automatically detect the type of probe and show the correct setting options.

Server (IPv4 address or DNS name)	If this probe is configured as the **Local Probe** of the PRTG core installation, it will connect to the core via 127.0.0.1, which you cannot change. If this probe is configured as a **Remote Probe**, enter the IP address or DNS name of the core server.
Probe GID	The **Probe GID (global ID (GID))** is a unique identifier for the probe. We recommend that you do not change it. Exception: Only if you substitute an existing remote probe from a different computer, you have to copy the GID from the old probe to the new probe. To do so, click the **Edit GID...** button and confirm the warning with **Yes**. You can then change the value. You cannot change the GID for a local probe. You can deny GIDs under **System Administration—Core & Probes** 2968 in the PRTG web interface. If you remove a remote probe from the device tree or if you deny a remote probe after installation 98, its global ID (GID) will be automatically entered in the **Deny GIDs** list.
Probe Access Key	You do not need an access key for **Local Probe** connections. On a **Remote Probe**, the **Probe Access Key** must match one of the access keys configured in your PRTG core server installation. If it does not match, the remote probe will not be able to connect to the core server. Please see the **System Administration—Core & Probes** 2968 section for more information. Check also allowed and denied IPs in **System Administration—Core & Probes** 2968 to ensure that the core server accepts the IP address of the remote probe.
Confirm Access Key	If you enter an access key for a remote probe, enter it in this field again to assure correctness.

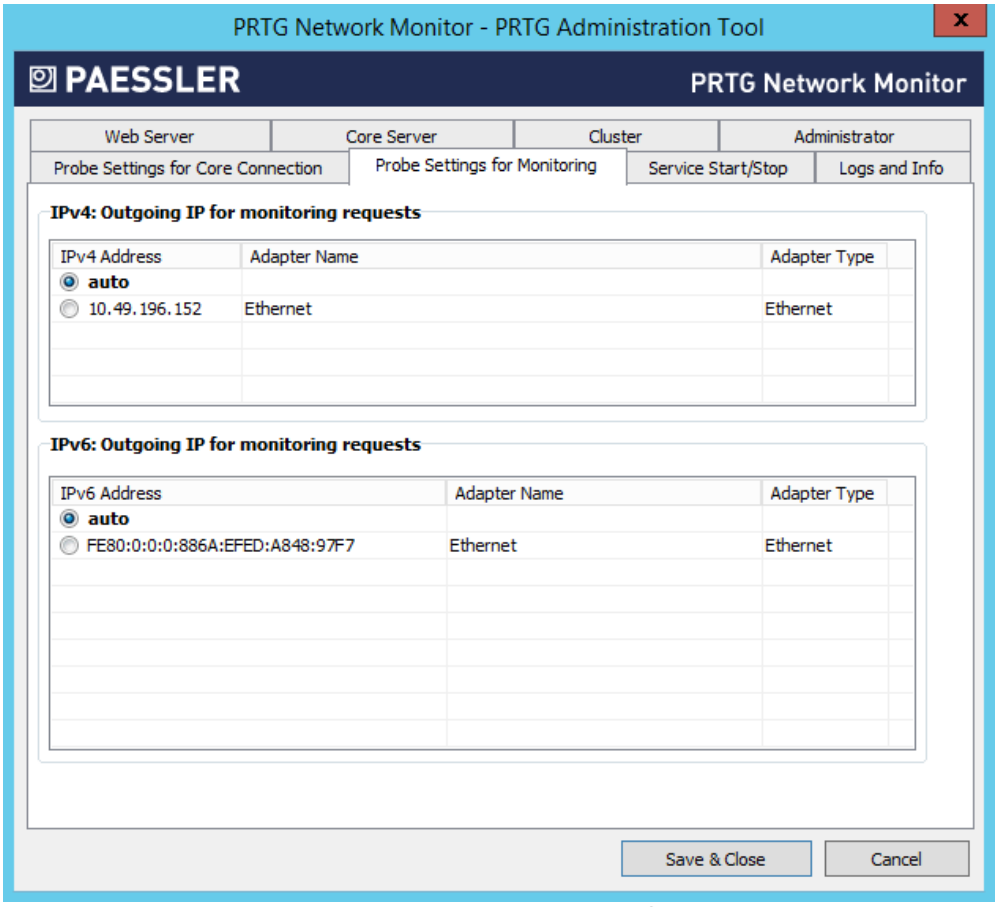
PATH FOR PROBE DATA STORAGE

Path	Define the data folder to which PRTG will store configuration and monitoring data. Click the **...** button to choose another folder on your system. Before you change the path, make sure you stop both the core server and the probe services and copy all data to the new location.

LANGUAGE FOR THE PRTG ADMINISTRATION TOOL FOR REMOTE PROBES

<your language>	Choose the language for the PRTG Administration Tool on your remote probe from the dropdown list. Default is **English**.

Probe Settings for Monitoring



PRTG Administration Tool: Probe Settings for Monitoring

PROBE SETTINGS FOR MONITORING

Define the IP address used for outgoing monitoring requests.

- If there is more than one IP on the current system available, you can specify the IP address that PRTG will use for outgoing monitoring requests of certain sensor types.
- This setting will be used for sensors using the following connection types: HTTP, DNS, FTP, IMAP, POP3, Port, Remote Desktop, SMTP, and SNMP.
- The setting is valid for all monitoring requests sent from this PRTG probe.
- This setting is useful for devices that expect a certain IP address when queried.
- Default setting is **auto**. PRTG will select an IP address automatically.

This feature does not support all sensor types for technical reasons.

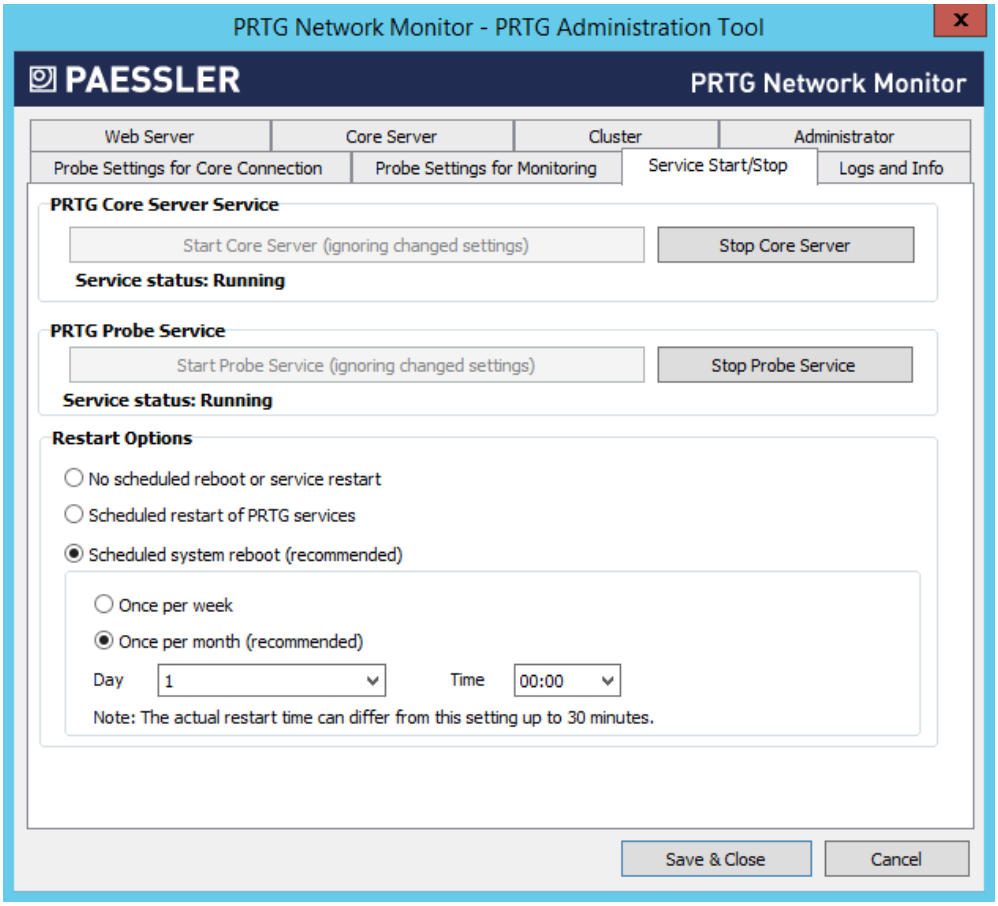
If you change this setting, some sensors might stop working. For example, sensors might show a **Down** status if the selected IP address is blocked on the way to or directly on the monitored device.

Outgoing IPv4	Define the IP address for outgoing requests using the IPv4 protocol. The list shows all IP addresses available on the current system. Choose a specific IP address or select **auto**.
Outgoing IPv6	Define the IP address for outgoing requests using the IPv6 protocol. The list shows all IP addresses available on the current system. Choose a specific IP address or select **auto**. For details about the basic concept of IPv6 in PRTG, please see the **IPv6** 133 section.

Service Start/Stop

You can stop and start PRTG Windows services manually. For connected probes, click **Start Core Server** to start the service or **Stop Core Server** to stop it. Both actions usually take from a few seconds up to several minutes to complete. You can also restart the core server and connected probes via the PRTG web interface under **Administrative Tools** 2988.

We recommend that you set a schedule for automatic system restarts.



PRTG Administration Tool: Start and Stop Service

You can also define a restart schedule on the **Settings** tab of a probe under **Restart Options**, in the PRTG web interface.

SCHEDULED RESTART SETTINGS

This setting is not available for local probes in PRTG on demand.

Restart Options	For best performance, we recommend that you regularly restart the Windows servers on which PRTG is running. To do this automatically for PRTG, you can schedule an automatic restart. Choose between the following options:

SCHEDULED RESTART SETTINGS

- **No scheduled reboot or service restart**: Do not perform any scheduled restart of services automatically. We recommend a manual restart every few weeks. You can initiate a restart of your PRTG core server and probes under **System Administration—Administrative Tools** 2987 in the PRTG web interface.
- **Scheduled restart of PRTG services**: Restart all PRTG services on the system where this probe runs on. If you choose this option on the local probe, the PRTG core server will restart as well. Define a schedule below.
- **Scheduled system reboot (recommended)**: We recommend this setting, although it is not set by default. Enter a schedule below. We recommend that you restart Windows servers once a month for best performance.

Restart Schedule

You can only see this setting if you selected a schedule option above. Choose how often you want to restart PRTG services or the Windows server:

- **Once per week**: Select a day of the week and a time below.
- **Once per month (recommended)**: Select a day of the month and a time below.

Specify Day

You can only see this setting if you selected a schedule option above. Select a specific day of a week (Monday to Sunday) or month (1st to 30th or Last). If you select **Last**, the restart will always be executed on the last day of the month, regardless of how many days the month has.

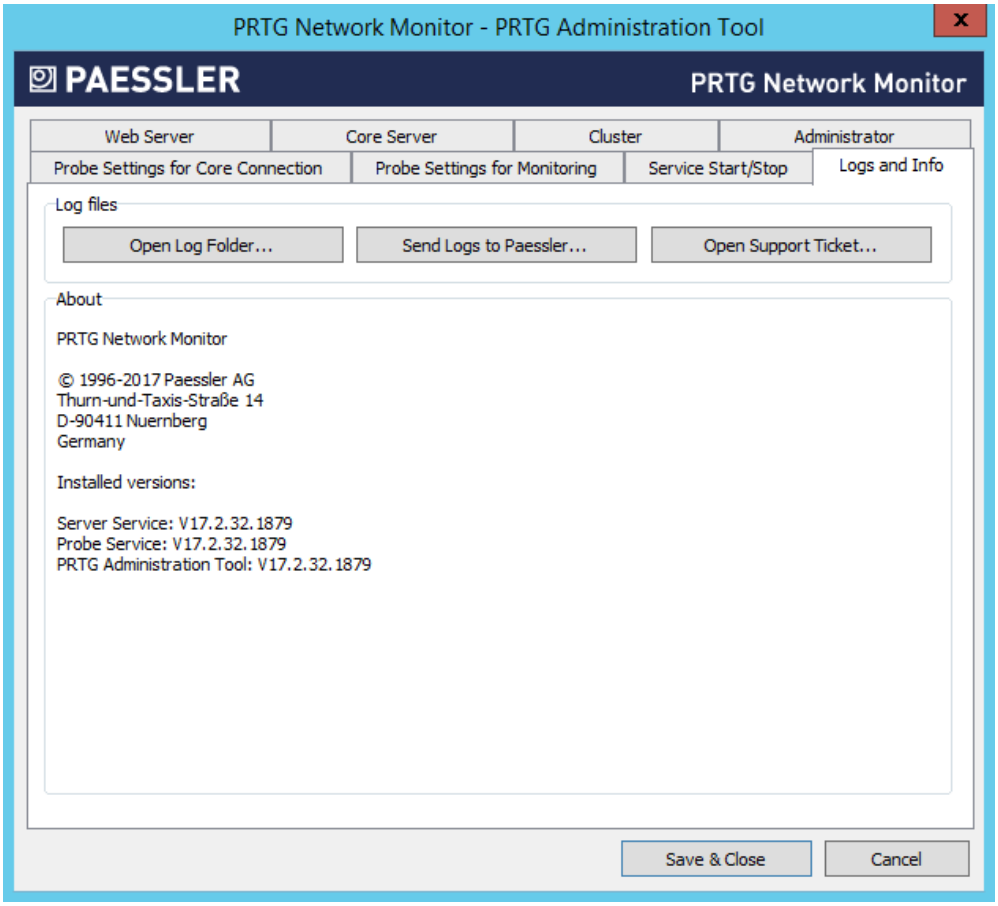
ⓘ If you select a date that does not exist in every month (for example, the 30th day in February), PRTG will automatically initiate the restart on the last day of this month.

Specify Hour

You can only see this setting if you selected a schedule option above. Select the time of day when PRTG will perform the restart.

ⓘ You will get a Windows warning message 10 minutes before the restart to inform you if you are a currently logged in user. The actual restart time can differ up to 30 minutes from the settings you enter here.

Logs and Info



PRTG Administration Tool: Logs and Info

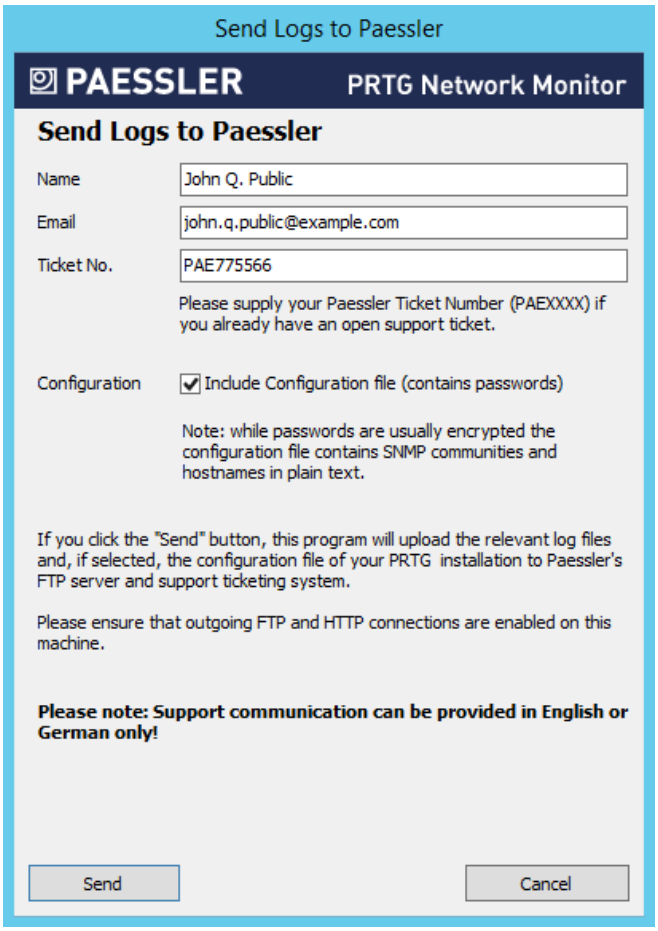
LOG FILES

Open Log Folder...	Open the PRTG Network Monitor data directory on your hard disk drive to access all logfiles that PRTG creates.
Send Logs to Paessler...	Open an assistant to send logfiles to the Paessler support team. Please see below for details 3166.
	You can send logfiles more easily with the support bundle via **Contact Support** 3024 in the PRTG web interface.
Open Support Ticket...	This will open the support form on the Paessler website in a browser window.
	If you need help, we recommend that you use the **Contact Support** 3024 option in the PRTG web interface instead.

The **About** section shows information about the version of installed PRTG programs and copyright.

Send Logs to Paessler

You can send logfiles more easily with the support bundle via **Contact Support** 3024 in the PRTG web interface.



Send Logs to Paessler

If you open a support ticket, Paessler support might ask you to send logfiles for further analysis. With the **Send Logs to Paessler...** button, PRTG will automatically collect, compress, and send your logfiles to our FTPS server.

SEND LOGS TO PAESSLER

Name	Enter your name.

SEND LOGS TO PAESSLER

Email	Enter a valid email address. You can provide any of your addresses, but we recommend that you use the email address of your PRTG account, which is entered by default.
Ticket No.	This field is optional. If you have already opened a ticket at Paessler support, please provide the ticket number you received. Your files will then be associated with your ticket automatically. Please enter the ticket number starting with PAE followed by four or more digits, for example, PAE12345. If you do not have a ticket number, leave this field empty.
Configuration	Define if you want to include the configuration file in the data. PRTG will remove all passwords from the config file before sending it to our support team.

Click the **Send** button to start the data upload. Ensure that FTPS and HTTP connections are allowed on this machine.

More

Video Tutorial: The PRTG Administration Tool

- https://www.paessler.com/support/videos/prtg-basics/administration-tool

Knowledge Base: Which ports does PRTG use on my system?

- https://kb.paessler.com/en/topic/61462

12.2 PRTG Administration Tool on Remote Probe Systems

If you start the **PRTG Administration Tool** on a system on which a PRTG **Remote Probe** 3196 runs, you can define various probe related settings, restart services, and view log information. You can also change many of these settings via the system administration 2907 and the probe settings tab 330 in the PRTG web interface 136.

This section describes the available settings in the PRTG Administration Tool when you open the tool on a PRTG remote probe system. This is not the complete set of available settings. If you need access to all possible settings regarding your whole PRTG installation, open the PRTG Administration Tool on the PRTG core server machine.

All settings you make here are valid only for the local installation running on the computer on which you open the PRTG Administration Tool. In order to change settings for another installation, for example, another remote probe installation, please log in to that computer and open the program there.

To get familiar with the different components of PRTG, we recommend that you read the **Architecture** 111 section. If you prefer a video introduction to the **PRTG Administration Tool**, see the **More** 3156 section below for more information.

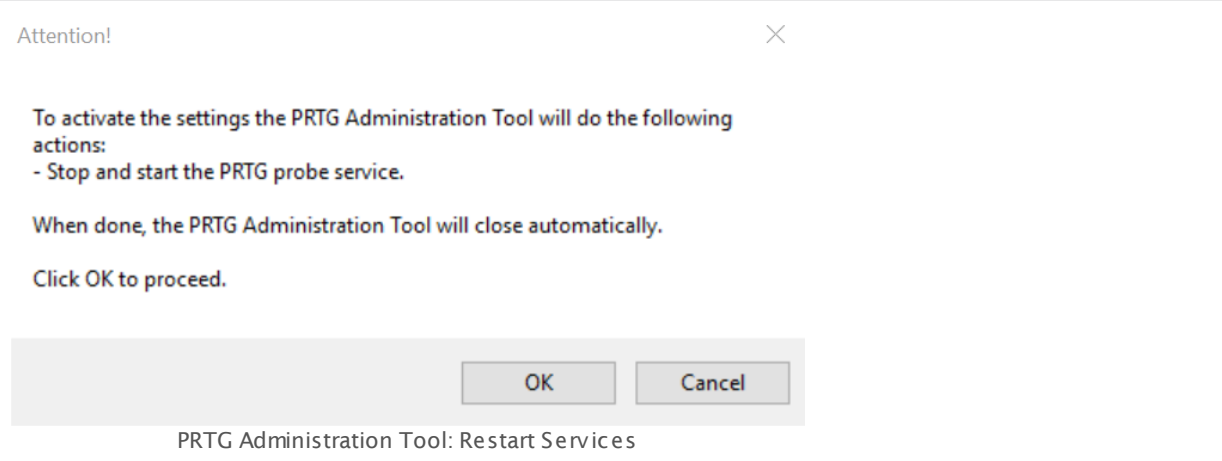
Start the PRTG Administration Tool

From the Windows start menu, select the **PRTG Network Monitor** group and click **PRTG Administration Tool** to open the application.

You can choose from these options in different tabs:

- Probe Settings for Core Connection 3158
- Probe Settings for Monitoring 3161
- Service Start/Stop 3162
- Logs and Infos 3165

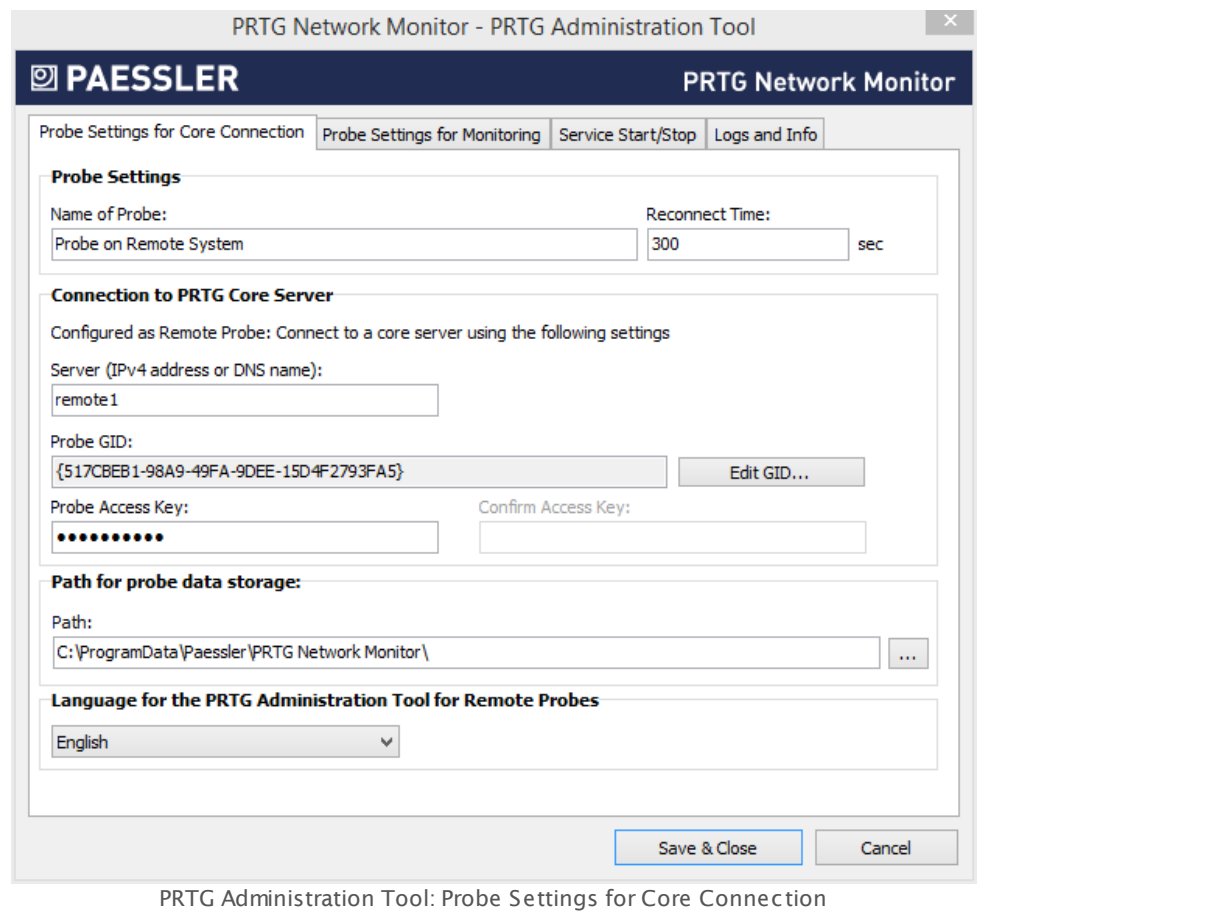
After you have changed settings, click the **Save & Close** button. A new window opens where PRTG asks you to agree to restart the PRTG core server service. Click **OK** if you do not want your changes to be ignored.



PRTG Administration Tool: Restart Services

Probe Settings for Core Connection

Define general settings regarding the probe and probe connections.



PRTG Administration Tool: Probe Settings for Core Connection

PROBE SETTINGS

Name of Probe	Enter a meaningful name to identify the probe. PRTG shows this name, for example, in the device tree, and in all alarms by default. Please enter a string.
Reconnect Time	Define the time that PRTG will wait until the probe tries to reconnect to the core server if the connection fails. Please enter an integer value.

CONNECTION TO PRTG CORE SERVER

These settings affect the way the probe will connect to the core server. A probe is either a local probe or a remote probe. PRTG will automatically detect the type of probe and show the correct setting options.

Server (IPv4 address or DNS name)	If this probe is configured as the **Local Probe** of the PRTG core installation, it will connect to the core via 127.0.0.1, which you cannot change. If this probe is configured as a **Remote Probe**, enter the IP address or DNS name of the core server.
Probe GID	The **Probe GID (global ID (GID))** is a unique identifier for the probe. We recommend that you do not change it. Exception: Only if you substitute an existing remote probe from a different computer, you have to copy the GID from the old probe to the new probe. To do so, click on the **Edit GID...** button and confirm the warning with **Yes**. You can then change the value. You cannot change the GID for a local probe. ⓘ You can deny GIDs under **System Administration—Core & Probes** 2968 in the PRTG web interface. If you remove a remote probe from the device tree or if you deny a remote probe after installation 98, its global ID (GID) will be automatically entered in the **Deny GIDs** list.
Probe Access Key	You do not need an access key for **Local Probe** connections. On a **Remote Probe**, the **Probe Access Key** must match one of the access keys configured in your PRTG core server installation. If it does not match, the remote probe will not be able to connect to the core server. Please see the **System Administration—Core & Probes** 2968 section for more information. ⓘ Check also allowed and denied IPs in **System Administration—Core & Probes** 2968 to ensure that the core server accepts the IP address of the remote probe.

CONNECTION TO PRTG CORE SERVER

Confirm Access Key	If you enter an access key for a remote probe, enter it in this field again to assure correctness.

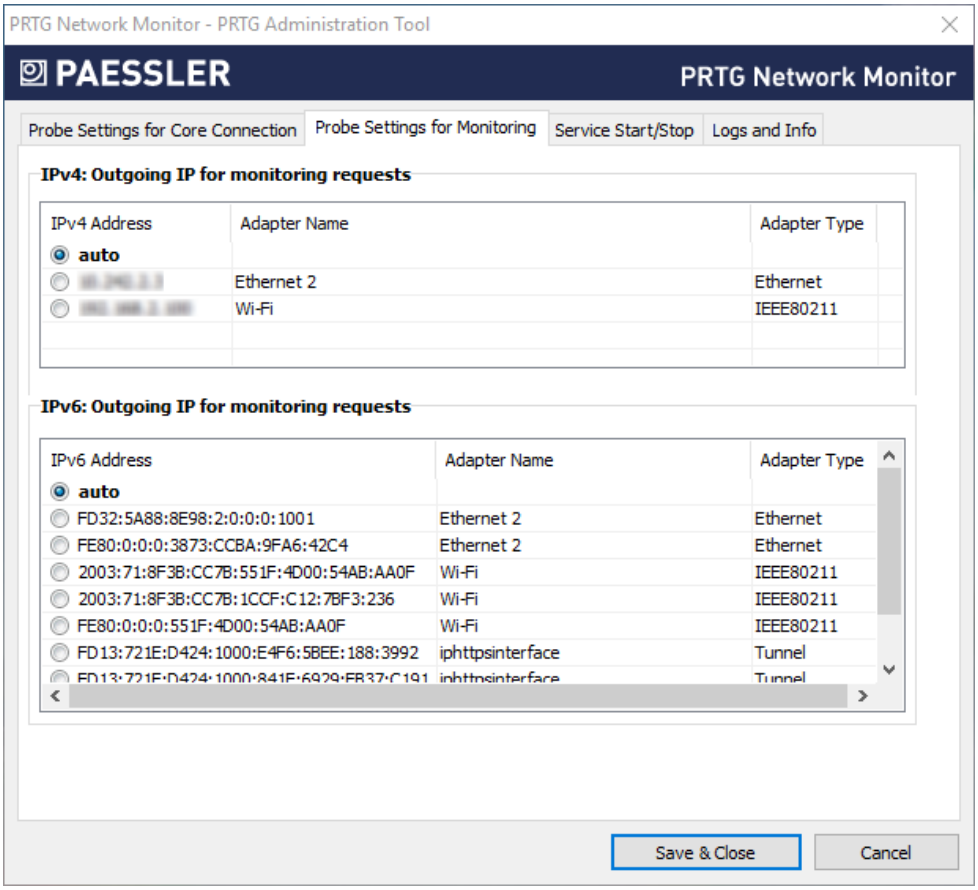
PATH FOR PROBE DATA STORAGE

Path	Define the data folder to which PRTG will store configuration and monitoring data. Click the **...** button to choose another folder on your system. Before you change the path, make sure you stop both the core server and the probe services and copy all data to the new location.

LANGUAGE FOR THE PRTG ADMINISTRATION TOOL FOR REMOTE PROBES

<your language>	Choose the language for the PRTG Administration Tool on your remote probe from the dropdown list. Default is **English**.

Probe Settings for Monitoring



PRTG Administration Tool: Probe Settings for Monitoring

PROBE SETTINGS FOR MONITORING

Define the IP address used for outgoing monitoring requests.

- If there is more than one IP on the current system available, you can specify the IP address that PRTG will use for outgoing monitoring requests of certain sensor types.
- This setting will be used for sensors using the following connection types: HTTP, DNS, FTP, IMAP, POP3, Port, Remote Desktop, SMTP, and SNMP.
- The setting is valid for all monitoring requests sent from this PRTG probe.
- This setting is useful for devices that expect a certain IP address when queried.
- Default setting is **auto**. PRTG will select an IP address automatically.

This feature does not support all sensor types for technical reasons.

PROBE SETTINGS FOR MONITORING

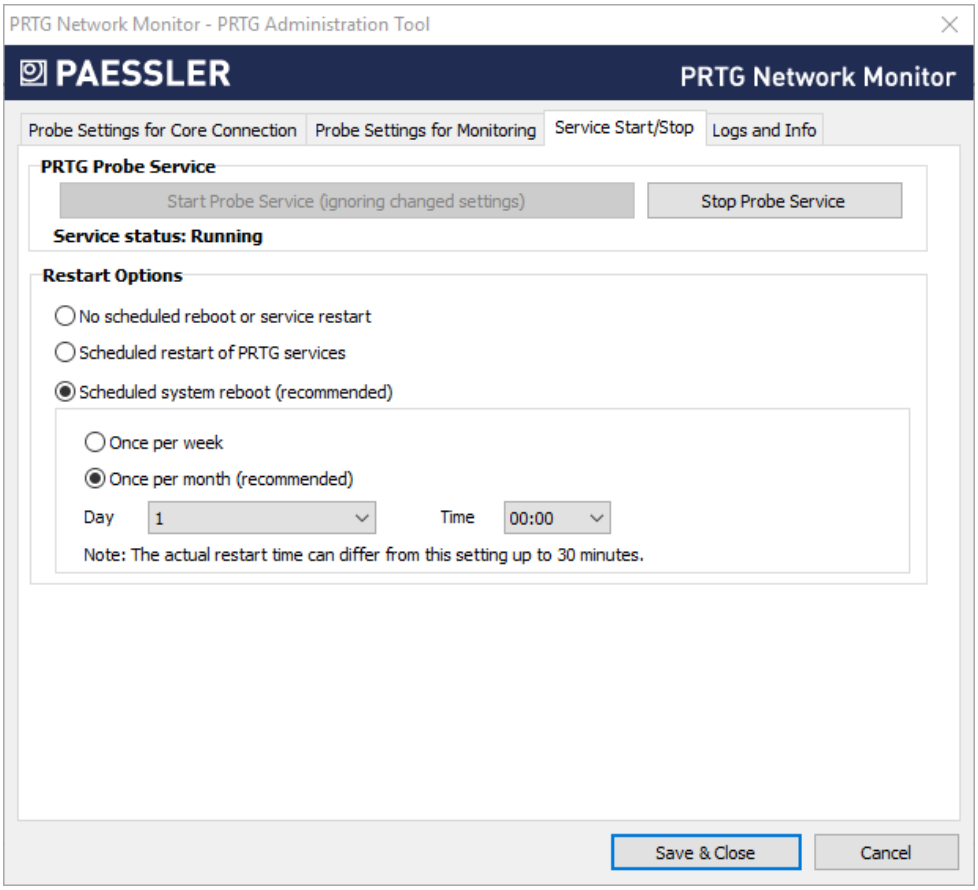
If you change this setting, some sensors might stop working. For example, sensors might show a **Down** status if the selected IP address is blocked on the way to or directly on the monitored device.

Outgoing IPv4	Define the IP address for outgoing requests using the IPv4 protocol. The list shows all IP addresses available on the current system. Choose a specific IP address or select **auto**.
Outgoing IPv6	Define the IP address for outgoing requests using the IPv6 protocol. The list shows all IP addresses available on the current system. Choose a specific IP address or select **auto**. For details about the basic concept of IPv6 in PRTG, please see the **IPv6** 133 section.

Service Start/Stop

You can stop and start PRTG Windows services manually. For connected probes, click **Start Probe Service** to start the service or **Stop Probe Service** to stop it. Both actions usually take from a few seconds up to several minutes to complete. You can also restart the core server and connected probes via the PRTG web interface under **Administrative Tools** 2988.

We recommend that you set a schedule for automatic restarts.



PRTG Administration Tool Start and Stop Service

You can also define a restart schedule on the **Settings** 312 tab of a probe under **Restart Options**, in the PRTG web interface.

SCHEDULED RESTART SETTINGS

This setting is not available for local probes in PRTG on demand.

Restart Options

For best performance, we recommend that you regularly restart the Windows servers on which PRTG is running. To do this automatically for PRTG, you can schedule an automatic restart. Choose between the following options:

- **No scheduled reboot or service restart**: Do not perform any scheduled restart of services automatically. We recommend a manual restart every few weeks. You can initiate a restart of your PRTG core server and probes under **System Administration—Administrative Tools** 2987 in the PRTG web interface.

SCHEDULED RESTART SETTINGS

- **Scheduled restart of PRTG services**: Restart all PRTG services on the system where this probe runs on. If you choose this option on the local probe, the PRTG core server will restart as well. Define a schedule below.
- **Scheduled system reboot (recommended)**: We recommend this setting, although it is not set by default. Enter a schedule below. We recommend that you restart Windows servers once a month for best performance.

Restart Schedule

You can only see this setting if you selected a schedule option above. Choose how often you want to restart PRTG services or the Windows server:

- **Once per week**: Select a day of the week and a time below.
- **Once per month (recommended)**: Select a day of the month and a time below.

Specify Day

You can only see this setting if you selected a schedule option above. Select a specific day of a week (Monday to Sunday) or month (1st to 30th or Last). If you select **Last**, the restart will always be executed on the last day of the month, regardless of how many days the month has.

If you select a date that does not exist in every month (for example, the 30th day in February), PRTG will automatically initiate the restart on the last day of this month.

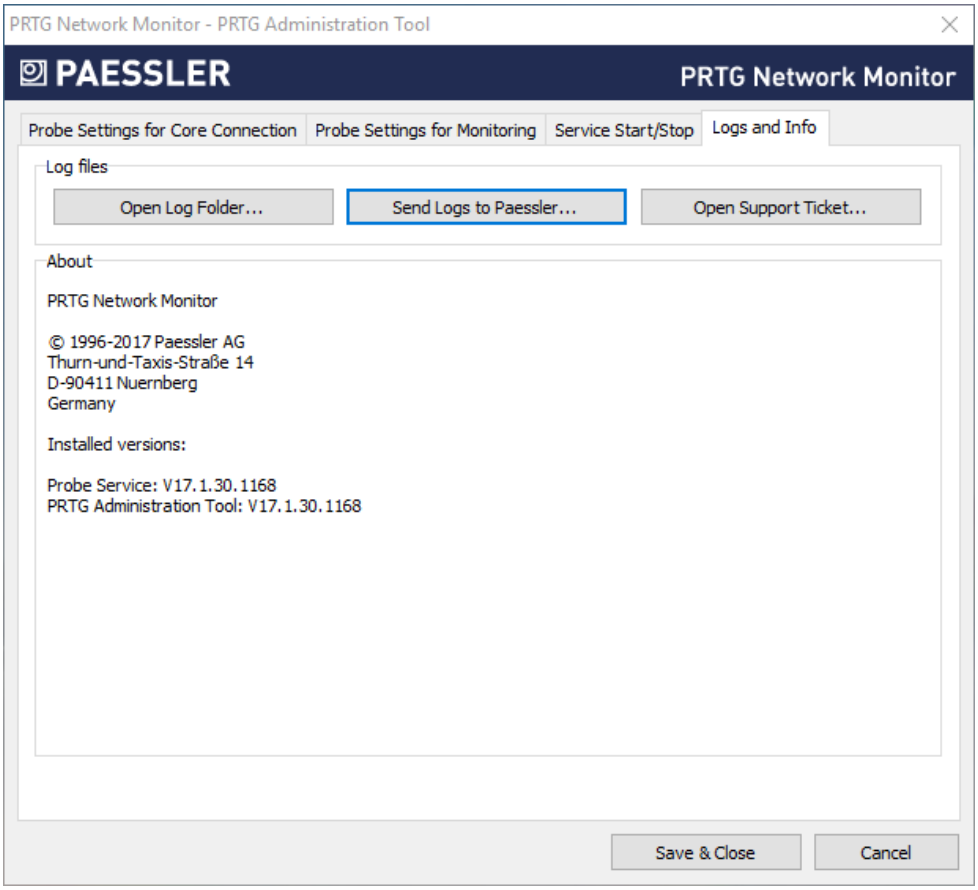
Specify Hour

You can only see this setting if you selected a schedule option above. Select the time of day when PRTG will perform the restart.

You will get a Windows warning message 10 minutes before the restart to inform you if you are a currently logged in user. The actual restart time can differ up to 30 minutes from the settings you enter here.

You can also define a restart schedule on the **Settings** tab of a probe, section **Scheduled Restart Settings** 330, in the PRTG web interface.

Logs and Info



PRTG Administration Tool: Logs and Info

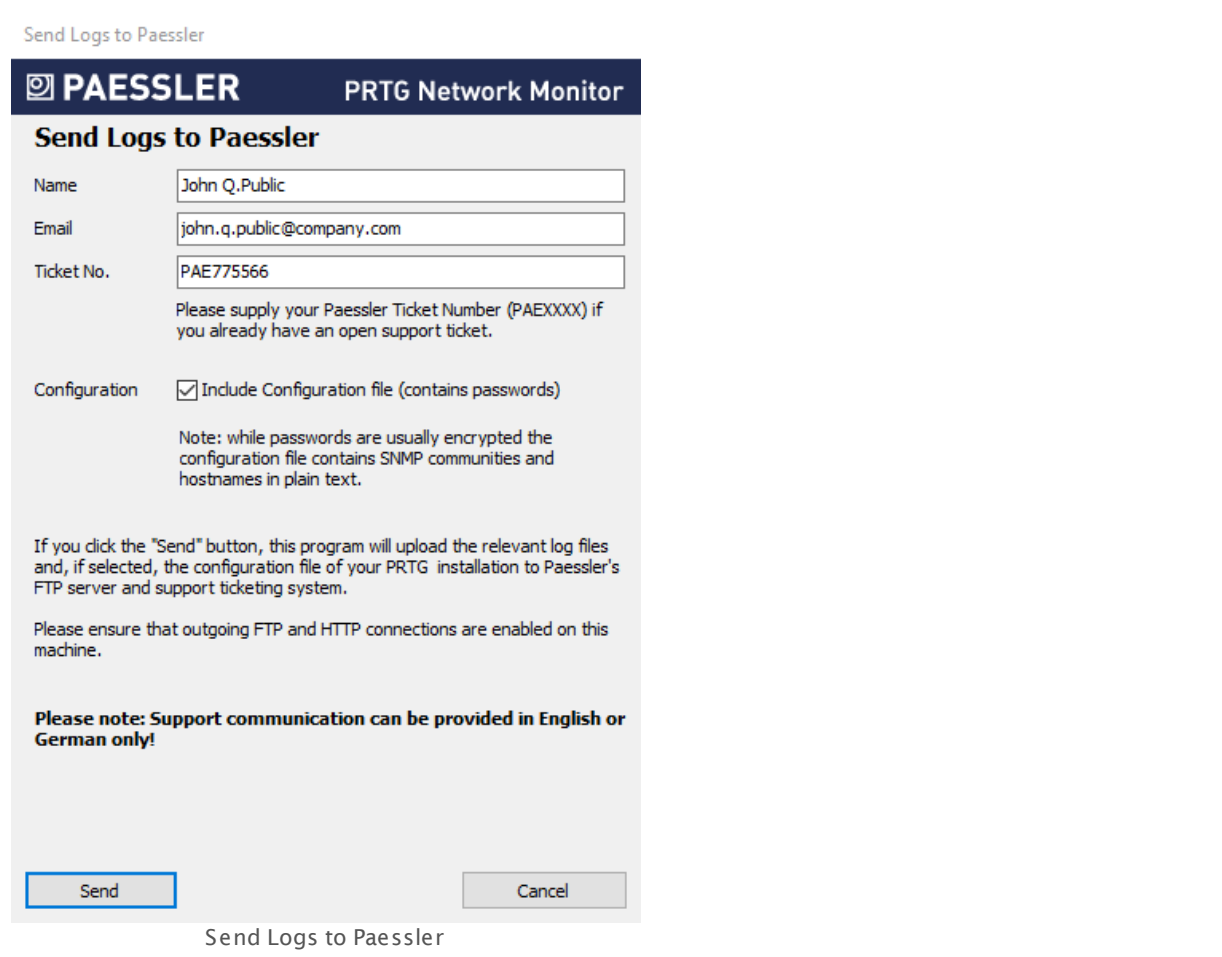
LOG FILES

Open Log Folder...	Open the PRTG Network Monitor data directory on your hard disk drive to access all logfiles that PRTG creates.
Send Logs to Paessler...	Open an assistant to send logfiles to the Paessler support team. Please see below for details 3166.
	You can send logfiles more easily with the support bundle via **Contact Support** 3024 in the PRTG web interface.
Open Support Ticket...	This will open the support form on the Paessler website in a browser window.
	If you need help, we recommend that you use the **Contact Support** 3024 option in the PRTG web interface instead.

The **About** section shows information about the version of installed PRTG programs and copyright.

Send Logs to Paessler

You can send logfiles more easily with the support bundle via **Contact Support** 3024 in the PRTG web interface.



Send Logs to Paessler

If you open a support ticket, Paessler support might ask you to send logfiles for further analysis. With the **Send Logs to Paessler...** button, PRTG will automatically collect, compress, and send your logfiles to our FTPS server.

SEND LOGS TO PAESSLER	
Name	Enter your name.

SEND LOGS TO PAESSLER

Email	Enter a valid email address. You can provide any of your addresses, but we recommend that you use the email address of your PRTG account, which is entered by default.
Ticket No.	This field is optional. If you have already opened a ticket at Paessler support, please provide the ticket number you received. Your files will then be associated with your ticket automatically. Please enter the ticket number starting with PAE followed by four or more digits, for example, PAE12345. If you do not have a ticket number, leave this field empty.
Configuration	Define if you want to include the configuration file in the data. PRTG will remove all passwords from the config file before sending it to our support team.

Click the **Send** button to start the data upload. Ensure that FTPS and HTTP connections are allowed on this machine.

More

Video Tutorial: The PRTG Administration Tool

- https://www.paessler.com/support/videos/prtg-basics/administration-tool

Knowledge Base: Which ports does PRTG use on my system?

- https://kb.paessler.com/en/topic/61462

Part 13

Advanced Topics

13 Advanced Topics

In this section, we cover topics that address more advanced PRTG users. If you already have some experience with PRTG, you might want to learn more about the following topics.

Advanced Topics

- Active Directory Integration 3171
- Application Programming Interface (API) Definition 3174
- Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors 3175
- Channel Definitions for xFlow, IPFIX, and Packet Sniffer Sensors 3180
- Define IP Ranges 3182
- Define Lookups 3183
- Regular Expressions 3193
- Add Remote Probe 3195
- Failover Cluster Configuration 3212
- Data Storage 3226
- Using Your Own SSL Certificate 3228
- Calculating Percentiles 3194

13.1 Active Directory Integration

PRTG offers a detailed rights management via different user groups. For detailed information please see **User Access Rights** 129.

To make user management easier, you can integrate an existing Active Directory into PRTG in four steps. During this process, you connect an Active Directory (AD) group with a user group in PRTG. All members of your AD group can then log in to PRTG using their AD domain credentials.

You cannot add single AD users to PRTG, but only allow access for entire groups. PRTG automatically creates a user account for each AD user who logs in to PRTG successfully.

This feature is not available in PRTG on demand.

Step 1: Prepare Your Active Directory

- In your Active Directory, ensure users you want to give access to PRTG are member of the same AD group.
- You can also organize users in different groups, for example, one group whose members will have administrator rights within PRTG, and another one whose members will have read-only rights within PRTG.

Step 2: Prepare Your PRTG Server

- Make sure the computer running PRTG is member of the domain you want to integrate it to. You can check this setting in your machine's **System Properties** (for example, **Control Panel | System and Security | System**, click **Change settings** link).

Step 3: Add Domain and Credentials (optional) to System Settings

- In the PRTG web interface 136, open the **System Administration—Core & Probes** 2971 settings.
- In section **Active Directory Integration**, enter the name of your local domain into the **Domain Name** field.
  You can only integrate one AD domain into PRTG.
- Optional: PRTG uses the same Windows user account that you use to run the PRTG Core Server Service. By default, this is the local system Windows user account. If this user does not have sufficient rights to query a list of all existing groups from the Active Directory, provide credentials of a user account with full AD access by using the **Use explicit credentials** option as **Access Type**.
  If you cannot save changes to **Core & Probes** settings because you get an **Error (Bad Request)** with the message **Active Directory Domain not accessible**, change from "local user" to **Use explicit credentials** for **Active Directory Integration** and provide the correct credentials for your domain.
- **Save** your settings.

Step 4: Add a New User Group

- Switch to the **User Groups** tab (see **System Administration—User Groups** 2982).
- Click on the **New User Group** button to add a new PRTG user group.
- In the dialog appearing, enter a meaningful name and set the Use Active Directory setting to **Yes**.
- From the Active Directory Group drop down menu, select the group of your Active Directory whose members will have access to PRTG. If you have a very large Active Directory, you will see an input field instead of a drop down. In this case, you can enter the group name only; PRTG will add the prefix automatically.
- With the New User Type setting, define the access rights 129 a user from the selected Active Directory group will have when logging in to PRTG for the first time. You can choose between **Read/Write User** or **Read Only User** (latter is useful to show data only to a large group of users).
- **Save** your settings.

Done

That's it. All users in this Active Directory group can now log in to PRTG using their AD domain credentials. Their user accounts will use the PRTG security context of the PRTG user group you just created.

Notes and Limitations

- Active Directory users can log on to the web interface 138 using their Windows username and password (please do not enter any domain information in PRTG's **Login Name** field). When such a user logs in, PRTG will automatically create a corresponding local account on the PRTG core server. Credentials are synchronized every hour.
- All requests to the Active Directory servers are cached for one hour, for performance reasons. If a password is changed in the Active Directory, you must either wait for 1 hour or clear the cache manually by clicking on the **Clear Caches** button on the **System Administration—Administrative Tools** 2988 page in the **Setup** 2907 menu).
- By default, there are not set any rights for the new PRTG user group. Initially, users in this group will not see any objects in the PRTG device tree. Edit your device tree object's settings 188 and set access rights for your newly created user group in the **Inherit Access Rights** section.
  The easiest way is to set access rights in the **Root Group Settings** 294.
- PRTG only supports explicit group rights. If your AD uses groups which are member of another group, PRTG will not regard inherited implicit rights of the parent group and therefore refuse login for members of those groups.
- PRTG ignores AD information about Organizational Units (OUs). These values cannot be read by PRTG. However, if you use the AD in an auto-discovery group 251, you can restrict the search to computers which are part of an OU.
- PRTG does not support SSO (single sign-on).
- You can integrate only one AD domain into PRTG.

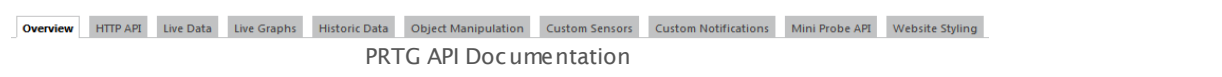
- For very large Active Directories, you will see an input field instead of a drop down when you add or modify a user group. In this case, you can enter the group name only. PRTG will add the prefix automatically.
- A PRTG user account for an AD user is only created if this AD user successfully logs in to PRTG! So if you want to send email notifications 2922 to an AD user group (using the option "Send to User Group" in the notification settings), for example, by choosing the default notification "Email to all members of group [AD group name]", a member of this AD group has to log in to PRTG at least once to be able to receive an email notification. If you want to avoid these single logons of your AD group members to create user accounts, enter the email address of the AD group into the "Send to Email Address" field in the notification settings and choose "None" for the "Send to User Group" option.
- If you want to delete an AD group from PRTG (due to some changes to the AD, for example), you have to delete all users which are in this PRTG user group first. This is because AD users always have this group as their primary group which cannot be changed.
- If you want to reflect changes to your AD in PRTG, you have to delete the AD user group and all members first. Then add the AD group anew. This is because PRTG does not synchronize with your AD automatically.

13.2 Application Programming Interface (API) Definition

The PRTG Application Programming Interface (API) enables you to access monitoring data and manipulate objects using HTTP requests, run your own written sensors and notifications, implement Mini Probes, and customize the web interface.

Detailed HTTP API Documentation

An interactive documentation of the API is integrated into your PRTG installation: Login to the web interface 138 and select **Setup** | **PRTG API** from the main menu.



PRTG API Documentation

In different tabs, the documentation provides information about:

- **HTTP API**: Access monitoring data and manipulate monitoring objects using HTTP requests. This tab includes an interactive query builder that you can use to test your queries. You can find more details about accessing monitoring data and manipulating objects on the tabs **Live Data**, **Live Graphs**, **Historic Data**, and **Object Manipulation**.
- **Custom Sensors**: Create your own sensors for customized monitoring. See also this Knowledge Base article: How can I share my self-written PRTG script/program with other PRTG users?
- **Custom Notifications**: Create your own notifications to send alarms to external systems.
- **Mini Probe API**: Create your own small probes for PRTG on premises to get monitoring data from any platform. For sample usages of the Mini Probe interface, see this Knowledge Base article: Where can I find PRTG Mini Probes which are ready to use?
- **Website Styling**: Customize the look and feel of PRTG on premises by adding your own CSS statements. For sample customizations of the web interface, see this Knowledge Base article: Can you provide sample CSS, JavaScript, HTML for customizing PRTG's web interface?

The documentation that comes with your PRTG installation fits exactly the PRTG version you are using.

More

Knowledge Base: Can you provide sample CSS, JavaScript, HTML for customizing PRTG's web interface?

- https://kb.paessler.com/en/topic/60130

Knowledge Base: How can I share my self-written PRTG script/program with other PRTG users?

- https://kb.paessler.com/en/topic/63737

Knowledge Base: Where can I find PRTG Mini Probes which are ready to use?

- https://kb.paessler.com/en/topic/61215

13.3 Filter Rules for xFlow, IPFIX and Packet Sniffer Sensors

You can use filter rules for the **Include Filter**, **Exclude Filter**, and **Channel Definition** fields of Packet Sniffer 3097, xFlow, and IPFIX 3099 sensors. The filter rules are based on the following format:

```
field[filter]
```

Valid Fields for All Sensors

FIELD	POSSIBLE FILTER VALUES
IP	IP address or DNS name (see Valid Data Formats 3178 below)
Port	Any number
SourceIP	IP address or DNS name (see Valid Data Formats 3178 below)
SourcePort	Any number
DestinationIP	IP address or DNS name (see Valid Data Formats 3178 below)
DestinationPort	Any number
Protocol	TCP, UDP, ICMP, OSPFIGP, any number
TOS	Type Of Service: any number
DSCP	Differentiated Services Code Point: any number

Additional Fields for Packet Sniffer Sensors Only

FIELD	POSSIBLE FILTER VALUES
MAC	Physical address (see Examples 3178 below)
SourceMAC	Physical address
DestinationMAC	Physical address
EtherType	IPV4, ARP, RARP, APPLE, AARP, IPV6, IPXold, IPX, any number

FIELD	POSSIBLE FILTER VALUES
VlanPCP	IEEE 802.1Q VLAN Priority Code Point
VlanID	IEEE 802.1Q VLAN Identifier
TrafficClass	IPv6 Traffic Class: corresponds to TOS used with IPv4
FlowLabel	IPv6 Flow Label

Additional Fields for NetFlow v5 and jFlow v5 Sensors Only

FIELD	POSSIBLE FILTER VALUES
Interface	Any number
ASI	Any number
InboundInterface	Any number
OutboundInterface	Any number
SenderIP	IP of the sending device. This is helpful if several devices send flow data on the same port, and you want to divide the traffic of each device into a different sensor channel. Possible values: IP address or DNS name (see Valid Data Formats 3178 below)
SourceASI	Any number
DestinationASI	Any number

Additional Fields for NetFlow v9 and IPFIX Sensors Only

FIELD	POSSIBLE FILTER VALUES
Interface	Any number
ASI	Any number

FIELD	POSSIBLE FILTER VALUES
InboundInterface	Any number
OutboundInterface	Any number
SenderIP	IP of the sending device. This is helpful if several devices send flow data on the same port, and you want to divide the traffic of each device into a different sensor channel. Possible values: IP address or DNS name (see Valid Data Formats 3178 below)
SourceASI	Any number
DestinationASI	Any number
MAC	Physical address
SourceMAC	Physical address
DestinationMAC	Physical address
Mask	Mask values represent subnet masks in with a single number (number of contiguous bits).
DestinationMask	Mask values represent subnet masks in with a single number (number of contiguous bits).
NextHop	IP address or DNS name (see Valid Data Formats 3178 below)
VLAN	VLAN values represent a VLAN identifier (any number)
SourceVLAN	VLAN values represent a VLAN identifier (any number)
DestinationVLAN	VLAN values represent a VLAN identifier (any number)

Additional Fields for sFlow Sensors Only

FIELD	POSSIBLE FILTER VALUES
Interface	Any number

FIELD	POSSIBLE FILTER VALUES
InboundInterface	Any number
OutboundInterface	Any number
SenderIP	IP of the sending device. This is helpful if several devices send flow data on the same port, and you want to divide the traffic of each device into a different sensor channel. Possible values: IP address or DNS name (see Valid Data Formats 3178 below)
MAC	Physical address
SourceMAC	Physical address
DestinationMAC	Physical address

Valid Data Formats

- IP fields support wildcards (*), range (10-20) and hostmask (/10, /255.255.0.0) syntax, as well as DNS names.
  IPv6 wildcards, IPv6 ranges, and IPv6 hostmasks are not supported.
- Number fields support range (80-88) syntax.
- Protocol and EtherType fields support numbers and a list of predefined constants.

For detailed information on IP ranges, see section **Define IP Ranges** 3182.

Examples

All of the following filter rules are valid examples:

```
SourceIP[10.0.0.1]
SourceIP[10.*.*.*]
SourceIP[10.0.0.0/10]
DestinationIP[10.0.0.120-130]
DestinationPort[80-88]
Protocol[UDP]
MAC[00-60-50-X0-00-01]
DSCP[46]
```

You can create more complex expressions using parentheses **( )** and the words **and**, **or**, or **and not**. For example, this is a valid filter rule:

```
Protocol[TCP] and not (DestinationIP[10.0.0.1] or SourceIP[10.0.0.120-130])
```

Related Topics

- **Channel Definitions for xFlow, IPFIX, and Packet Sniffer Sensors** 3180
- **Monitoring Bandwidth via Packet Sniffing** 3097
- **Monitoring Bandwidth via Flows** 3099

Knowledge Base: How can I change the default groups and channels for xFlow and Packet Sniffer sensors?

- https://kb.paessler.com/en/topic/60203

13.4 Channel Definitions for xFlow, IPFIX, and Packet Sniffer Sensors

When adding Custom xFlow sensors, Custom IPFIX 3099, or Custom Packet Sniffing sensors 3097, you have the option to provide a **Channel Definition**. In this field enter your channel definitions using the following syntax (one entry per channel):

```
#<id>:<Name>
<Rule>
```

Syntax

- The **<id>** needs to be 1 or a higher number and must be unique for the sensor. This means each channel definition must have a unique ID.
  The maximum channel ID you can use is 2147483648 (2^31). Higher IDs are not supported. We recommend that you use channel IDs like 1, 2, 3, and so on.
- The **<id>** is linked to the historic data.
  As soon as you change the ID, you will loose the history for this particular channel that the ID was linked to.
- One rule can span multiple lines.
- The next rule starts with a # as first character in a line.
- The **<name>** is the channel's display name.
- The rules are processed top to bottom (the number does not matter) and the data is accounted to the first match.
- PRTG adds one channel named **Other** automatically. This channel counts all traffic for which you have not defined a channel.
- After the name you can use an optional **[<unit>]** to override the automatic unit which is based on the source sensors.

The **<Rule>** syntax is identical to the one described in the Filter Rules for xFlow and Packet Sniffer Sensors 3175 section. Because data is accounted to the first match, make sure you start with the most specific rule at the top and get less specific to the bottom.

We recommend that you write the rules list in an external editor first and then paste it into the **Channel Definition** field of the sensor in PRTG. Otherwise, if the rules contain an error, the entries will be removed when you add the rules in case!

Example

General example:

```
#5:HTTP
Protocol[TCP] and
(SourcePort[80] or DestinationPort[80] or SourcePort[8080] or
DestinationPort[8080])
```

Channel definition example for differentiating by protocol:

```
#1:TCP
Protocol[TCP]

#2:UDP
Protocol[UDP]

#3:ICMP
Protocol[ICMP]
```

Related Topics

- **Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors** 3175
- **Monitoring Bandwidth via Packet Sniffing** 3097
- **Monitoring Bandwidth via Flows** 3099

More

Knowledge Base: How can I change the default groups and channels for xFlow and Packet Sniffer sensors?

- https://kb.paessler.com/en/topic/60203

13.5 Define IP Ranges

In some setting fields, you can either enter a host name or single IP address, or you can define IP ranges. PRTG follows a common syntax for this. IP ranges are available, for example, for xFlow and Packet Sniffer sensors 386 and for probe connection settings 2968.

For the supported syntax of the automatic network discovery functionality in PRTG, see section **Auto-Discovery** 252 (**IP Selection Method**).

Available Options

OPTION	DESCRIPTION	SYNTAX	EXAMPLE(S)
Simple	Enter a fixed IP address.	a.b.c.d	10.0.10.9
Hostname	Enter a hostname. PRTG will resolve it to an IP address in your network.	hostname	device-xyz
Hostmask	Enter a hostmask. A hostmask defines the relevant bits of the IP address.	a.b.c.d/h or a.b.c.d/e.f.g.h	10.0.0.0/255
Range	Enter an IP address range. Replace each of **a**, **b**, **c**, **d** by either ▪ * (asterisk) for any value; corresponds to 0-255 —or— ▪ **x-y** for any range between 0 and 255.	a.b.c.d	10.0.0.1-20 or 10.*.0.* or 10.0.0-50.*

13.6 Define Lookups

PRTG uses **lookups** for some sensor types and for some sensors with custom channels. In general, lookups make data more human friendly because they map status values as returned by a device (usually integers) to more informative expressions in words that show you the status of a monitored device as a clear message.

Additionally, lookups can also define the sensor status [163] that will be shown in correlation with certain status codes, just like sensor channel limits [2783] can define a sensor status, too. For example, for a printer, PRTG can show a sensor in a yellow **Warning** [163] status with channel values, provided by lookups, like "Toner Low" instead of simple status codes, like "1".

You can customize lookups individually and define your own texts that a sensor channel can show. See the section **Customizing Lookups** [3188] below.

If a channel uses lookups, we strongly recommend that you control the sensor status only via the lookup definition and not use channel limits! See also section **Sensor Channels Settings** [2783].

Lookups do not change data in the PRTG database, but they merely change the way sensor channels are shown. Any change to lookup definition files will apply to historic data as well as to live data.

Some exceptions apply to the **SNMP Custom String Lookup Sensor** [1679] that basically does an "inverse lookup". It does not map an integer to a text message but looks only for matching strings in the lookup definition and shows a status based on this text value.

Customizing lookups is not possible for PRTG on demand instances.

Requirement: Channel Unit "Custom"

All sensor channels with enabled **Value Lookup** need to use the channel **Unit** "Custom". For details, refer to the section **Sensor Channels Settings** [2783].

There are sensors that provide the unit **Value Lookup** for channels in their sensor settings. Do not use the "custom" unit for channels of these sensors if you want to use lookups! This would result in malfunctioning lookup channels. For the following sensor types, choose the unit **Value Lookup** in the sensor settings and select your lookup file directly when adding the sensor:

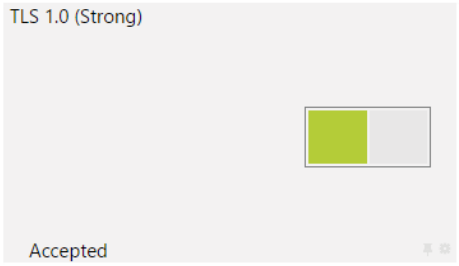
- **Google Analytics Sensor** [827]
- **Microsoft SQL v2 Sensor** [1135]
- **MySQL v2 Sensor** [1151]
- **Oracle SQL v2 Sensor** [1253]
- **PostgreSQL Sensor** [1363]
- **SNMP Custom Advanced Sensor** [1658]
- **SNMP Custom Table Sensor** [1689]

Visualization of Lookup Channels

PRTG can display gauges or switches for channels which use lookups. We recommend that you stay below 120 lookup values to display informative gauges for primary channels. Non-primary channels have an upper limit of around 40 lookup values for gauges.

The various states displayed in gauges always follow the clockwise order **Up** (green) < **Warning** (yellow) < **Down** (red) < **Unknown** (Gray / Black).

A Gauge Showing the Status of a Lookup Channel



A Switch Showing the Status of a Boolean Lookup Channel

Lookups Directory and Format

Lookups are defined in XML format in files ending in **.ovl**. PRTG's standard lookup files are located in the PRTG program directory 3226 in the **\lookups** subfolder. These files are maintained by PRTG itself. In each of the files lookups are defined for one or more sensors. Furthermore, the lookups folder contains the **\custom** subfolder to store your customized lookups.

The files follow a basic principle. For each numeric value you can define:

- A message that the sensor will look up and show instead of the numerical value
- The status that the sensor will show

Use the **SNMP Custom String Lookup Sensor** 1679 to map a string into a corresponding status. Please use the lookup type 3190 **SingleInt** for this purpose.

You cannot access this directory on PRTG on demand instances.

Example

The following code illustrates the lookup definition for the toner status of the **SNMP HP LaserJet Hardware** 1791 sensor:

```
<?xml version="1.0" encoding="UTF-8"?>
<ValueLookup id="oid.paessler.hplaserjet.tonerstatus" desiredValue="1" xmlns:xsi="http://www.w3.org/2001/X
       <Lookups>
              <SingleInt state="Ok" value="0">Toner Okay</SingleInt>
              <SingleInt state="Warning" value="1">Toner Low</SingleInt>
              <SingleInt state="Error" value="2">No Toner Cartridge Loaded</SingleInt>
       </Lookups>
</ValueLookup>
```

The schema in the example provides an insight how lookups are defined:

- The **<?xml>** tag in the first line defines the content as XML.
- The **<ValueLookup>** tag in the second line contains:
  - The **ID** which is shown in the **Sensor Channels Settings** 2782.
  - The **desiredValue** 3189 attribute contains the value which is used for the calculation of the "Coverage". In this example, **1** is defined as desired value.
  - The **xsi** attributes refer to PRTG's predefined XML schema definitions (which allow easy editing of lookup files with supported editors). We recommend that you use the default value.
- Between the tags **<Lookups>** and **</Lookups>** the particular lookups for the sensor data are defined:
  - A lookup entry starts with a tag containing the type of the status value, the lookup type (in this example, this is always **<SingleInt>**).
  - Separated by whitespace, the **state** attribute defines the status the sensor will show. Allowed values are: **Ok**, **Warning**, **Error**, and **None** ("None" does not trigger a status change).
  - The **value** attribute defines which numeric value will trigger the lookup. This is the value that PRTG will receive from the device.
  - The **text** defines the substitution text that is shown instead of the value. For example, this can be a status message.
- The same way all other possible lookups are defined. The lookup definitions are closed by the tag **</Lookups>**. The file closes with **</ValueLookup>**.

In our example, the lookup file will have the following effect:

Value as Reported from HP Printer	Value Shown in PRTG (Sensor Channel)	Sensor Status Shown by PRTG
0	Toner Okay	Up
1	Toner Low	Warning
2	No Toner Cartridge Loaded	Down

The XML Schema

An exemplary schema of the XML files containing the lookup definitions can be sketched like this:

```
<?xml version="1.0" encoding="UTF-8"?>
<ValueLookup id="..." desiredValue="..." undefinedState="..." xmlns="..." xsi="...">
	<Lookups>
		<SingleInt state="..." value="...">status text</SingleInt>
		<Boolean state="..." value="...">status text</Boolean>
		<BitField state="..." value="...">status text</BitField>
		<Range state="..." from="..." to="...">status text</Range>
		[several other lookup definitions]
	</Lookups>
</ValueLookup>
```

Element	Description	Attributes, Value Assignment, and Content
<?xml> content	This is the XML declaration. Every XML file begins with it.	▪ **version** and **encoding** are "1.0" resp. "UTF-8" ▪ content: **<ValueLookup>**contentValueLookup**</ValueLookup>**
<ValueLookup> contentValueLookup **</ValueLookup>**	Defines the **ID** of the channel, what **desiredValue** is used, the status for undefined values (**undefinedState**), and links to PRTG's predefined schema definitions, which allow editing of lookup files with supported editors.	▪ **id**: Specifies how the name of the lookup file is shown in the **Sensor Channels Settings** 2782. ▪ **desiredValue** 3189: Please see below. ▪ **undefinedState**: Optionally define a status for values that are not defined in the lookup file. If the target device returns a value that is not included in the lookup definition, the sensor will show this status (**Ok**, **Warning**, **Error**, or **None**) with an according message. Without a definition of "undefinedState", the sensor will only show the returned value. ▪ **xmlns:xsi/xsi**: refers to predefined XML schema definition ▪ contentValueLookup: lookup definitions **<Lookups>**contentLookups**</Lookups>**
<Lookups> contentLookups **</Lookups>**	Defines the particular lookups for the sensor data.	▪ contentLookups: one or more lookup entries, see below
<SingleInt> status text **</SingleInt>** **<Boolean>** status text **</Boolean>** **<BitField>** status text **</BitField>** **<Range>** status text	Each element defines one lookup entry. There can be one or more entries in this format. SingleInt, Boolean, BitField, and Range are lookup types 3190.	▪ **state**: defines the state the sensor will show; allowed values: **Ok**, **Warning**, **Error**, **None** ▪ **value**: defines the value which triggers the lookup. Please enter an integer value. **Range** needs always both values "from" and "to". ▪ status text: defines a **status text** that will be used as substitution text and shown instead the integer value. For

Because all the XML files containing lookup definitions are delivered in a pre-given schema as indicated above, you can customize lookups accordingly.

Customizing Lookups

If you want to change the status definitions of a specific sensor channel, you basically have to do the following:

1) Find out the (file) name of the lookup file in the settings of the sensor channel 2782 you want to change the behavior for.

2) From the PRTG program directory 3226 subfolder **\lookups**, copy this file into the **\lookups \custom** subfolder (ensure you do not change the file name!).

3) Change the duplicated file as you like. See the example below.

This feature is not available in PRTG on demand.

All default lookup files are located in the **\lookups** subfolder in the PRTG program directory 3226. To customize existing lookups, copy the desired lookup file from the lookups folder to the **\lookups\custom** subfolder or create a new .ovl file there. When using the same ID in the ValueLookup tag, the files in the **\lookups\custom** folder will have a higher priority than the original files in the **\lookups** folder. This way, PRTG handles your customizations preferably instead of the original lookup settings. If you want to use custom lookup definitions in addition to the existing lookups, define a new ID in the lookup file which is not used by another lookup file. PRTG identifies lookup definitions via this ID, it does not use the file name.

Open the file with an XML or text editor and adjust the lookups to your personal preferences. You can define your own messages as well as you can customize sensor states for the particular return values. For example, if you do not want show an "Error" (a sensor **Down** status) for the return value "2" but only a warning, then you can replace "Error" with "Warning".

The possible states are given in the **LookupState.xsd** file in the custom directory. Following the schema of the XML files that are delivered with PRTG enables you to edit the lookups in a safe way.

If you imported an oidlib file 1915 that contains lookups 3183 (you can see this in section **Lookup** in the MIB Importer), you can define your own sensor states for returning values. If you add an **SNMP Library Sensor** 1912 using this oidlib, PRTG will create a lookup definition file using the **lookupname** of the chosen library as **id** parameter. Override this lookup definition with your own custom lookup as described in this section. This is important because lookups that are added via an oidlib will not contain any state definitions and result in a **Warning** status 163 of the sensor by default because of the entry undefinedState="Warning".

If you use an **SNMP Custom String Lookup Sensor** 1679, you can create a new custom lookup definition in the **\lookups\custom** directory with the expected return values. In this case, use the **lookupname** of the chosen library as **id** parameter to override the lookups from the oidlib file.

When you save an edited lookup, make sure that it is saved as an .ovl file. Otherwise, the lookup might accidentally be saved as a .txt file and might not be loaded.

Example for Lookups Customization

For example (just for illustration purposes), imagine you would like

1) to have the status "Warning" for all undefined values that the target device might return,

2) to change the status for the return value "2" from "Down" to "Warning",

3) and to add the status "None" to the example 3185 above.

Then do the following:

- Copy the file oid.paessler.hplaserjet.tonerstatus to the **\lookups\custom** subfolder of your PRTG installation.
- Open this file with an editor.
- Leave the ID value unchanged to prioritize the customized lookup to the original file.
- Insert the status definition for undefined values into the ValueLookup element: undefinedState="Warning"
- Replace "Error" with "Warning" for value "2".
- Add a a "SingleInt" element with status "None" for the (hypothetical) return value "3".
- Save the file and reload 3192 the custom lookup folder in PRTG.

The customized lookup file will finally look like this:

```
<?xml version="1.0" encoding="UTF-8"?>
<ValueLookup id="oid.paessler.hplaserjet.tonerstatus" desiredValue="1" undefinedState="Warning" xmlns:xsi=
       <Lookups>
              <SingleInt state="Ok" value="0">Toner Okay</SingleInt>
              <SingleInt state="Warning" value="1">Toner Low</SingleInt>
              <SingleInt state="Warning" value="2">No Toner Cartridge Loaded</SingleInt>
              <SingleInt state="None" value="3">Unknown status of toner</SingleInt>
       </Lookups>
</ValueLookup>
```

See also **SNMP Custom String Lookup Sensor—Example** 1686 for a lookup definition that maps a string value to a sensor status.

desiredValue Attribute

It is necessary to define a **desiredValue** in the lookup files. The desiredValue corresponds to a status value triggering a lookup. PRTG calculates the percentage of time this specific state has been monitored. The result is displayed for all data tables and graphs that show averaged values.

Considering the example above where the desiredValue is "1", PRTG will calculate the percentage of time the toner status has been "Warning". If in a time span of five minutes four of five sensor scans returned a "Warning" status, PRTG would show an average of 80% for this time span, because in 80% of the time the sensor showed a "Warning".

Lookup Types: SingleInt, Boolean, BitField, Range

Besides the lookup type **SingleInt** as seen above, there are three other lookup types: **Boolean**, **BitField** and **Range**. Using these types you can define lookup values beyond simple integers.

Lookup Type	Description	Syntax
SingleInt	Uses an **integer** to define a lookup for one status value.	value="int" Only signed 32-bit integers are supported.
Boolean	Uses **0** or **1** to define a lookup for two different status values.	value="0" value="1"
BitField	Uses a **bitfield** for multiple status values.	Only use it if you have basic knowledge about bitmasks. Please see the section **More** 3192 below for a general introduction. Every value has to equal a power of two (for example, 1, 2, 4, 8, 16, 32, 64, etc.). The **SNMP Custom String Lookup Sensor** 1679 does not support BitFields.
Range	Uses an inter range **from-to** to define a lookup for several status values.	from="int" to="int" Using ranges, the parameters "from" and "to" always have to be defined. If you want to query only one single value in a range file, this value must be set as parameter for "from" **and** "to" (for example, from="2" to="2"). The **SNMP Custom String Lookup Sensor** 1679 does not support ranges. Only signed 32-bit integers are supported.

You can use only **one** kind of lookup type in **one** lookup file. This means, only or SingleInts, or Boolean, or BitField, or Ranges. Different lookup types in one file are not allowed.

Define Lookup Files in Sensor Channel Settings

For each sensor with a custom channel, you can define a lookup file to use with the option **Value Lookup** in the sensor channel settings 2782. This option is visible for many **SNMP sensors**, some **application sensors**, and always for the following sensor types:

- **EXE/Script Sensor** 747
- **EXE/Script Advanced Sensor** 759 (if a **Custom** unit is defined)
- **SNMP Custom Sensor** 1649

For details, see section **Sensor Channel Settings** 2782.

Loading Lookups

You can (re)load the defined lookups in the custom folder by clicking the **Load Lookups** button in the PRTG web interface under **Setup | System Administration | Administrative Tools** 2987.

A sensor whose lookup file you have modified and reloaded will not re-evaluate this lookup before the next sensor scan. For sensors with large scanning intervals, use the **Check Now** option from the context menu 226 to immediately apply the new lookup definition and to avoid an incorrect sensor status.

Debugging—What will happen if...?

- A return value is defined in the lookups that never will be returned by a device because the value is not assigned: The value will never be triggered, so PRTG simply ignores this entry.
- PRTG receives a return value that is not defined for lookups: No substitution message can be found. PRTG will just show the return value. You can optionally define a status for unknown values with a definition of **undefinedState** in the **ValueLookup** element (see section **Define Lookups—The XML Schema** 3186 above).
- Different lookup types are in one lookup file: This is not allowed and PRTG will discard this lookup definition. If you use miscellaneous lookup types in one file, for example, ranges and singleInts together, the PRTG system will create a ticket when loading lookups or restarting the PRTG server with the following error message: Value lookup file "[...]" could not be loaded ("" is not a valid integer value)".
- Incorrect XML code: PRTG will create a new ticket when loading lookups or restarting the PRTG server with a corresponding error message and discard this lookups definition.
- A lookup file has a file ending other than .ovl: The file will not be loaded.

More

Video Tutorial: How to configure lookups in PRTG Network Monitor

- https://www.paessler.com/support/videos/prtg-advanced/prtg-lookups

Wikipedia: Masks (computing)

- http://en.wikipedia.org/wiki/Bit_mask

13.7 Regular Expressions

For some sensors (for example, some HTTP sensors 386 and email sensors 391), you can use regular expressions to match a search pattern. PRTG suppors PCRE-RegEx. See below for examples with the most common patterns.

Common Search Patterns

Find matches containing the word **error** or **alarm**:

```
\b(error|alarm)\b
```

Find matches containing the words **error** and **alarm** in any order:

```
(?=.*\berror\b)(?=.*\balarm\b).*
```

Find matches containing all of the words **tree**, **flower**, **leaf**, and **bug**, in any order:

```
(?=.*\btree\b)(?=.*\bflower\b)(?=.*\bleaf\b)(?=.*\bbug\b).*
```

It is not possible to match an empty string using the PRTG regex search with sensors.

Example

The search pattern

```
(?=.*\berror\b)(?=.*\balarm\b).*
```

will match the following expressions:

- alarm error
- error alarm
- I am an error and I evoke an alarm
- I am an alarm and I indicate an error
- An alarm combined with an error indeed!
- An error combined with an alarm, too!

More

Regex Tester: Test Regular expressions interactively

- http://regexpal.com

Wikipedia: Regular expression

- http://en.wikipedia.org/wiki/Regular_expression

13.8 Calculating Percentiles

PRTG not only monitors your network and informs you in the case of issues that are worth you taking a closer look at in the here and now. PRTG also stores a lot of historic measurement data gathered from your sensors. This means that you have a great base for statistical analysis and evaluation of what is and was happening in your network.

When creating a **Report** 2862 with PRTG, you get raw data, sums, averages and percentages of your monitoring data.

Additionally, PRTG also offers percentile calculation. This statistical method puts your data in order, for example, from the lowest value to the highest value, and calculates the percentile you want, optimally informing you about the distribution of your network relevant data.

For example, if you request the 95th percentile, you know that 95 percent of the measured data is below a certain value, and thanks to PRTG, you know what this certain value is.

If applied, for example, to bandwidth, you know what values you are talking about when talking about the 5 percent of unusually high bandwidth consumption and which value your users do not exceed 95 percent of the time. Service providers often use percentiles to offer a fairer billing that excludes infrequent usage peaks.

If you want to know more about the formula that PRTG uses for percentile calculation, see this Knowledge Base article: What are percentiles and what differences do they make in PRTG reports?

Create a report for several sensors and device groups using the **Report** 2862 feature or create reports for single sensors using the **Historic Data Reports** 175.

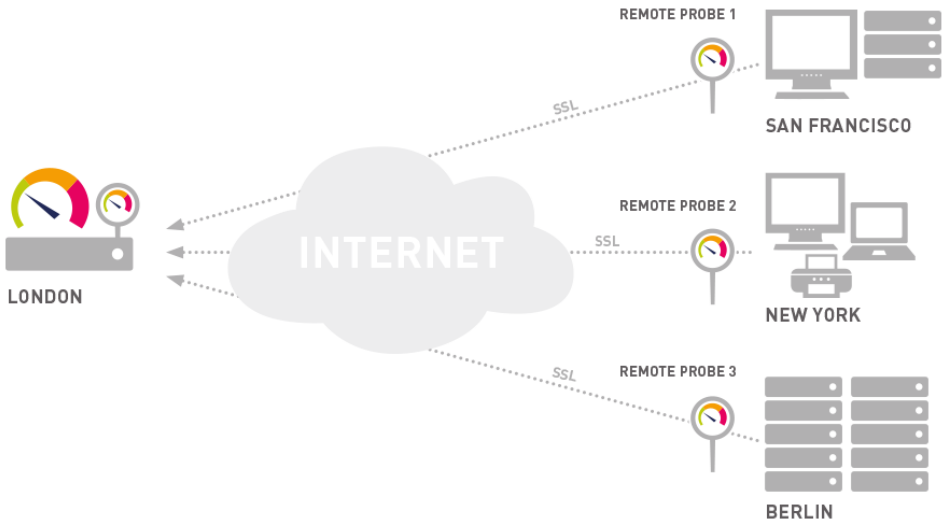
More

Knowledge Base: What are percentiles and what differences do they make in PRTG reports?

- https://kb.paessler.com/en/topic/9563

13.9 Add Remote Probe

You can extend your monitoring by installing one or more **Remote Probes**[3196]. A remote probe installation is required to monitor your local network with a PRTG on demand instance. Remote probes also allow you to monitor different sub-networks that are separated by a firewall from your PRTG on premises core server, to keep an eye on remote locations, and are useful in several other scenarios.



Monitoring Remote Locations via Remote Probes

Click here to enlarge: http://media.paessler.com/prtg-screenshots/monitoring-remote-locations-via-remote-probes.png

Extend Your Monitoring Now

Installing remote probes is easy—you can do it within a few minutes. Please see the sections linked below for further instructions.

- Background: **Remote Probes and Multiple Probes**[3196]
- Installing: **Remote Probe Quick Install**[3199]
- Step by Step: **Remote Probe Setup**[3206]

More

Video Tutorial: Core Server and Remote Probes

- https://www.paessler.com/support/video_tutorials/distributed_monitoring

13.9.1 Remote Probes and Multiple Probes

Upon installation, PRTG creates the first probe automatically, called the **Local Probe**. It runs on the same machine as the PRTG core server and monitors all devices from this system, using the sensors you have configured.

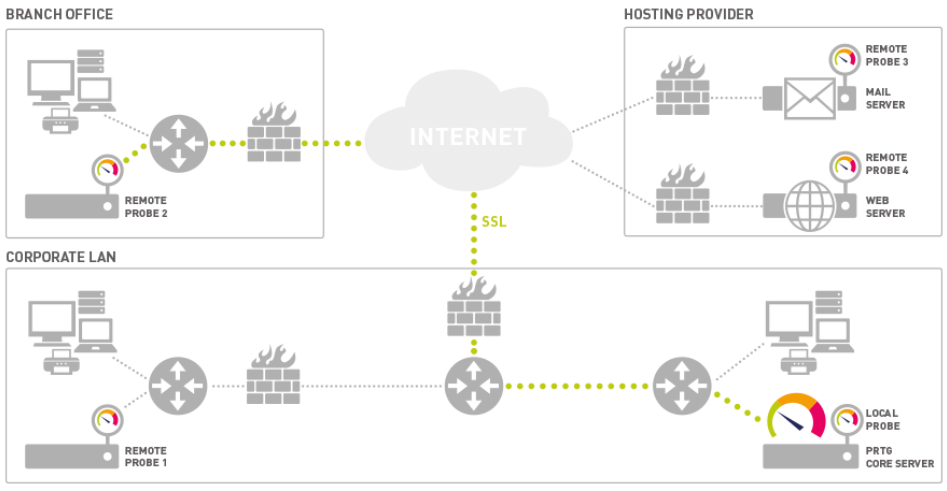
Working with only one local probe should suffice for Local Area Network (LAN) monitoring with PRTG on premises and if you want to monitor one location only. For LAN monitoring with PRTG on demand, at least one remote probe is required.

Scenarios Requiring Remote Probes

There are several situations that make it necessary to work with **Remote Probes** in the same LAN or in remote locations. Among these situations are the following:

- You run a PRTG on demand instance and want to monitor your local network.
- You have more than one location and you need to make sure that services are available from all locations.
- Your network is separated in several LANs by firewalls, and the local probe cannot monitor specific services across the firewalls.
- You want to monitor systems in a secure network, and you need a secure connection between the PRTG server and this network.
- You want to sniff packets on another computer.
- You want to monitor NetFlow data on another computer.
- You experience performance issues with CPU intensive sensors like packet sniffer or NetFlow sensors and need to distribute the load over more than one PC.

The following chart shows an example for a remote probe scenario.



Monitoring a Distrubuted Network with PRTG

Click here to enlarge: http://media.paessler.com/prtg-screenshots/remote_probes_en.png

The PRTG core server inside the Corporate LAN (bottom right) is able to monitor:

- Services inside the Corporate LAN using the **Local Probe**.
- Services behind a firewall in the Corporate LAN using **Remote Probe 1**.
- Secured services inside the Branch Office (top left) using **Remote Probe 2**.
- Secured services on Mail Server and Web Server using **Remote Probe 3** and **Remote Probe 4** installed directly on these servers.
- Public services on the internet using any of the probes.

How Probes Work

As soon as a probe is started, it automatically connects to the PRTG core server 112, downloads the sensor configuration, and begins its monitoring tasks. The core server sends new configuration data to a probe as soon as the monitoring configuration is changed by the user. Probes monitor autonomously and send the monitoring results back to the core server for each check they have performed.

If the connections between core and probe fail for any reason (for example, a reboot of the computer running the core server) the probe continues monitoring and stores the results. During a connection loss a buffer stores a maximum of 500,000 sensor results in the RAM memory of the remote probe system (up to 50 - 200 MB). This means that for 100 sensors with one minute interval the monitoring results of up to 3 days can be buffered (or 52 minutes for 10,000 sensors with one minute interval). The probe automatically reconnects to the core as soon as it is available again and transmits all monitoring results gathered during the connection loss.

The connection between probe and core is initiated by the probe, secured using Transport Layer Security (TLS). This means that the data sent back and forth between core and probe is not visible to someone capturing data packets. The core server provides an open TCP/IP port and waits for connection attempts from probes. If a new probe connects for the first time, the administrator will receive a ToDo ticket 200 and will then see the new probe in the device tree.

As a security precaution, the probe must be manually acknowledged by the administrator in the device tree before any sensors can be created and monitored. The administrator can also deny a probe which will then be disconnected. No further connection attempts will be accepted and the probe IP is added to the **Deny IPs** list in the probes system settings (see **System Administration—Core & Probes** 2967 section). This ensures that unauthorized probes cannot connect to a core server.

Because the probe initiates the connection, you must ensure that a connection can be established from the outside world to your core server. For example, you may need to open any necessary ports in your firewall and you may need to specify a Network Address Translation (NAT) rule for your network. The process is the same as if you wanted to allow access to the web server provided by the PRTG core server via port 443, for example. Usually it is sufficient to open or forward TCP port 23560 (default) on the machine that runs the core server; on probe side it is not necessary to open any port in most cases.

If you run PRTG in a cluster installation, remote probes also connect to your failover node(s) in addition to the master node and send monitoring data. This works as described above for a single PRTG server. If your master node fails, you can still see monitoring data on your failover (s). You can define the **Cluster Connectivity** of each probe in its **Administrative Probe Settings** 330.

Automatic Probe Update

Whenever a new version of PRTG is installed on the core server, all remote probes will automatically download and install the updated version of the probe as soon as they reconnect to the updated core installation.

The local probe has already been updated during the core installation. All remote probes automatically download the new binaries using the TLS-secured probe or core connection. The download of the 4 MB file takes anywhere from a few seconds (in a LAN) to a few minutes (via internet connections), depending on the available bandwidth. As soon as the update has been downloaded the probe disconnects, installs the update, and reconnects to the core server. This takes between 20 and 100 seconds. Please note that during the update phase the monitoring of the local probe can be affected due to the bandwidth required for the downloads.

If the automatic update of a remote probe fails for some reason, please update the remote probe manually by downloading and executing the installer 3206 on the probe computer. If a remote probe keeps being disconnected after an update, please check if the server with the remote probe has two network connections with different IP addresses. Make sure these addresses are in the list of allowed IPs in the Core & Probes settings 2968.

More

- **Remote Probe Quick Install** 3199
- **Remote Probe Setup** 3206

Video Tutorial: Core Server and Remote Probes

- https://www.paessler.com/support/video_tutorials/distributed_monitoring

13.9.2 Remote Probe Quick Setup

Install a PRTG Remote Probe directly by right-clicking on a device in the PRTG device tree. This semi-automatic installation mechanism is an alternative to the **Remote Probe Setup Using Installer** 3206.

This is an experimental feature. It may not work in all situations. In this case, please see Debugging 3204 and try the standard remote probe installation 93.

This feature is not available in PRTG on demand.

To install a Remote Probe directly from the device tree in the PRTG web interface, follow the steps below.

- Step 1: Meet the Requirements 3199
- Step 2: Prepare the Core Server 3200
- Step 3: Provide Credentials 3202
- Step 4: Install the Remote Probe 3202
- Step 5: Approve the New Remote Probe 3204

Before you start, take a closer look at the requirements in the first three steps.

Do you run PRTG Network Monitor in a cluster? Then mind this important note 3208.

Step 1: Meet the Requirements

To install a probe remotely on a computer please ensure that the following conditions are true.

- The target computer runs the operating system Windows 7 or later.
- The target computer is accessible through Remote Procedure Call (RPC). This is usually the case when your PRTG server and the target computer are located in the same LAN segment. Otherwise, open Windows services.msc on the target computer and start the Remote Procedure Call (RPC) service.
- Programs are allowed to communicate through your Windows Firewall. Open the settings of your Firewall and choose **Allow programs to communicate through Windows Firewall**. Mark the checkbox for **Remote Service Management**, and the checkbox **Public** in the corresponding line.
- Connections between remote probes and the PRTG core server require port 23560. Please open or forward this port in your firewall configuration.

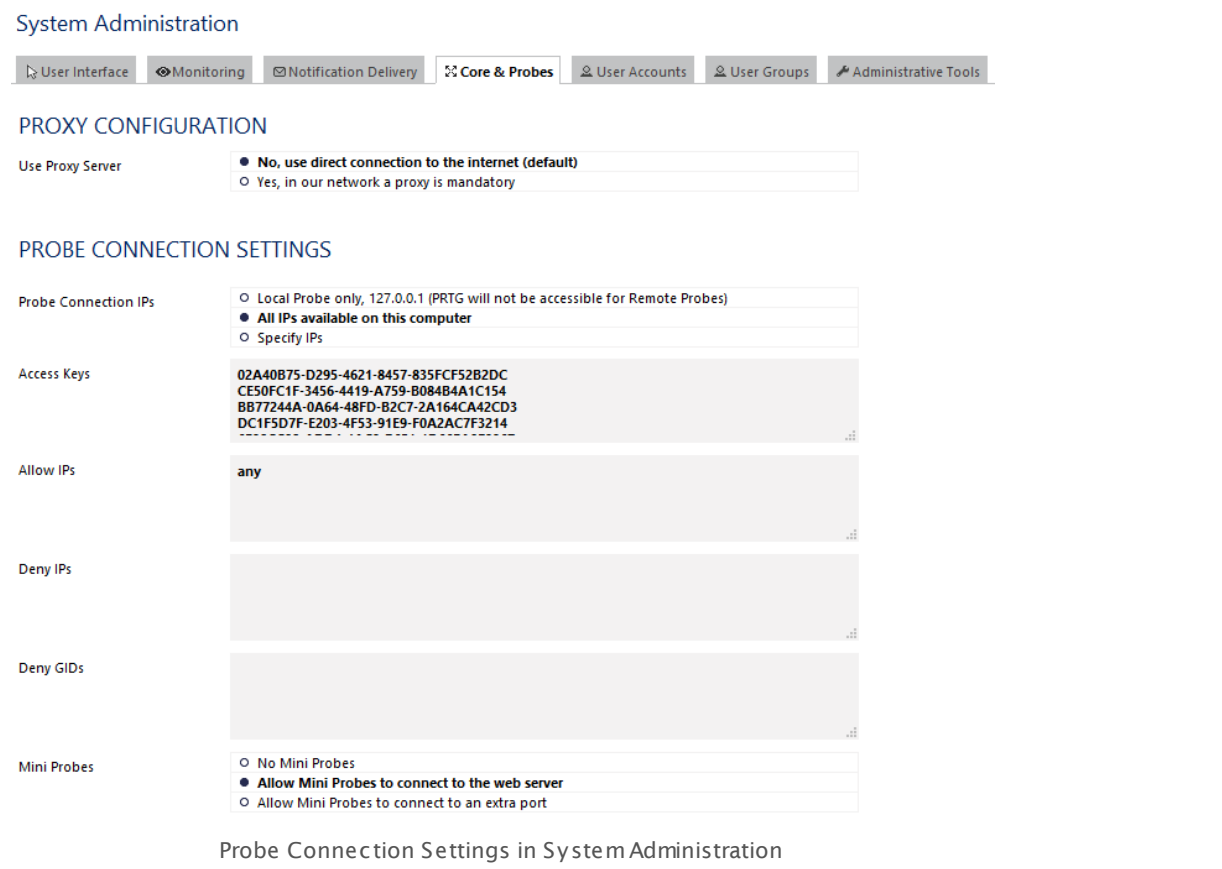
You cannot install a remote probe on the local probe device and the Remote Probe Quick Setup is also not available for devices on remote probes. Please use the Remote Probe Installer 3206.

You cannot install a remote probe on the computer the PRTG core server runs on because the core server already includes a local probe service.

Step 2: Prepare the Core Server

Because your remote probe needs to connect to your PRTG core server, your PRTG core server needs to accept incoming remote probe connections. So, please prepare your PRTG core server first.

Edit the relevant settings in System Administration—Core & Probes 2967. From the main menu in the PRTG web interface 138, select **Setup | System Administration | Core & Probes** to access the probes settings and go to the **Probe Connection Settings**.



Probe Connection Settings in System Administration

By default, a core server accepts connections from the **Local Probe only** (IP address 127.0.0.1). This setting is the most secure setting, but it does not allow any remote probe to connect to your PRTG core server.

To accept remote probes, choose one of the following settings:

- **All IPs available on this computer**: Any IP on your core server system accepts incoming probe connections.
- **Specify IPs**: Specify selected IP addresses that accept incoming connections.

Other settings are:

- In the **Access Keys** field, you can enter a new access key that can be used for a core probe connection. The access key can include arbitrary signs and have arbitrary length. During the remote probe install process PRTG will add an access key automatically, so usually you will not have to define a key here.
- In the **Allow IPs** field, you can enter the IP address of the computer you want to install a remote probe on. To make things easier, you can also enter the word **any:** this will set the core server to accept remote probes connecting from any IP address.
  If you use **any**, make sure you write the word in lower case only! Any other variations will not be valid!
- In the **Deny IPs** field, you can enter the IP address of the computers that you do not want to connect to the PRTG core server.
- In the **Deny GIDs** field, you can enter the global ID (GID) of a device in your network that you do not want to connect to the PRTG core server. Future probe connections from this device will be denied automatically.
  What is a global ID (GID)? It is the ID that PRTG Network Monitor attributes to every device that you include in your monitoring.

When you are done, click **Save** to save your settings. If you click **Cancel**, all changes to the core and probe settings will be discarded.

If you change this setting, PRTG needs to restart the core server to apply your changes. After clicking the **Save** button, a dialog box appears which asks you to confirm the required core server restart. Click **OK** to trigger the restart and follow the instructions on the screen. During the restart all the users of the PRTG web interface, of the **Enterprise Console** 3028, or of **PRTG Apps for Mobile Network Monitoring** 3082 will be disconnected and reconnected.

For further information about the core probe connection settings, see also the **System Administration—Core & Probes** 2967 section.

To edit the core probe connection settings you can also use the **PRTG Administration Tool** 3135 on your core server.

PRTG Cluster and Remote Probes Outside the LAN

If you use the **Clustering** 116 feature of PRTG and you want to run remote probes outside your local network, you have to make sure your cluster nodes and the addresses they use are reachable from the outside! Check your cluster node settings under **System Administration—Cluster** 2992 before installing a remote probe outside your local network. Enter addresses (DNS names or IPs) which are valid for both cluster nodes to reach each other and for remote probes to reach all cluster nodes individually. Remote probes outside your LAN cannot connect to your cluster nodes if they use local addresses.

If you already have a remote probe installed outside your LAN and the probe is disconnected because of this, please follow these steps:

1. Uninstall the current remote probe.
2. Update the cluster node settings 2992 with addresses that are reachable from outside your LAN.

3. Restart your PRTG core servers.
4. Install the remote probe again. It will then obtain the IP address or DNS name entries that it can reach.

See also section **Failover Cluster Configuration—Remote Probes in Cluster** 3215.

Step 3: Provide Credentials

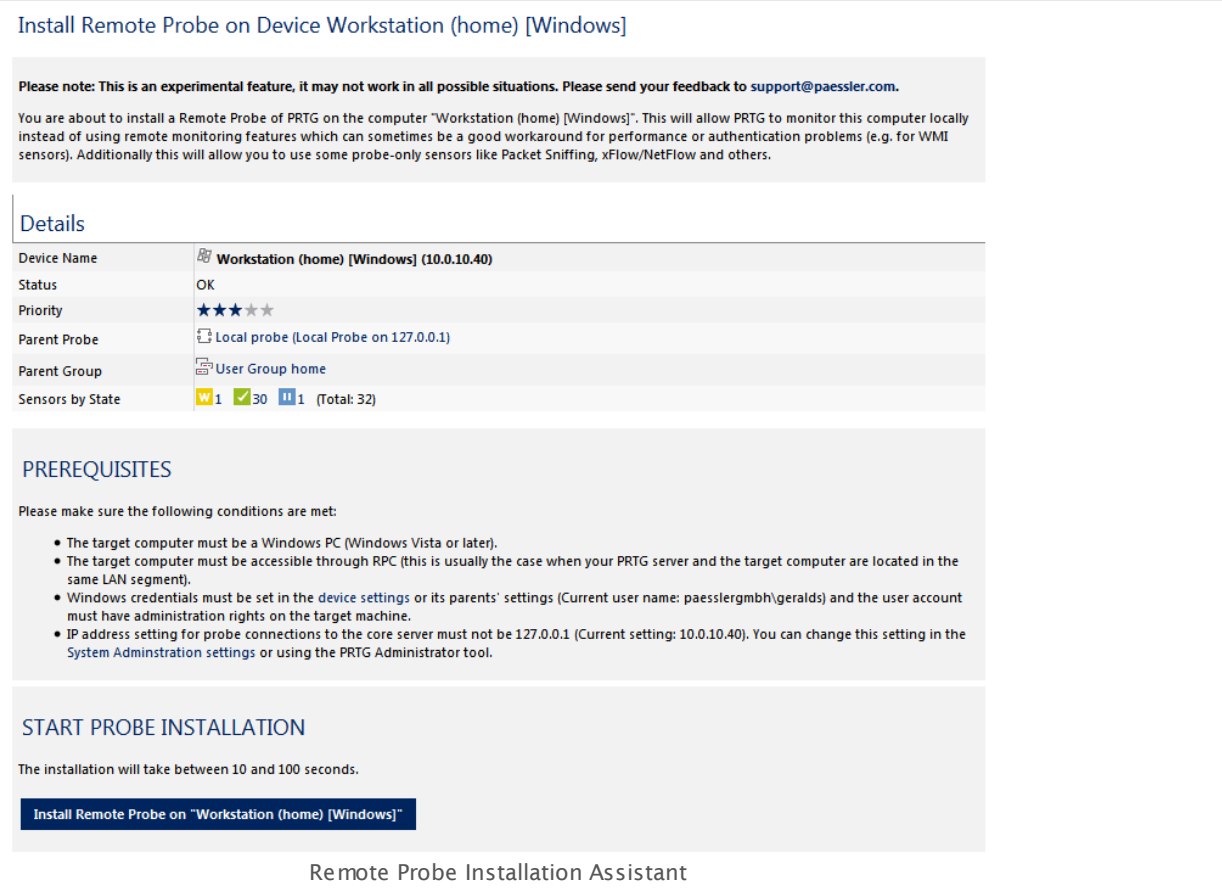
If not done yet, add a device 360 to PRTG that represents the target computer on which you want to install the remote probe. Set the correct Windows credentials for this device.

- Open the **Device Settings** 360.
- In the **Credentials for Windows Systems** section, provide **Domain or Computer Name**, **User**, and **Password** for the target computer.
- You can also inherit 122 the credentials from the settings of a parent object in the device tree.

Make sure this user account has administration rights on the target computer.

Step 4: Install the Remote Probe

- In the device tree overview, open the context menu 222 of the target device.
- Choose **Device Tools | Install Remote Probe...**.
  This option is only available on devices on the PRTG on premises local probe.
- The install assistant will appear on a new page.

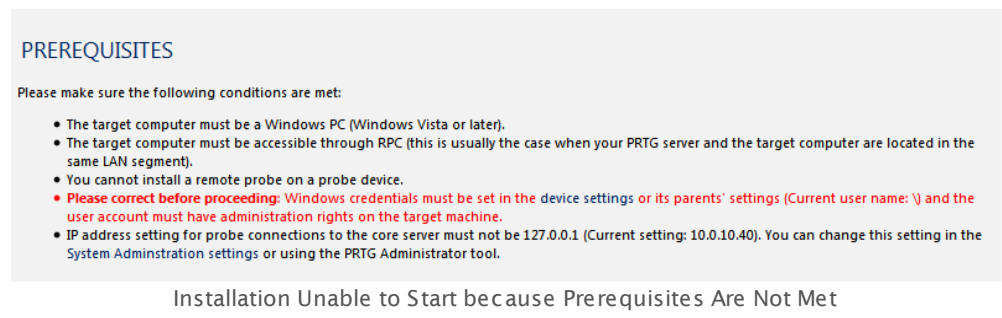


Remote Probe Installation Assistant

The installation assistant is divided into four sections:

- Experimental feature notice and short introduction
- **Details**: Overview about the device: name, status, priority, parent probe, parent group, and sensor states in place with their number
- **Prerequisites**: For details, see Step 1 3199.
- **Start Probe Installation**: Time estimation for installation and installation start button

Make sure you meet the following requirements. If not, PRTG cannot start the installation process. Open requirements are highlighted in red.



Installation Unable to Start because Prerequisites Are Not Met

If everything is okay you can install the remote probe on the target computer by clicking the button **Install Remote Probe on "[device name]"**. Wait until the process has ended.

If the installation was successful, the following message will appear in the **Start Probe Installation** section: **Done. Result is: OK**.

Every time you start an installation, PRTG automatically adds a new key to **Access Keys** in **System Administration—Core & Probes** 2967, no matter if the installation has been successful or not.

Step 5: Approve the New Remote Probe

If the installation was successful, you will receive further instructions after the result message. As indicated, go back to the device tree 151 and acknowledge the new probe. The approval button will appear under the node of the new remote probe. You will also receive a new ToDo ticket 201.

Click **Approve and auto-discover new probe** to acknowledge the created remote probe and instantly start an **Auto-Discovery** 249 in this network. Click **Approve new probe** to acknowledge the remote probe without running an auto-discovery. You can also discard the probe by clicking **Deny new probe**.

When denying or removing a remote probe, this device's global ID (GID) will be included into **Deny GIDs** in **System Administration—Core & Probes** 2967. Future probe connections from this device will be denied automatically.

Denying the remote probe in the PRTG device tree does not uninstall the probe, but only denies access to the core server. The probe will continue to run on the target system until you uninstall it manually.

After approving, the approval button will turn into a **Working** status. Please wait while the probe connects. Once approved, PRTG automatically creates a set of sensors for the probe to ensure that bottle-necks on the probe will always be noticed. We recommend that you keep these sensors. Now you can create groups, devices and sensors to customize your monitoring via the new probe.

Debugging

- Please note that installing a remote probe directly from the device tree in the PRTG web interface is an experimental feature. It may be the case that this approach is not possible in all situations.
- Please follow the steps of this chapter closely when encountering problems with the Remote Probe Quick Install. Especially consider the conditions as described in Step 1 3199 of this section like Windows Firewall settings.
- If the quick installation procedure described in this section does not work with your setup, please install your remote probes manually and see how to do so in **Remote Probe Setup Using Installer** 3206.

More

Knowledge Base: How can I customize PRTG's ports for core-probe-connections?

- https://kb.paessler.com/en/topic/65084

13.9.3 Remote Probe Setup Using Installer

In section **Install a PRTG Remote Probe** 93, we accompany your remote probe installation using the Remote Probe Installer. Here you find further information about necessary settings for a successful core probe connection and debugging tips.

- Step 1: Prepare the Core Server 3206
- Step 2: Download and Install Remote Probe 3209
- Step 3: Approve New Probe and Start Monitoring 3209
- Debugging Probe Connection Problems 3210

For a semi-automatic installation of a Remote Probe directly from the device tree in the PRTG web interface, see section **Remote Probe Quick Setup** 3199.

Do you run PRTG in a cluster? Then mind this important note 3208.

Step 1: Prepare the Core Server

Because your remote probe needs to connect to your PRTG core server, your PRTG core server needs to accept incoming remote probe connections. So, please prepare your PRTG core server first.

Edit the relevant settings in **System Administration—Core & Probes** 2967. From the main menu in the PRTG web interface 138, select **Setup | System Administration | Core & Probes** to access the probes settings and go to the **Probe Connection Settings**.

Probe Connection Settings in System Administration

By default, a core server accepts connections from the **Local Probe only** (IP address 127.0.0.1). This setting is the most secure setting, but it does not allow any remote probe to connect to your PRTG core server.

To accept remote probes, choose one of the following settings:

- **All IPs available on this computer**: Any IP on your core server system accepts incoming probe connections.
- **Specify IPs**: Specify selected IP addresses that accept incoming connections.

Other settings are:

- In the **Access Keys** field, you can enter a new access key that can be used for a core probe connection. The access key can include arbitrary signs and have arbitrary length. During the remote probe install process PRTG will add an access key automatically, so usually you will not have to define a key here.
- In the **Allow IPs** field, you can enter the IP address of the computer you want to install a remote probe on. To make things easier, you can also enter the word **any:** this will set the core server to accept remote probes connecting from any IP address.
  If you use **any**, make sure you write the word in lower case only! Any other variations will not be valid!

- In the **Deny IPs** field, you can enter the IP address of the computers that you do not want to connect to the PRTG core server.
- In the **Deny GIDs** field, you can enter the global ID (GID) of a device in your network that you do not want to connect to the PRTG core server. Future probe connections from this device will be denied automatically.
  What is a global ID (GID)? It is the ID that PRTG Network Monitor attributes to every device that you include in your monitoring.

When you are done, click **Save** to save your settings. If you click **Cancel**, all changes to the core and probe settings will be discarded.

If you change this setting, PRTG needs to restart the core server to apply your changes. After clicking the **Save** button, a dialog box appears which asks you to confirm the required core server restart. Click **OK** to trigger the restart and follow the instructions on the screen. During the restart all the users of the PRTG web interface, of the **Enterprise Console** 3028, or of **PRTG Apps for Mobile Network Monitoring** 3082 will be disconnected and reconnected.

For further information about the core probe connection settings, see also the **System Administration—Core & Probes** 2967 section.

To edit the core probe connection settings you can also use the **PRTG Administration Tool** 3135 on your core server.

PRTG Cluster and Remote Probes Outside the LAN

If you use the **Clustering** 116 feature of PRTG and you want to run remote probes outside your local network, you have to make sure your cluster nodes and the addresses they use are reachable from the outside! Check your cluster node settings under **System Administration—Cluster** 2992 before installing a remote probe outside your local network. Enter addresses (DNS names or IPs) which are valid for both cluster nodes to reach each other and for remote probes to reach all cluster nodes individually. Remote probes outside your LAN cannot connect to your cluster nodes if they use local addresses.

If you already have a remote probe installed outside your LAN and the probe is disconnected because of this, please follow these steps:

1. Uninstall the current remote probe.
2. Update the cluster node settings 2992 with addresses that are reachable from outside your LAN.
3. Restart your PRTG core servers.
4. Install the remote probe again. It will then obtain the IP address or DNS name entries that it can reach.

See also section **Failover Cluster Configuration—Remote Probes in Cluster** 3215.

Step 2: Download and Install the Remote Probe

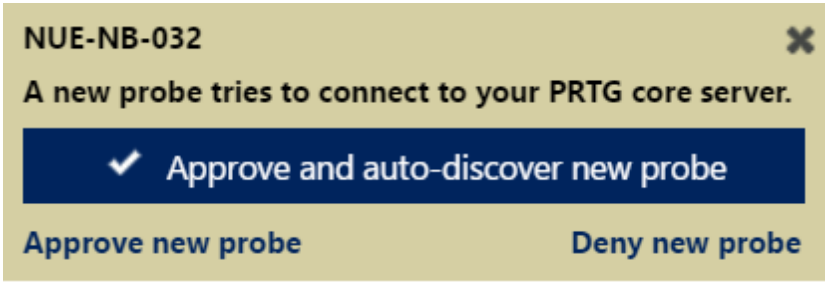
On the computer on which you want to install your remote probe, log in to the PRTG web interface 138, download the setup file, and install it. For more detailed instructions, please follow the steps described in **Install a PRTG Remote Probe** 93.

The PRTG core system already includes a local probe service. This is why you cannot additionally install a remote probe on that system.

The version numbers of core and probe services must match. By default, PRTG updates probes automatically when a new version is installed on the PRTG core server. To update your remote probe manually, open a web browser on your remote computer and download the remote probe installer as described in this manual section.

Step 3: Approve the New Probe and Start Monitoring

Remember to log in to the PRTG web interface to acknowledge your new remote probe!



Remote Probe Approval

If you successfully installed the remote probe from a PRTG on demand installation, you will see the following dialog box.

When you deny or remove a remote probe, PRTG will automatically add this device's global ID (GID) to the **Deny GIDs** list in **System Administration—Core & Probes** 2967. Future probe connections from this device will be denied automatically.

Denying the remote probe in the PRTG device tree does not uninstall the probe, but only denies access to the core server. The probe will continue to run on the target system until you uninstall it manually.

For unwanted probe connections, you can click **Deny new probe**.

When you deny or remove a remote probe, PRTG will automatically add this device's global ID (GID) to the **Deny GIDs** list in **System Administration—Core & Probes** 2967. Future probe connections from this device will be denied automatically.

Once approved, PRTG automatically creates a set of sensors for the probe to ensure you can detect bottle-necks on the probe system immediately. We recommend that you keep these sensors. You can now create groups, devices, and sensors for monitoring via the new probe.

Furthermore, when a new probe connects to the core server for the first time, PRTG creates a new ToDo ticket 201.

Debugging Probe Connection Problems

If you have trouble with your core probe connection, make sure that you meet the following requirements:

- The IP address of the computer on which you want to install a remote probe is not listed in the **Deny IPs** field.
- The default port 23560 for probe connections is not blocked by firewall rules on your core server's side.

If you need to set a different port (not recommended), see this Knowledge Base article: How can I customize PRTG's ports for core-probe-connections?

Furthermore, you can also take a look at the probe's log files. The probe process writes log files with a file name in the format **PRTG Probe Log (x).log**. Open the one with the most recent date.

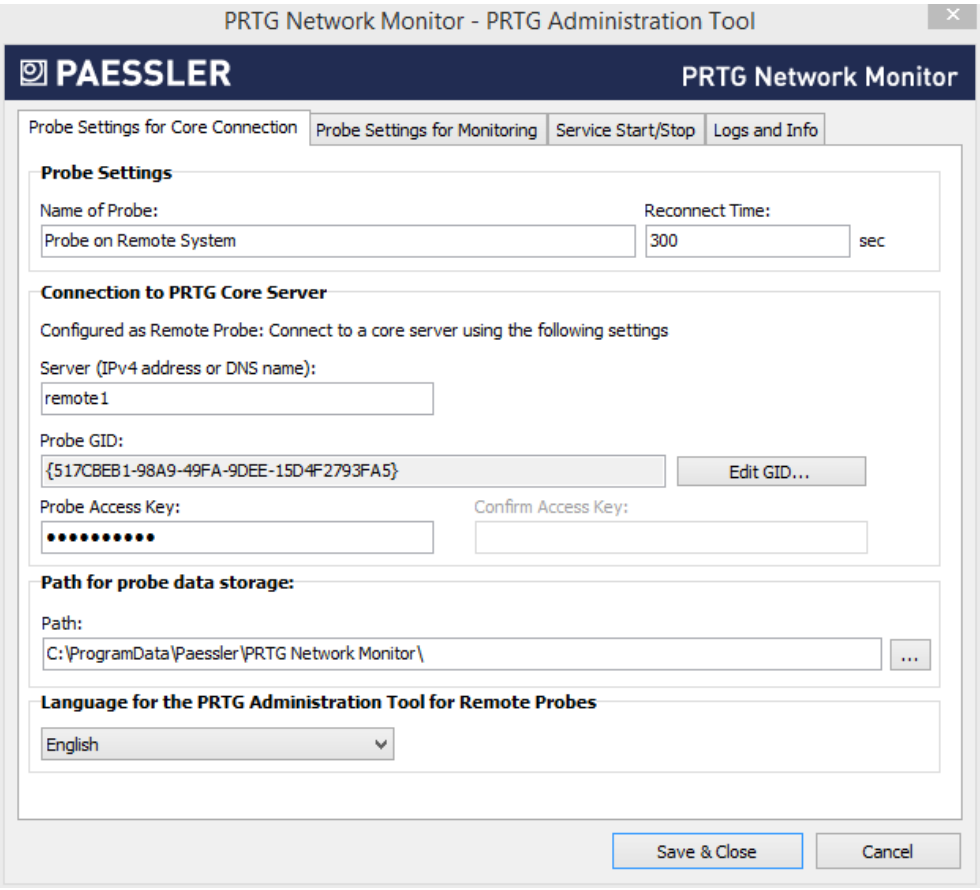
For a correct connection the probe log should look similar to this:

```
11.08.2012 16:15:15 PRTG Probe Server V12.3.2.5101
11.08.2012 16:15:15 Starting Probe on "WINXPVMWARE"
11.08.2012 16:15:15 Data Path: C:\documents and settings\All Users\a[...]
11.08.2012 16:15:15 Local IP: 0.0.0.0
11.08.2012 16:15:15 Core Server IP and Port: 10.0.2.167:23560
11.08.2012 16:15:15 Probe ID: -1
11.08.2012 16:17:01 Connected to 10.0.2.167:23560
11.08.2012 16:17:06 Login OK: Welcome to PRTG
```

If the connection fails, for example due to an incorrect **Access Key**, or due to incorrect **IP** settings (see **Step 2** 3209), you will see:

```
11.08.2012 16:31:02 Try to connect...
11.08.2012 16:31:02 Connected to 10.0.2.167:23560
11.08.2012 16:31:07 Login NOT OK: Access key not correct!
```

If you need to adjust any probe settings for the connection to the core server, use the **PRTG Administration Tool** 3157 on your probe system.



Remote Probe Settings in PRTG Administrator

In the **Connection to PRTG Core Server** tab, you can then edit the following settings:

- **Server**: Enter the IP address or DNS name of the core server the remote probe will connect to. If Network Address Translation (NAT) is used, this has to be the IP address that is externally visible, because the remote probe will connect from outside your network.
- **Probe Access Key** and **Confirm Access Key**: Enter the access key that the probe will send to the core server. This access key has to be defined on the PRTG core server. Make sure the key phrases match exactly.

Remember to always click **Save & Close** to confirm your settings and to (re)start the probe service.

For more detailed information about these settings, see section **PRTG Administration Tool** 3157.

More

Knowledge Base: How can I customize PRTG's ports for core-probe-connections?

- https://kb.paessler.com/en/topic/65084

13.10 Failover Cluster Configuration

PRTG offers single failover clustering in all licenses—even using the freeware edition. A single failover cluster consists of two servers (Current Master node and Failover node), each of them running one installation of PRTG. They are connected to each other and exchange configuration and monitoring data.

This feature is not available in PRTG on demand.

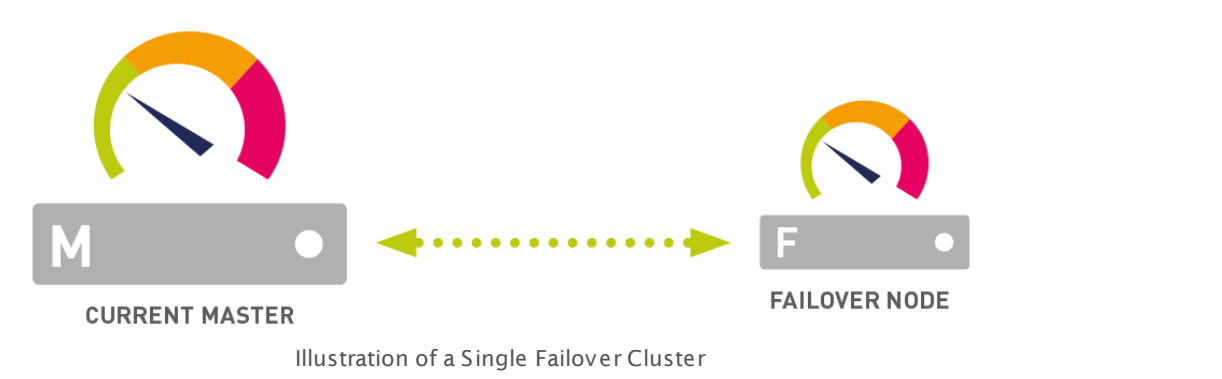


Illustration of a Single Failover Cluster

Click here to enlarge: http://media.paessler.com/prtg-screenshots/clustering-1_en.png

For setting up a cluster you need two or more servers. There is one PRTG core server installation 84 necessary on each of them—with different settings configured for each type of node. In return, you benefit from seamless high-available monitoring with automatic failover and multi-location monitoring.

In a cluster, you can run:

- **1 Master Node**
  On the master node, you set up your devices and configuration. Also notifications, reporting, and many other things are handled by the master node.

- **Up to 4 Failover Nodes**
  You can install one, two, three, or four additional nodes for fail-safe, gapless monitoring. For more than one failover node you need additional licenses 3224. Each of these nodes can monitor the devices in your network independently, collecting their own monitoring data. You can review the data in a summarized way, that enables you to compare monitoring data from different nodes.

During an outage of one node, you will see data gaps for the time of the outage on that node. However, data for that time span will still be available on all other cluster nodes.

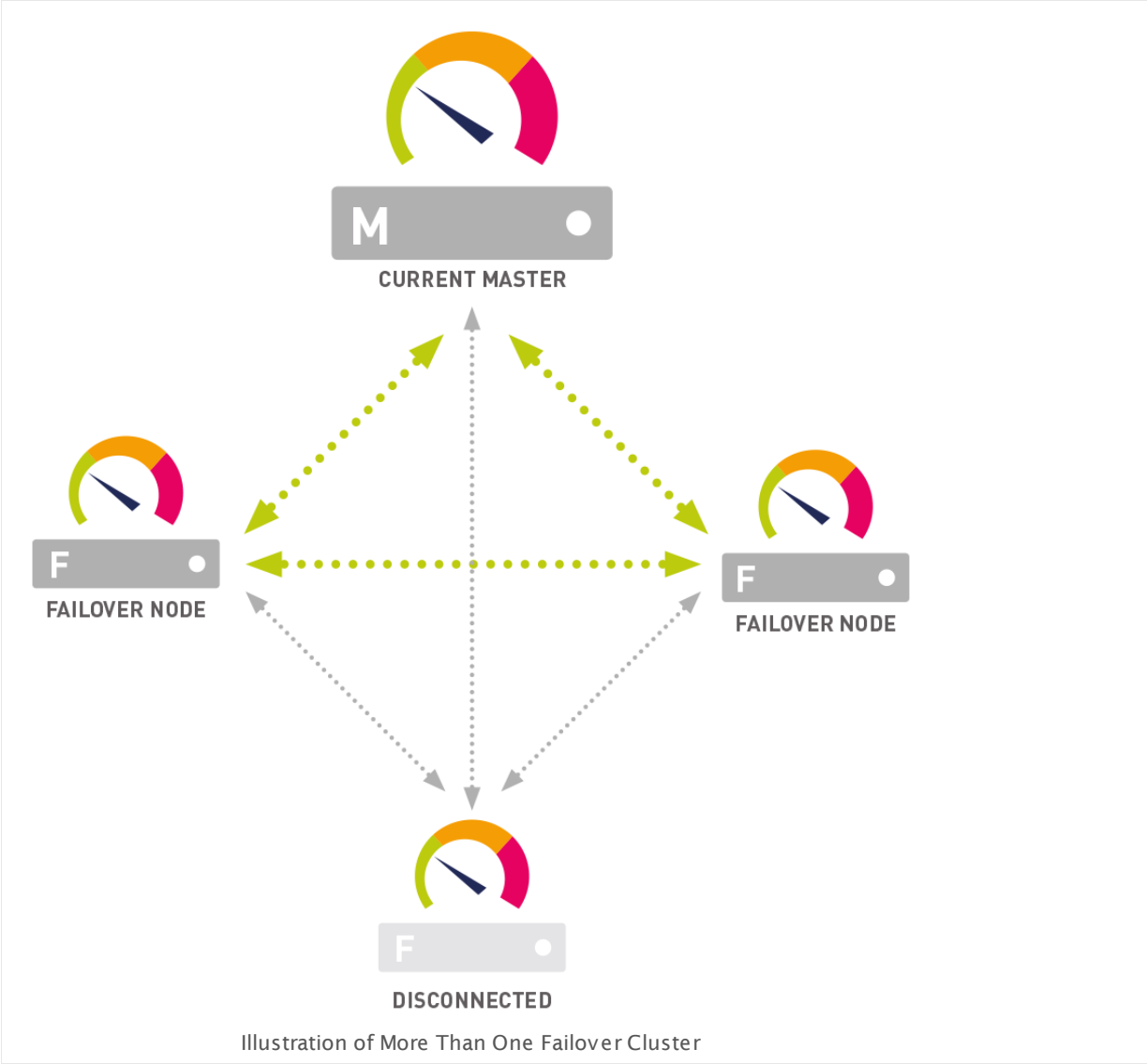


Illustration of More Than One Failover Cluster

Click here to enlarge: http://media.paessler.com/prtg-screenshots/clustering-2_en.png

Before Getting Started: Cluster Notes

Configuring a cluster with one failover node is the most common way to set up a seamless network monitoring with PRTG. You will need two servers running any Windows version (Windows 7 or later). Your servers can be real hardware (strongly recommended!) or virtual machines.

For details, see section Detailed System Requirements 25.

Please consider the following notes about PRTG clustering.

- Your servers must be up and running.

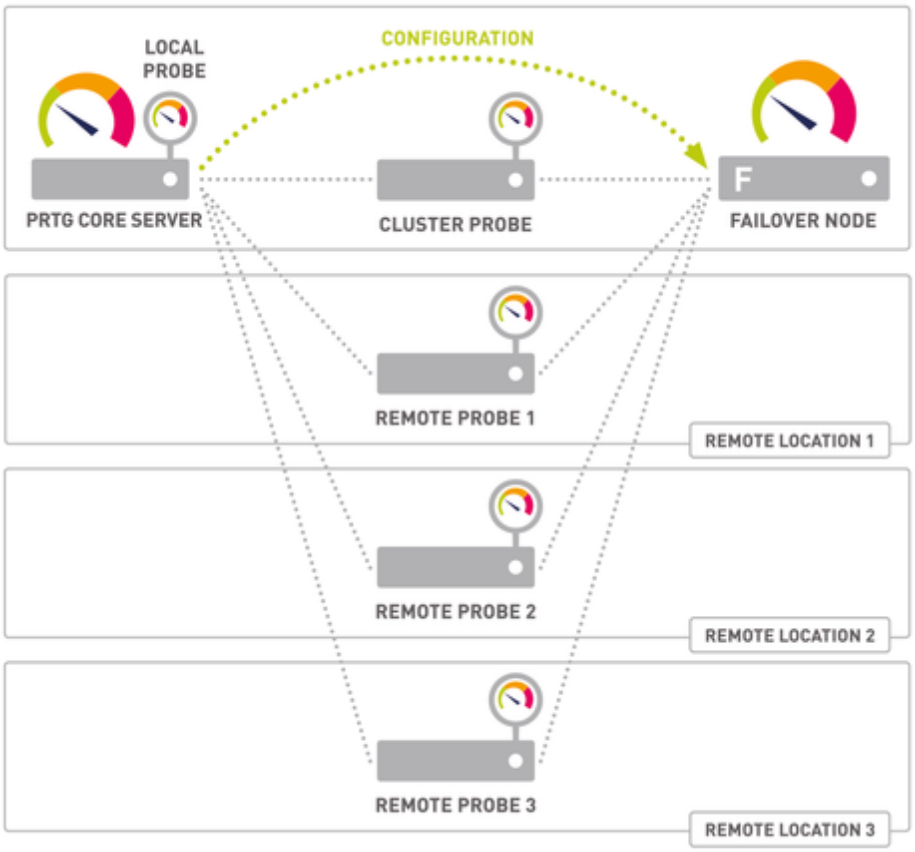
- Your servers must be similar in regard to the system performance and speed (like CPU, RAM memory).
- In a cluster setup, each of the cluster nodes will individually monitor the devices added to the **Cluster Probe**. This means that monitoring load will increase with every cluster node. Please make sure your devices and network can handle these additional requests. Often, a larger scanning interval for your entire monitoring is a good idea. For example, set up a scanning interval of 5 minutes in the **Root Group Settings** 294.
- We recommend that you install PRTG on dedicated real-hardware systems for best performance.
- Please bear in mind that a server running a cluster node may in rare cases be rebooted automatically without notice (for example, because of special software updates).
- Both servers must be visible for each other through the network.
- Communication between the two servers must be possible in both directions. Please make sure that no software or hardware firewall blocks communication. All communication between nodes in the cluster is directed through one specific TCP port. You will define it during cluster setup (by default, it is **TCP port 23570**).
- **Email notifications for failover:** The Failover Master will send notifications if the Primary Master is not connected to the cluster. To ensure that PRTG can deliver emails in this case, please configure the **Notification Delivery** 2961 settings so that PRTG can use them to deliver emails from your failover node as well. For example, use the option to set up a secondary Simple Mail Transfer Protocol (SMTP) email server. This fallback server must be available for the failover master so that it can send emails over it independently from the first email server.
- Make your servers safe! From every cluster node, there is full access to all stored credentials as well as other configuration data and the monitoring results of the cluster. Also, PRTG software updates can be deployed through every node. So, please make sure you take security precautions to avoid security attacks like hackers and Trojans. Secure every node server the same careful way as the master node server.
- Run the nodes in your cluster either on 32-bit or 64-bit Windows versions only. Avoid using both 32-bit and 64-bit versions in the same cluster, as this configuration is not supported and may result in an unstable system. Also, ZIP compression for the cluster communication will be disabled and you may encounter higher network traffic between your cluster nodes.
- If you run cluster nodes on Windows systems with different timezone settings and use **Schedules** 2938 to pause monitoring of defined sensors, schedules will apply at the local time of each node. Because of this, the overall status of a particular sensor will be shown as **Paused** every time the schedule matches a node's local system time. Please use the same timezone setting on each Windows with a cluster node to avoid this behavior.
- The password for the **PRTG System Administrator** login to PRTG is not automatically synchronized on cluster nodes. You need to manually change it on each node. On a failover node, open the **PRTG Administration Tool** 3146 and change the password on the **Administrator** tab. Click **Save&Close** to save your new password.
- Stay below 2,500 sensors per cluster for best performance in a single failover. Clusters with more than 5,000 sensors are not supported. For each additional failover node, divide the number of sensors by two.

In cluster mode, you cannot use sensors which wait for data to be received. Because of this, you can use the following sensor types only on a local or remote probe 112:

- HTTP Push Count 929
- HTTP Push Data 939
- HTTP Push Data Advanced 951
- IPFIX 1063 and IPFIX (Custom) 1075
- jFlow V5 1095 and jFlow V5 (Custom) 1107
- NetFlow V5 1207 and NetFlow V5 (Custom) 1219
- NetFlow V9 1230 and NetFlow V9 (Custom) 1242
- Packet Sniffer 1278 and Packet Sniffer (Custom) 1289
- sFlow 1457 and sFlow (Custom) 1469
- SNMP Trap Receiver 2143
- Syslog Receiver 2309

Remote Probes in Cluster

PRTG provides cluster support for remote probes. This means that all your probes can connect to all your cluster nodes, the primary master node as well as the failover node. Because of this you can still see monitoring data of remote probes and sensor warnings and errors even when your master node fails.



Remote Probes with Cluster Connectivity

Please consider the following notes about PRTG clustering with remote probes.

- You have to allow remote probe connections to your failover nodes. To do so, log in to each server in your cluster and open the **PRTG Administration Tool** 3139. On the **Core Server** tab, define to accept connections from remote probes on each cluster node.
- If you use remote probes outside your local network: You have to use IP addresses or DNS names for your cluster nodes that are valid for both the cluster nodes to reach each other and for remote probes to reach all cluster nodes individually. Open the **System Administration—Cluster** 2992 settings and adjust the entries for cluster nodes accordingly so that these addresses are reachable from the outside. New remote probes try to connect to these addresses but cannot reach cluster nodes which use private addresses.
- If you use Network Address Translation (NAT) with remote probes outside this NAT: You have to use IP addresses or DNS names for your cluster nodes that are reachable from the outside. If your cluster nodes are inside the NAT and the cluster configuration only contains internal addresses, your remote probes from outside the NAT will not be able to connect. The PRTG core server must be reachable under the same address for both other cluster nodes and remote probes.
- A remote probe only connects to the PRTG core server with the defined IP address when starting. This PRTG server must be the **Primary Master**!

- Initially, existing remote probes are not visible on failover nodes. You need to set their **Cluster Connectivity** first in the **Administrative Probe Settings** 330 to be visible and working with all cluster nodes. Choose option **Probe sends data to all cluster nodes** for each remote probe that you want to connect to all cluster nodes.
- Newly connected remote probes are visible and working with all cluster nodes immediately after you have acknowledged the probe connection. The connectivity setting **Probe sends data to all cluster nodes** is default for new probes.
- As soon as a probe is activated for all cluster nodes, it connects automatically to the correct IP addresses and ports of all cluster nodes.
- Once a remote probe has connection data from the Primary Master, it can connect to all remaining cluster nodes also when the Primary Master fails.
- Changes to connection settings of cluster nodes are automatically sent to your remote probes.
- If a PRTG server (which is a cluster node) in your cluster is currently not running, your probes will deliver monitoring data 3197 after the restart of this server. This happens individually for each PRTG server in your cluster.
- If you switch on cluster connectivity for a probe, it will not deliver monitoring data from the past when cluster connectivity was off. For sensors using difference values, the difference between the current value and the last value is shown with the first new measurement (if the respective sensor previously sent values to the PRTG server).
- Except for this special case, all PRTG servers show the same values of sensors on devices you add to the Cluster Probe.
- The responsible PRTG server for the configuration and management of a remote probe is always the master that is currently active. This means that all tasks of the PRTG core server are only executed by the current master. If you use a split cluster with several master nodes, only the master that appears first in the cluster configuration is responsible.

You can use remote probes in a cluster as described above, which is showing monitoring data of all your probes on all nodes in your cluster. However, you cannot cluster a remote probe itself. To ensure gapless monitoring for a specific remote probe, install a second remote probe on a machine in your network next to the existing probe, and create all devices and sensors of the original probe on it. For example, you can clone 2812 the devices from the original probe. The second probe would be a copy of the first probe then and you can still monitor the desired devices if the original probe fails.

Probes that send data to all cluster nodes result in increased bandwidth usage. Choose the option **Probe sends data only to primary master node** in the **Administrative Probe Settings** 330 for one or more remote probes to lower bandwidth usage if necessary.

Please explicitly check on each cluster node if a remote probe is connected. PRTG does not notify you if a remote probe is disconnected from a node in the cluster. For example, log in to the PRTG web interface on a cluster node and check in the device tree if your remote probes are connected.

Start Now!

Ready to get started? Please go to section **Failover Cluster Step by Step** 3219!

More

Knowledge Base: What's the Clustering Feature in PRTG?

- https://kb.paessler.com/en/topic/6403

Knowledge Base: What are the bandwidth requirements for running a PRTG Cluster?

- https://kb.paessler.com/en/topic/8223

Knowledge Base: What is a Failover Master and how does it behave?

- https://kb.paessler.com/en/topic/7663

Knowledge Base: I need help with my PRTG cluster configuration. Where do I find step-by-step instructions?

- https://kb.paessler.com/en/topic/41913

Knowledge Base: PRTG Cluster: How do I convert a (temporary) Failover Master node to be the Primary Master node?

- https://kb.paessler.com/en/topic/34853

Paessler Blog: Cluster Support for Remote Probes: Failover Nodes Show Remote Probe Data

- https://www.paessler.com/blog/2015/07/02/all-about-prtg/cluster-support-for-remote-probes

13.10.1 Failover Cluster Step by Step

This section will guide you through a step-by-step process to set up a failover cluster. Please follow these instructions carefully to successfully integrate two or more PRTG installations into one failover cluster.

Before getting started, please make sure you consider the information in section **Failover Cluster Configuration** 3212.

This feature is not available in PRTG on demand.

Step 1: Install Core Servers

We will start with setting up a single failover cluster, consisting of two PRTG core server installations, each running on an individual server. Please use your license key twice to install the PRTG core server on two different computers.

If you already run an installation of PRTG, this will be your future Master Node. In this case, please install a second core server on another computer only. Make sure you use the same license key for both installations.

Before you start to set up a cluster, please make sure you run exactly the same PRTG version (build number) on all (future) nodes (install updates for existing installations, if necessary).

Once the cluster is established, any updates you install on one node will be deployed to all other cluster nodes automatically.

For details about the installation process, please see **Install a PRTG Core Server** 84.

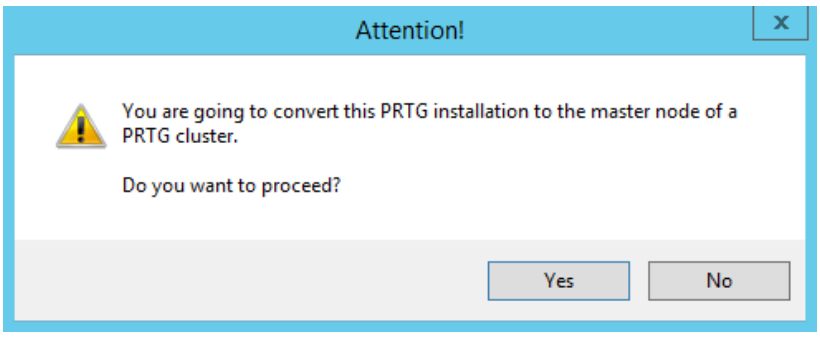
Step 2: Configure Master Node

Decide which of your PRTG core server installations will be your future Master Node. If you already run an installation of PRTG in your network for some time, this should be your master, so your existing monitoring configuration is being kept.

On the Master Node server, from the Windows start menu, open the **PRTG Administration Tool** 3141. On the Cluster tab, click on the following button:

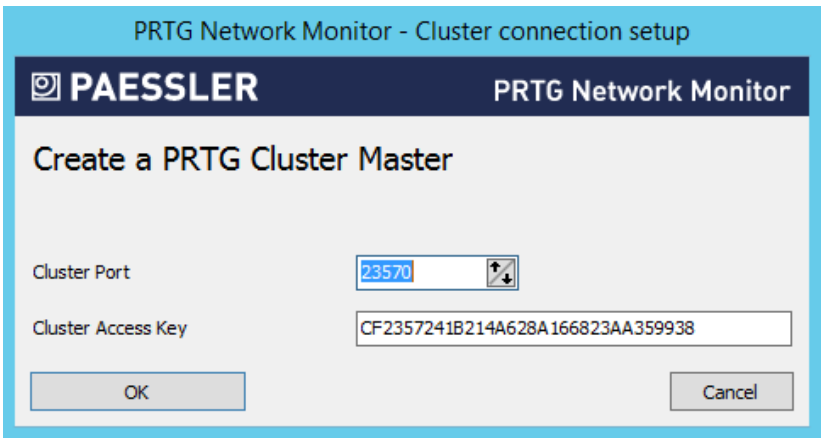
Create a PRTG Cluster...

- Click this button to start creating a cluster. The current PRTG core server will then be the **Master Node** of your cluster.
- Click **Yes** to confirm the conversion of this installation into a cluster master node.



Converting an Installation into a Cluster Master Node

- A new dialog box will appear.



PRTG Administrator: Creating a Cluster Master

- Enter a **Cluster Port**. This is the port on which the internal communication between the different cluster nodes is sent. Make sure connections between cluster nodes are possible on the selected port.
- Enter or paste a **Cluster Access Key**. This is a unique access key. All nodes in a cluster have to be configured with the same cluster access key in order to join the cluster. Connection attempts with the wrong access key will be rejected.
- We recommend that you use the default value.
- Save the **Cluster Access Key** so you have it at hand when configuring your **Failover Node (s)**.
- After confirming your settings you will be asked to restart Windows services. Please do so in order for your changes to take effect.

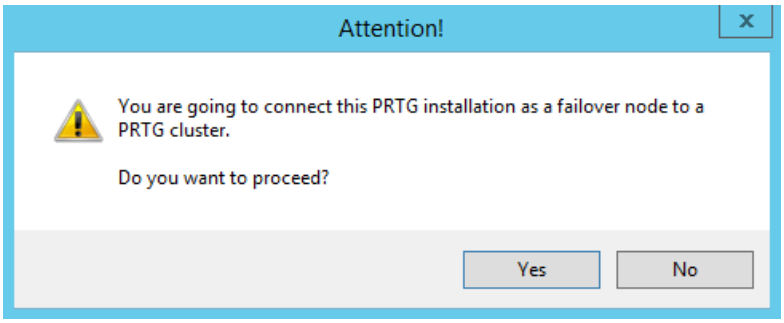
Step 3: Configure Failover Node

On the server that will be your Failover Node, open the PRTG Administration Tool 3141. On the Cluster tab, click the following button:

Join a PRTG Cluster...

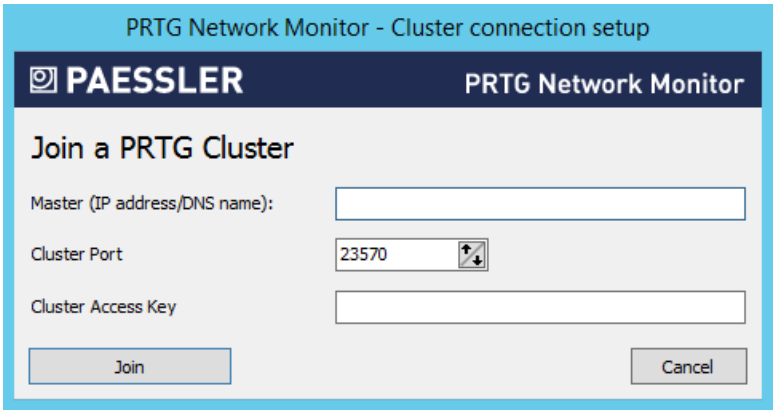
- Click this button to add this installation to an existing cluster that already has a **Master Node**. The current PRTG core server will then be a **Failover Node** in the cluster.

- This button is also available if you are currently running your PRTG installation in **Cluster Mode: Master Node**. This option will then change your master node to a failover node!
- Click **Yes** to confirm the conversion of this installation into a failover node.



Converting an Installation into a Cluster Failover Node

- A dialog box will appear.



PRTG Server Administrator

- Enter a **Master IP address/DNS name** for your cluster. It must be reachable from the machine running the failover node.
- Enter the other settings as defined in the settings of your **Master Node.** Please make sure you use the same settings on all nodes in your cluster.
- Enter a **Cluster Port**. This is the port on which the internal communication between the different cluster nodes is sent. Make sure connections between cluster nodes are possible on the selected port.
- Enter or paste a **Cluster Access Key**. This is a unique access key. All nodes in a cluster have to be configured with the same cluster access key in order to join the cluster. Connection attempts with the wrong access key will be rejected.
- After confirming your settings you will be asked to restart Windows services. Please do so in order for your changes to take effect.

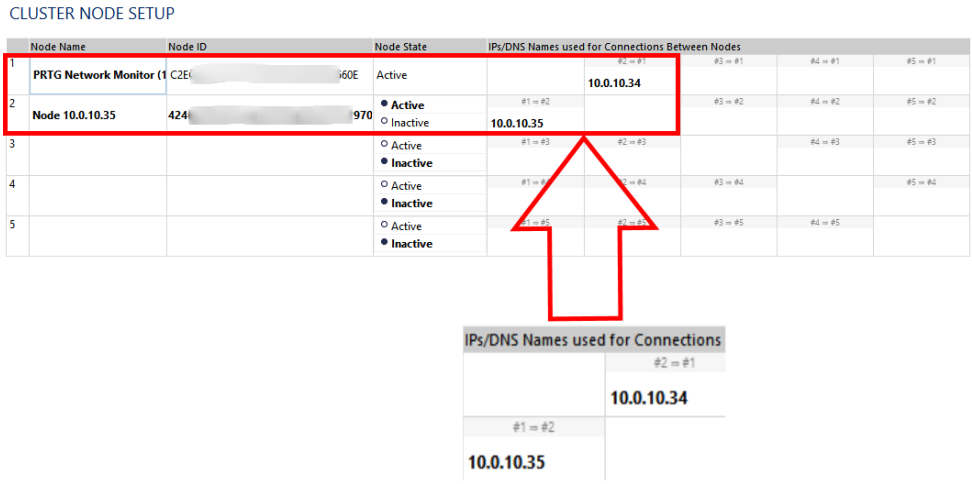
Step 4: Confirm Failover Node

Now you need to confirm the new failover node by setting it to **Active** in the master node's settings.

In a browser window, log in to the PRTG web interface 138 of the Master Node server.

In the **System Administration—Cluster** 2992 settings, you will see your "Master Node" server in the first line of the cluster list and your "Failover Node" server below.

If you use remote probes 3196 outside your local network, for each core server in the cluster use a DNS name or IP address that the probes can reach from the outside. Enter the entries in the **Cluster Node Setup** 2992 table accordingly (see below). The addresses must be valid for both the cluster nodes to reach each other and for remote probes to reach all cluster nodes individually. Remote probes outside your LAN cannot reach private IP addresses or DNS names!

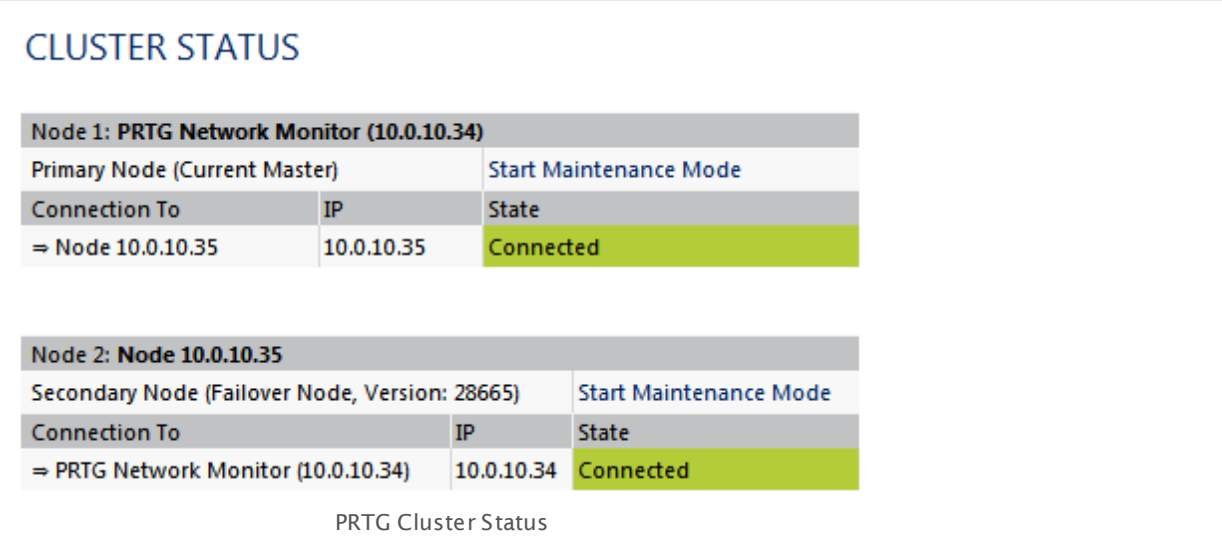


System Administration: Cluster Node Setup

For the "Failover Node", set the radio button for **Node State** to **Active** and **Save** the changes. The nodes will now connect and exchange configuration data. This may take a few minutes.

Step 5: Check Cluster Connection

In two browser windows, log in to the PRTG web interfaces of both of your PRTG installations. Open the cluster status page in both windows by clicking on the narrow cluster information bars at the top of each window. You should see a cluster status with your two nodes in a **Connected** state after a few minutes.


CLUSTER STATUS

Node 1: **PRTG Network Monitor (10.0.10.34)**		
Primary Node (Current Master)		Start Maintenance Mode
Connection To	IP	State
⇒ Node 10.0.10.35	10.0.10.35	Connected

Node 2: **Node 10.0.10.35**		
Secondary Node (Failover Node, Version: 28665)		Start Maintenance Mode
Connection To	IP	State
⇒ PRTG Network Monitor (10.0.10.34)	10.0.10.34	Connected

PRTG Cluster Status

Step 6: Trouble Shooting

Having any problems? If your nodes cannot connect, please see

- the cluster log entries on the **PRTG Status—Cluster Status** 3010 page of the web interface
- the core server log file, a text file in the logs directory of your PRTG data folder (see section **Data Storage** 3226).

In the latest entries of these logs, you can see messages about any errors that might have occurred. These will give you hints on where to find a solution.

If you encounter connection problems between the two cluster nodes, please make sure no software or hardware firewall is blocking communication on the cluster port defined during cluster setup. Communication between the nodes must be possible in both directions in order for the cluster to work properly.

Step 7: Move Sensors to the Cluster Probe Now

That's it. You have successfully set up your failover cluster. All devices that you create or move under the **Cluster Probe** are monitored by both servers.

To monitor your existing configuration via all cluster nodes, on your master node, please move your groups, devices, and sensors from the local probe to the cluster probe! Objects, including their settings, will then be transferred to all cluster nodes automatically.

Step 8: Move Custom Content to Failover Nodes

On startup of the cluster master node, maps 2885 and custom lookups 3183 are automatically transmitted to the failover nodes. While changes to maps are automatically synchronized, you have to manually (re-)load lookups 3192 on all nodes. Other custom content has to be copied manually from the according folders 3226 on the master node to the same folders on the failover nodes:

- Device templates 2818: **\devicetemplates** subfolder of PRTG
- Custom sensors 2778: **\Custom Sensors** subfolder of PRTG
- MIB files 3088: **\MIB** subfolder of PRTG
- SNMP libraries 1913: **\snmplibs** subfolder of PRTG
- Notifications 2916: **\Notfications** subfolder of PRTG
- The **\webroot** subfolder of PRTG if you customized the PRTG web interface, for example

Add More Failover Nodes

If you want to add an additional failover node to your cluster, you will need an additional license key for two and three failover nodes, and two additional license keys to run four failover nodes.

In a cluster, only core servers running on the same size of license 21 can be combined. For example, you can use several "PRTG 5000" licenses or several "PRTG 1000" licenses in one cluster. To add another failover node to your cluster, please set up a new PRTG core server installation on a new server, using an additional license key. Then proceed with **Step 3** 3220 and following. Use a second license key to set up both your second and third failover node, and use a third license key to set up your fourth failover node. Each failover cluster is technically limited to five cluster nodes: as a maximum, you can run one master node and four failover nodes in one cluster.

Stay below 2,500 sensors per cluster for best performance in a single failover. Clusters with more than 5,000 sensors are not supported. For each additional failover node, divide the number of sensors by two.

More

Knowledge Base: My PRTG Cluster is messed up. How can I start over?

- https://kb.paessler.com/en/topic/41903

Advanced Topics

- **Active Directory Integration** 3171
- **Application Programming Interface (API) Definition** 3174
- **Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors** 3175
- **Channel Definitions for xFlow, IPFIX, and Packet Sniffer Sensors** 3180
- **Define IP Ranges** 3182

- Define Lookups 3183
- Regular Expressions 3193
- Add Remote Probe 3195
- Failover Cluster Configuration 3212
- Data Storage 3226
- Using Your Own SSL Certificate 3228
- Calculating Percentiles 3194

13.11 Data Storage

PRTG stores the monitoring configuration, monitoring data, logs, tickets, and reports, as well as support and debug data into different folders on the core server or the system running a **Remote Probe** 3195. Additionally, there is data from PRTG in the program directory (for example, scripts for your custom sensors 2778) and in the Windows registry.

You can find data in different locations. For detailed information, see this Knowledge Base article: How and where does PRTG store its data?

You cannot access these directories on the PRTG on demand core server system.

PRTG Program Directory

32-bit systems:

```
%programfiles%\PRTG Network Monitor
```

64-bit systems:

```
%programfiles(x86)%\PRTG Network Monitor
```

These are the default paths. If you specified another installation directory, you will find your data there.

PRTG Data Folder

On Windows Vista (not officially supported), Windows 7, Windows 2008, Windows 8, and Windows 2012:

```
%programdata%\Paessler\PRTG Network Monitor
```

On Windows XP and Windows Server 2003 (both are not officially supported):

```
%ALLUSERSPROFILE%\Application data\Paessler\PRTG Network Monitor
```

These are the default paths, depending on your Windows version. If you specified a custom path for data storage, please look it up in the **PRTG Administration Tool** 3139: Open this application and switch to the **Core Server** tab. You will find the path there.

Windows Registry

System settings on 32-bit systems:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Paessler\PRTG Network Monitor
```

System settings on 64-bit systems:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Paessler\PRTG Network Monitor
```

Enterprise Console settings:

```
HKEY_CURRENT_USER\Software\Paessler\PRTG Network Monitor\WinGUI
```

HTTP Full Web Page Sensor: Cached Files

If you use the HTTP Full Web Page Sensor, files might be cached in this directory;

```
C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.
```

More

Knowledge Base: How and where does PRTG store its data?

- https://kb.paessler.com/en/topic/463

13.12 Using Your Own SSL Certificate with PRTG's Web Server

This section gives you a brief overview on how to use your own trusted SSL certificate files with the PRTG web server.

This only applies to PRTG on premises instances, not to PRTG on demand.

What is SSL?

PRTG supports Secure Sockets Layer (SSL) to encrypt all data entered and shown in the **Web Interface** 136, in the **Enterprise Console** 3028, or in the **Smartphone Apps** 3082. This ensures that no sensitive information can be intercepted when sending data between the PRTG core server and your client software.

By default, PRTG is already delivered with an SSL certificate so you can use secure connections to your PRTG core server. However, these certificate files are not signed by a valid authority, which is why browsers show an **SSL Certificate Warning** 142 when you try to access the web interface. Despite this warning your connection is still encrypted successfully.

To remove the browser warning, you can obtain a certificate that is valid for your own domain name and signed by a valid authority. You can request your own trusted certificate from an issuer like GoDaddy, DigiCert, InstantSSL, or StartSSL, for example. The certificate must be provided in a suitable format and you have to import it correctly for your PRTG server.

Importing Trusted SSL Certificates for PRTG

There are many different issuers for certificates, and there are different formats certificates can be provided in. PRTG needs three different files, named correctly, containing data in the expected encoding and format. This can the manual import of an issued certificate slightly complicated, because there are various certificate files that you must retrieve from a certificate authority (CA). So, to ease the installation of a trusted certificate, we provide the freeware tool **PRTG Certificate Importer**.

The PRTG Certificate Importer combines and converts all files that a CA bundle contains automatically for the use with PRTG and stores the certificate files into the correct path on your PRTG server. In the best case, you just provide the path to your received CA bundle and let the tool do the rest. We strongly recommend that you use the PRTG Certificate Importer if you want to install a trusted certificate for PRTG!

For more information about this tool and a download link, see the Paessler website: PRTG Certificate Importer

Manual Certificate Import

Although we recommend that you use the PRTG Certificate Importer because it is much more comfortable, you still can import your trusted certificate manually. If you do so, please note that PRTG requires three different certificate files in a PEM encoded format and an unencrypted private key:

- **prtg.crt**: This is the certificate for your PRTG server. It has to be stored in PEM encoded format.

- **prtg.key**: This is the private key matching your server certificate. It has to be stored in PEM encoded format and may not be encrypted! Please make sure that you provide this file in decrypted format! The best way to check this is to open the file in a text editor. If you find a line containing the word "ENCRYPTED", the file still needs to be decrypted before you can use it with PRTG. Please decrypt using an SSL tool (for example, OpenSSL) and your key password.
- **root.pem**: This is the public root certificate of your certificate's issuer. It has to be stored in PEM encoded format and must contain all necessary root certificates of your issuer in one file. If there is more than one PEM encoded root certificate, please use a text editor to copy all of them into a single file (the order does not matter).

PEM encoded files must not contain Unix line breaks! Only Windows line breaks are supported.

Once ready, copy these three files to the **/cert** sub folder of your PRTG program directory (please backup existing files) and restart your PRTG core server service (see **PRTG Administration Tool** 3151).

PRTG services will not be able to start if the files are not provided in exactly the expected format!

For detailed instructions and examples, installation descriptions for various certificates (including Wildcard certificates), as well as links to certificate tools and converters, please see the **More** 3229 section below.

More

Freeware Network Tools: PRTG Certificate Importer—Installing Trusted SSL Certificates for PRTG Network Monitor

- https://www.paessler.com/tools/certificateimporter

Knowledge Base: How can I establish a secure web interface connection to PRTG?

- https://kb.paessler.com/en/topic/273

Knowledge Base: How can I use a trusted SSL certificate with the PRTG web interface?

- https://kb.paessler.com/en/topic/283

Part 14

Appendix

14 Appendix

Please find further information about PRTG and used terms in the following sections.

- Glossary 3233
- List of Abbreviations 3237
- List of Icons 3242
- Support and Troubleshooting 3243
- Legal Notices 3254
- Differences between PRTG on premises and PRTG on demand 3244

14.1 Glossary

This section explains special words used in the context of PRTG Network Monitor.
Here, only explanations are given. For information on where to find detailed instructions for a specific key word, please see the **Index** section.

Channel

The monitoring data of a sensor is shown in sensor channels. For example, for sensors that measure network traffic, there is one channel each for traffic in and traffic out. You can set various triggers for each channel, so you can define sensor status changes or notifications based on the monitoring data received.

Cluster

You can configure PRTG as a failover cluster for fail-safe monitoring. In a cluster, one or more core servers work together in one configuration. Every node can monitor every device in a network for gapless monitoring, so you can additionally compare monitoring results measured from different perspectives.

Cluster Node

Sometimes used as synonym for Node.

Cluster Probe

When running PRTG in cluster mode, a cluster probe is automatically created. All objects created on the cluster probe or below in the device tree are monitored by all nodes in the cluster. Create or move objects there to monitor them fail-safely. If one node fails, the other nodes will continue to monitor them. You can add groups and devices to the probe. On a PRTG installation, the cluster probe runs as part of this installation's local probe. Your remote probes can send monitoring data to your cluster nodes so you can view the data of each probe on each cluster node.

Core Server

The central unit of PRTG. It receives monitoring data from the probe(s) and handles reporting and notifications, provides the web server for the user interfaces, and many other things. In a cluster, one core server is installed on every node.

Dashboard

In the **Home** menu of the web interface are several pre-configured dashboards available that show a quick overview of the overall status of your monitoring configuration. You can create custom dashboards using the Maps function.

Device

A device in PRTG represents a "real" physical device in the network. For an easily understandable tree structure, you usually create one PRTG device for each physical device you want to monitor (exceptions apply to some sensors that you can only create on the local probe 3235 device, and for sensor types that are not bound to a certain device, such as HTTP sensors, which are also usually created on the local probe). You can add one or more sensors 3236 on every device.

Device Tree

The configuration of PRTG is represented in a hierarchical tree structure, the device tree, containing all objects 3235. While building the tree, you can relate to your network's topology to make your monitoring setup easy to understand.

Failover Master (Node)

If the primary master 3235 node fails, a failover node 3234 is promoted to current failover master and takes over the master role until the primary master node re-joins the cluster 3233.

Failover Node

In a cluster 3233 a failover node monitors all sensors 3236 on the cluster probe 3233, providing monitoring data for the core server 3233. Additionally, it serves as a backup in case the master node 3235 fails.

Geo Maps

Geo Maps show the different locations of your devices on a map, depending on the location data that you provide in the settings of groups or devices. The tiles on the maps that represent your devices also show the overall status of a location. This is useful for monitoring distributed networks.

Group

A group is an organizational unit in your PRTG tree structure that helps to arrange your devices. You can add devices or additional sub-groups to existing groups. This way you can model your physical network's topology within the PRTG configuration.

Library

Libraries are a way to show parts of your device tree 3234 in a different layout or with different filters enabled. There is an editor available that allows you to create libraries directly in your browser.

Local Probe

The local probe is installed together with the core server. All objects created on the local probe, or below it in the device tree, are monitored by the local core system. You can add groups and devices to the probe.

Map

Maps (sometimes referred to as "dashboard") are a way to present monitoring the way you want to arrange it. There is an editor available that allows creating maps directly in your browser.

Master Node

In a cluster, the master node controls the settings and cluster management. It also takes over notifications. All changes to the monitoring configuration are made on the master node.

Node

In a cluster there is one master node and one or more failover nodes. On each node, one PRTG core server installation is running independently. All nodes are connected to each other, exchanging configuration and monitoring data.

Object

All different items in the device tree are generally referred to as objects or monitoring objects. An object can be a probe, a group, a device, or a sensor.

Primary Master (Node)

The primary master node in a cluster is the node that is master by configuration. Only if it fails, one of the failover nodes becomes failover master and takes over the master role until the primary master node re-joins the cluster.

Probe

On a probe, the actual monitoring takes place. A probe can run as local probe on the local system where the core server is installed. There are also cluster probes and remote probes.

Remote Probe

A remote probe is a small piece of software installed on a computer in the local or remote network. It scans the network from there and sends monitoring results to the core server 3233. Once the connection is established, the remote probe is shown in the PRTG tree structure. All objects 3235 created on the remote probe, or below it in the device tree 3234, are monitored by the remote system running the remote probe. You can add groups 3234 and devices 3234 to the probe. In a cluster 3233, remote probes can connect to all cluster nodes so you can view monitoring data of a probe on all nodes.

Sensor

A sensor monitors one aspect of a device 3234. For example, monitoring if a device responds to a Ping request is done by one sensor. Monitoring the traffic of one Ethernet port of a router device is done by another sensor. For monitoring the CPU load of the local system yet another sensor is set up, and so on. The data of sensors is shown in their respective channels 3233.

Sensor Tree

Sometimes used as synonym for device tree 3234.

Tickets

Tickets 200 are created by the system or a PRTG user and contain important messages or action steps for the administrator or another specific user to take. Every ticket should be viewed to take appropriate actions. You can access the list of tickets from the main menu.

xFlow

Paessler designates all kinds of flow protocols as xFlow. Currently, PRTG supports NetFlow V5 and V9, IPFIX, sFlow V5, and jFlow V5.

14.2 List of Abbreviations

Please see below for a list of abbreviations used in this documentation.

ADO: ActiveX Data Objects (ADO)

ADSL: Asymmetric Digital Subscriber Line (ADSL)

AJAX: Asynchronous Java Script and XML (AJAX)

API: Application Programming Interface (API)

CBQoS: Class Based Quality of Service (CBQoS)

cDOT: clustered Data ONTAP (cDOT)

CGI: Common Gateway Interface (CGI)

CIFS; Common Internet File System (CIFS)

CLI: command-line interface (CLI)

CoS: Class of Service (CoS)

CSV: Comma Seperated Values (CSV)

DAG: Database Availability Group (DAG)

DHCP: Dynamic Host Configuration Protocol (DHCP)

DMZ: Demilitarized Zone (DMZ)

DSCP: Differentiated Services Code Point (DSCP)

DNS: Domain Name Service (DNS)

DSCP: Differentiated Services Code Point (DSCP)

FAT: File Allocation Table (FAT)

FTP: File Transfer Protocol (FTP)

FTPS: FTP over SSL (FTPS)

FQDN: Fully Qualified Domain Name (FQDN)

GID: global ID (GID)

GUI: Graphical User Interface (GUI)

GUID: Globally Unique Identifier (GUID)

HTTP: Hypertext Transfer Protocol (HTTP)

HTTPS: Hypertext Transfer Protocol Secure (HTTPS)

ICMP: Internet Control Message Protocol (ICMP)

ICPIF: Impairment Calculated Planning Impairment Factor (ICPIF)

iDRAC: Integrated Dell Remote Access Controller (iDRAC)

IIS: Microsoft Internet Information Services (IIS)

iLO: HP Integrated Lights-Out (iLO)

IMAP: Internet Message Access Protocol (IMAP)

IPFIX: IPFIX (Internet Protocol Flow Information Export)

IPMI: Intelligent Platform Management Interface (IPMI)

IPsec: Internet Protocol Security (IPsec)

iSCSI: internet Small Computer System Interface (iSCSI)

JSON: JavaScript Object Notation (JSON)

LAN: Local Area Network (LAN)

LDAP: Lightweight Directory Access Protocol (LDAP)

MIB: Management Information Base (MIB)

MoID: Managed Object ID (MoID)

MOS: Mean Opinion Score (MOS)

MSP: Managed Service Provider (MSP)

NAS: Network Attached Storage (NAS)

NAT: Network Address Translation (NAT)

NFS: Network File System (NFS)

NSA: Network Security Appliance (NSA)

NTFS: New Technology File System (NFTS)

NTLM: NT LAN Manager (NTLM)

OID: Object Identifier (OID)

OMSA: OpenManage Server Administrator (OMSA)

PDF: Portable Document Format (PDF)

PDV: Packet Delay Variation (PDV)

POP3: Post Office Protocol version 3 (POP3)

QoS: Quality of Service (QoS)

RADIUS: Remote Authentication Dial-In User Service (RADIUS)

REST: Representational State Transfer (REST)

RMON: Remote Monitoring (RMON)

RPC: Remote Procedure Call (RPC)

RTT: Round Trip Time (RTT)

SaaS: Software as a Service (SaaS)

SAN: Storage Area Network (SAN)

SASL: Simple Authentication and Security Layer (SASL)

SCVMM: System Center Virtual Machine Manager (SCVMM)

SIP: Session Initiation Protocol (SIP)

SLA: Service Level Agreement (SLA)

S.M.A.R.T.: Self-Monitoring, Analysis and Reporting Technology (S.M.A.R.T.)

SMB: Server Message Block (SMB)

SMTP: Simple Mail Transfer Protocol (SMTP)

SNI: Server Name Identification (SNI)

SNMP: Simple Network Management Protocol (SNMP)

SNTP: Simple Network Time Protocol (SNTP)

SOAP: Simple Object Access Protocol (SOAP)

SPAN: Switched Port Analyzer (SPAN)

SQL: Structured Query Language (SQL)

SRP: Secure Remote Password (SRP)

SSH: Secure Shell (SSH)

SSL: Secure Sockets Layer (SSL)

SSO: Single Sign-On (SSO)

TCP: Transport Control Protocol (TCP)

TFTP: Trivial File Transfer Protocol (TFTP)

TLS: Transport Layer Security (TLS)

UAC: User Account Control (UAC)

UCS: Unified Computing System (UCS)

UDP: User Datagram Protocol (UDP)

UNC: Uniform Naming Convention (UNC)

UPnP: Universal Plug and Play (UPnP)

UTC: UTC (Coordinated Universal Time)

UUID: Universally Unique Identifier (UUID)

VoIP: Voice over IP (VoIP)

VPN: Virtual Private Network (VPN)

WAN: Wide Area Network (WAN)

WBEM: Web-Based Enterprise Management (WBEM)

WMI: Windows Management Instrumentation (WMI)

WQL: Windows Management Instrumentation Query Language (WQL)

WSUS: Windows Server Update Services (WSUS)

XML: Extensible Markup Language (XML)

14.3 List of Icons

Please see below for a list of icons used in this documentation.

There is more detailed information on how this feature works exactly.

This feature is in beta status and may not function properly in all situations.

There is more information on this topic in another section in the PRTG manual.

There is more information on this topic in the Paessler Knowledge Base.

Notes that contain information about potential errors and that offer tips on how to keep them from occurring.

Notes that contain extremely critical information. Pay close attention to these notes, otherwise they could have serious consequences.

Notes that contain critical information. Pay close attention to these notes, otherwise PRTG might not function properly.

Notes that contain additional information.

Step-by-step instructions.

Examples on how to use a feature.

Calls to action. These contain tips, requirements, or instructions on what you need to enter in certain fields, or inform you that certain programs or apps need to be installed.

This information is relevant for PRTG on demand.

This information is relevant for PRTG on premises.

14.4 Support and Troubleshooting

Need help with PRTG? There are several ways to get support and troubleshoot.

Video Tutorials

A video says more than a thousand words—watch tutorials for PRTG from Paessler and other PRTG users.

- https://www.paessler.com/support/videos

Paessler Knowledge Base

In the Knowledge Base, you can search in hundreds of articles about PRTG. You can post your own questions and answers, too!

- https://kb.paessler.com

Open a Support Ticket

Users that have purchased a license can open support tickets, which will usually be answered by Paessler's staff in less than 24 hours on business days. Please use the support form 3022 that is available in PRTG to contact our support team. This is the best way to get detailed help quickly. If you cannot use this form, contact us via our webpage.

- https://shop.paessler.com/en/openticket

14.5 Differences between PRTG on Premises and PRTG on Demand

Please see below for the differences between the settings and features that PRTG on premises and PRTG on demand have to offer.

Licensing, Payment, Infrastructure

TOPIC	PRTG ON PREMISES	PRTG ON DEMAND BETA
Trial Period	30 days	10 days
Freeware	freeware (100 sensors) available	no freeware, smallest edition is PRTG-500
Payment	one-time license fee plus yearly maintenance	monthly fee
PRTG Edition Size Flexibility	upgrade only	upgrade or downgrade
Max. Installation Size	unrestricted	5,000 sensors
PRTG Update Management	done by user	done by Paessler
Enterprise Console	full support	not supported: connections are not possible

Features

FEATURE	PRTG ON PREMISES	PRTG ON DEMAND BETA
Cluster	☺	⊘
Customizations (CSS, HTML, lookups, maps, device icons)	☺	⊘

FEATURE	PRTG ON PREMISES	PRTG ON DEMAND BETA
Freeware (100 sensors)	☺	⊘
RDP Access to Core Server	☺	⊘
Historic Data Purging (manually defined)	☺	⊘
Active Directory Integration	☺	⊘
License settings via PRTG web interface	☺	⊘
Recommended Sensors on Local Probe	☺	⊘
Auto-Discovery on Local Probe	☺	⊘
Mini Probes	☺	⊘
Device Tools on Local Probe	☺	⊘
Proxy Server settings	☺	⊘
System Information on Local Probe	☺	⊘
PRTG Administration Tool on PRTG Core Server	☺	⊘
MIB import and and usage as oidlib with SNMP Library sensor	☺	⊘
MIB import for SNMP Trap Receiver sensor	☺	⊘
Notification types: ▪ SMS/Pager Message ▪ Add Entry to Event Log ▪ Syslog Message	☺	⊘

FEATURE	PRTG ON PREMISES	PRTG ON DEMAND BETA
▪ SNMP Trap Message ▪ Execute Program		
Re-login request on setup pages after 15 minutes	☺	⊘

Sensors on Local Probe of PRTG on Demand

If you use PRTG on demand, you can add the following sensors only to remote probes.

SENSOR ON LOCAL PROBE	PRTG ON DEMAND BETA
Active Directory Replication Errors Sensor	⊘
ADO SQL v2 Sensor	⊘
Dell PowerVault MDi Physical Disk Sensor	⊘
Dell PowerVault MDi Logical Disk Sensor	⊘
Enterprise Virtual Array Sensor	⊘
Event Log (Windows API) Sensor	⊘
Exchange Backup (Powershell) Sensor	⊘
Exchange Database DAG (Powershell) Sensor	⊘
Exchange Database (Powershell) Sensor	⊘
Exchange Mailbox (Powershell) Sensor	⊘

SENSOR ON LOCAL PROBE	PRTG ON DEMAND BETA
Exchange Mail Queue (Powershell) Sensor	⊘
Exchange Public Folder (Powershell) Sensor	⊘
EXE/Script Advanced Sensor	⊘
EXE/Script Sensor	⊘
File Content Sensor	⊘
File Sensor	⊘
Folder Sensor	⊘
HTTP Full Web Page Sensor	⊘
HTTP Push Count Sensor	⊘
HTTP Push Data Advanced Sensor	⊘
HTTP Push Data Sensor	⊘
Hyper-V Cluster Shared Volume Disk Free Sensor	⊘
Hyper-V Host Server Sensor	⊘
Hyper-V Virtual Machine Sensor	⊘
Hyper-V Network Adapter Sensor	⊘
Hyper-V Virtual Storage Sensor	⊘
IPFIX (Custom) Sensor	⊘
IPFIX Sensor	⊘
IPMI System Health Sensor	⊘

SENSOR ON LOCAL PROBE	PRTG ON DEMAND BETA
jFlow V5 (Custom) Sensor	⊘
jFlow V5 Sensor	⊘
Microsoft SQL v2 Sensor	⊘
MySQL v2 Sensor	⊘
NetFlow V5 (Custom) Sensor	⊘
NetFlow V5 Sensor	⊘
NetFlow V9 (Custom) Sensor	⊘
NetFlow V9 Sensor	⊘
Oracle SQL v2 Sensor	⊘
Oracle Tablespace Sensor	⊘
Packet Sniffer (Custom) Sensor	⊘
Packet Sniffer Sensor	⊘
PerfCounter Custom Sensor	⊘
PerfCounter IIS Application Pool Sensor	⊘
Port Range Sensor	⊘
Port Sensor	⊘
PostgreSQL Sensor	⊘
Python Script Advanced Sensor	⊘
QoS (Quality of Service) Round Trip Sensor	⊘

SENSOR ON LOCAL PROBE	PRTG ON DEMAND BETA
QoS (Quality of Service) One Way Sensor	⊘
sFlow (Custom) Sensor	⊘
sFlow Sensor	⊘
Share Disk Free Sensor	⊘
SMTP Sensor	⊘
SNMP Trap Receiver Sensor	⊘
Syslog Receiver Sensor	⊘
Windows MSMQ Queue Length Sensor	⊘
Windows Physical Disk I/O Sensor	⊘
Windows Print Queue Sensor	⊘
Windows Updates Status (Powershell) Sensor	⊘
Windows CPU Load Sensor	⊘
WMI Custom Sensor	⊘
WMI Custom String Sensor	⊘
WMI Event Log Sensor	⊘
WMI Exchange Server Sensor	⊘
WMI Exchange Transport Queue Sensor	⊘
WMI File Sensor	⊘

SENSOR ON LOCAL PROBE	PRTG ON DEMAND BETA
WMI Free Disk Space (Multi Disk) Sensor	⊘
WMI HDD Health Sensor	⊘
Windows IIS 6.0 SMTP Received Sensor	⊘
Windows IIS 6.0 SMTP Sent Sensor	⊘
Windows IIS Application Sensor	⊘
WMI Logical Disk I/O Sensor	⊘
WMI Memory Sensor	⊘
Windows Network Card Sensor	⊘
Windows Pagefile Sensor	⊘
Windows Process Sensor	⊘
WMI Remote Ping Sensor	⊘
WMI Security Center Sensor	⊘
WMI Service Sensor	⊘
WMI SharePoint Process Sensor	⊘
WMI Share Sensor	⊘
Windows System Uptime Sensor	⊘
WMI UTC Time Sensor	⊘
WMI Vital System Data Sensor	⊘
WMI Volume Sensor	⊘

SENSOR ON LOCAL PROBE	PRTG ON DEMAND BETA
WSUS Statistics Sensor	⊘
WMI Microsoft SQL Server 2005 Sensor (Deprecated)	⊘
WMI Microsoft SQL Server 2008 Sensor	⊘
WMI Microsoft SQL Server 2012 Sensor	⊘
WMI Microsoft SQL Server 2014 Sensor	⊘
WMI Microsoft SQL Server 2016 Sensor	⊘
WMI Terminal Services (Windows 2008+) Sensor	⊘
WMI Terminal Services (Windows XP/Vista/2003) Sensor	⊘

Settings

SETTING TITLE	SETTING NAME	PRTG ON PREMISES	PRTG ON DEMAND BETA
Auto-Update	When a New Version is Available	☺	⊘
	Installation Time	☺	⊘
	Release Channel	☺	⊘
Notifications	SMS/Page Message	☺	⊘
	Add Entry To Event Log	☺	⊘

SETTING TITLE	SETTING NAME	PRTG ON PREMISES	PRTG ON DEMAND BETA
	Syslog Message	☺	⊘
	SNMP Trap Message	☺	⊘
	Execute Program	☺	⊘
Core & Probes	Proxy Configuration	☺	⊘
	Probe Connection IPs	☺	⊘
	Mini Probes	☺	⊘
	Mini Probe Port	☺	⊘
Probe Administrative Tools	Restart Local Probe	☺	⊘
Scanning Intervals	Available Intervals (definition of individual intervals)	☺	⊘
Notification Delivery	SMTP Delivery	☺	⊘
	SMS Delivery	☺	⊘
Recommended Sensors Detection	Detection Engine	☺	⊘
User Interface (Website)	DNS Name	☺	⊘
	Google Analytics Tracking ID	☺	⊘
User Interface (Web Server)	IP Address for Web Server	☺	⊘
	TCP Port for Web Server	☺	⊘
	Web Server Port	☺	⊘

SETTING TITLE	SETTING NAME	PRTG ON PREMISES	PRTG ON DEMAND BETA
	Web Server Security	☺	⊘
	SSL Security	☺	⊘
	Currently Active IP Address/ Port Combination(s)	☺	⊘
User Accounts	Login Name	☺	⊘
	Password	☺	⊘
	Passhash	☺	⊘
Core Administrative Tools	Create Configuration Snapshot	☺	⊘
	Write Core Status File	☺	⊘
	Clear Caches	☺	⊘
	Load Lookups	☺	⊘
	Restart Core Server	☺	⊘
Advanced Network Analysis	System Information	☺	⊘
Scheduled Restart Settings (Local Probe)	Restart Options	☺	⊘
	Restart Schedule	☺	⊘
	Specify Day	☺	⊘
	Specify Hour	☺	⊘

14.6 Legal Notices

Build using Indy Internet Direct (http://www.indyproject.org/). This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). Uses the net-SNMP library, see "netsnmp-license.txt". Uses the DelphiZip library distributed under the GNU LESSER GENERAL PUBLIC LICENSE (http://www.delphizip.net/). Uses FastMM (http://sourceforge.net/projects/fastmm/), TPLockBox (http://sourceforge.net/projects/tplockbox) and Delphi Chromium Embedded (http://code.google.com/p/delphichromiumembedded/) under the Mozilla Public License 1.1 (MPL 1.1, available from http://www.mozilla.org/MPL/MPL-1.1.html). Soundfiles from http://www.soundsnap.com. Uses Public Domain regional maps from the "CIA World Factbook" webpage of the CIA (https://www.cia.gov/library/publications/the-world-factbook/docs/refmaps.html). Uses the "wkhtmltopdf" (http://code.google.com/p/wkhtmltopdf/) library distributed under the GNU LESSER GENERAL PUBLIC LICENSE (see wkhtmltopdf_lgpl-3.0.txt). Icons from http://www.androidicons.com. Uses the IPMIUTIL library under the BSD 2.0 license, see "ipmi_bsd-2.0.txt". Uses PhantomJS, see "phantomjs-license.bsd".. Uses the Npgsql - .Net Data Provider for Postgresql library (for license information see ipmi_bsd-2.0.txt).

All product names, company names, and logos referenced to or depicted herein are the trademarks™, registered® trademarks, or service marks of the respective owners. Use of them, their occurrence, or references to their occurrence in graphical representations of the web interface herein is solely for informational purposes and does not imply any affiliation with or endorsement by the respective owners.

Last manual export: Friday, June 23, 2017 6:14:33 PM

Last change to this manual (YYYY-MM-DD): 6/23/2017