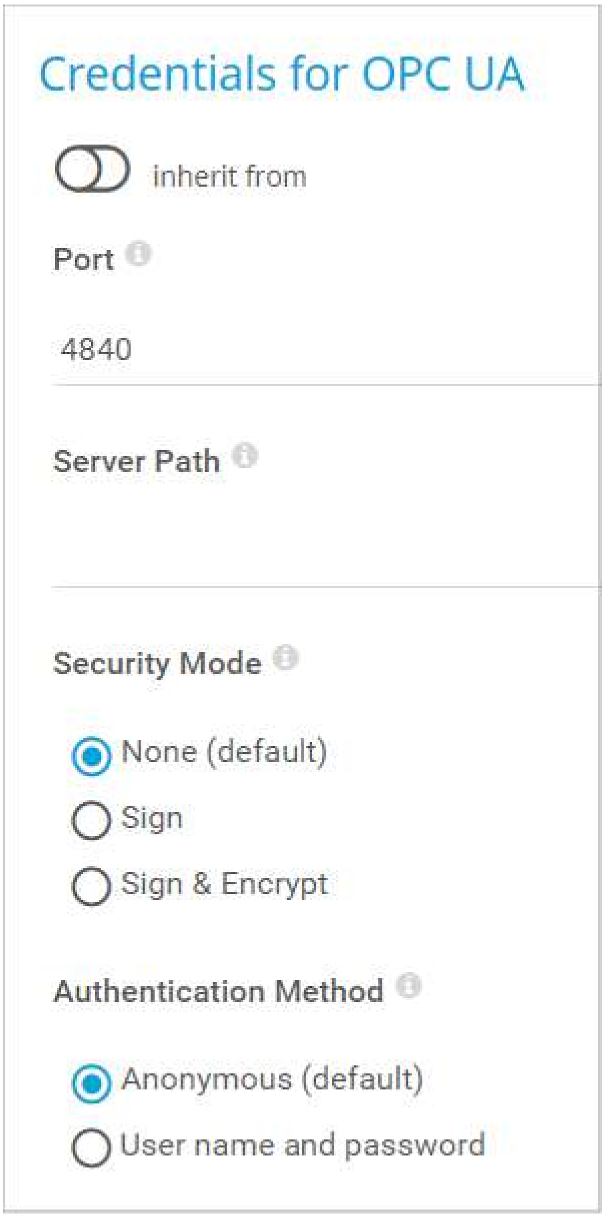
Setting	Description
User Name	Enter a user name for access to the ONTAP System Manager.
Password	Enter the password for access to the ONTAP System Manager.
Port	Enter the port for the connection to the ONTAP System Manager. The default port for secure connections is 443.
Protocol	Select the protocol that you want to use for the connection to the ONTAP System Manager. Choose between: ▪ HTTPS (default) ▪ HTTP

Credentials for OPC UA

Click ✓ to interrupt the inheritance 135.

ⓘ The settings you define in this section apply to the following sensors:

- Beckhoff IPC System Health
- OPC UA Certificate
- OPC UA Custom
- OPC UA Server Status



Credentials for OPC UA

inherit from

Port

4840

Server Path

Security Mode

● None (default)
○ Sign
○ Sign & Encrypt

Authentication Method

● Anonymous (default)
○ User name and password

Credentials for OPC UA

Setting	Description
Port	Enter the port for the connection to the OPC Unified Architecture (OPC UA) server. The default port for secure connections is 4840.
Server Path	Enter the path of the OPC UA server endpoint if you run more than one server under the same IP address or DNS name.
Security Mode	Select if you want to use encryption: ▪ None (default): Do not use encryption. ▪ Sign: Sign messages between the sensor and the OPC UA server.

Setting	Description
	▪ Sign & Encrypt: Sign and encrypt messages between the sensor and the OPC UA server.
Security Policy	This setting is only visible if you select Sign or Sign & Encrypt above. Select if you want to use a security policy and define which policy you want to use: ▪ None (default): Do not use a security policy. ▪ Basic256Sha256: Use the Basic256Sha256 security policy. ▪ Basic256: Use the Basic256 security policy.
Client Certificate	This setting is only visible if you select Sign or Sign & Encrypt above. Enter the certificate that you created for authenticating the sensor against the OPC UA server. ⓘ The certificate must meet the following requirements: ▪ The key size must be 2048-bit. ▪ The secure hash algorithm must be SHA256. ▪ DataEncipherment must be part of the KeyUsage certificate extension. ▪ A uniform resource indicator (URI) must be set in subjectAltName. ▪ The certificate must be in Privacy-Enhanced Mail (PEM) format.
Client Key	This setting is only visible if you select Sign or Sign & Encrypt above. Enter the client key for access to the OPC UA server. ⓘ The client key must be in PEM format and it must be encrypted using the Client Key Password.
Client Key Password	This setting is only visible if you select Sign or Sign & Encrypt above. Enter the password for the client key.
Authentication Method	Select if you want to connect without credentials or define credentials for access to the OPC UA server: ▪ Anonymous (default): Connect without credentials. ▪ User name and password: Define credentials for the connection. ⓘ Most OPC UA servers do not support User name and password authentication without a client certificate. To use User name and password authentication, select Sign or Sign & Encrypt under Security Mode and Basic256Sha256 or Basic256 under Security Policy and enter the Client Certificate, Client Key, and Client Key Password that you want to use.

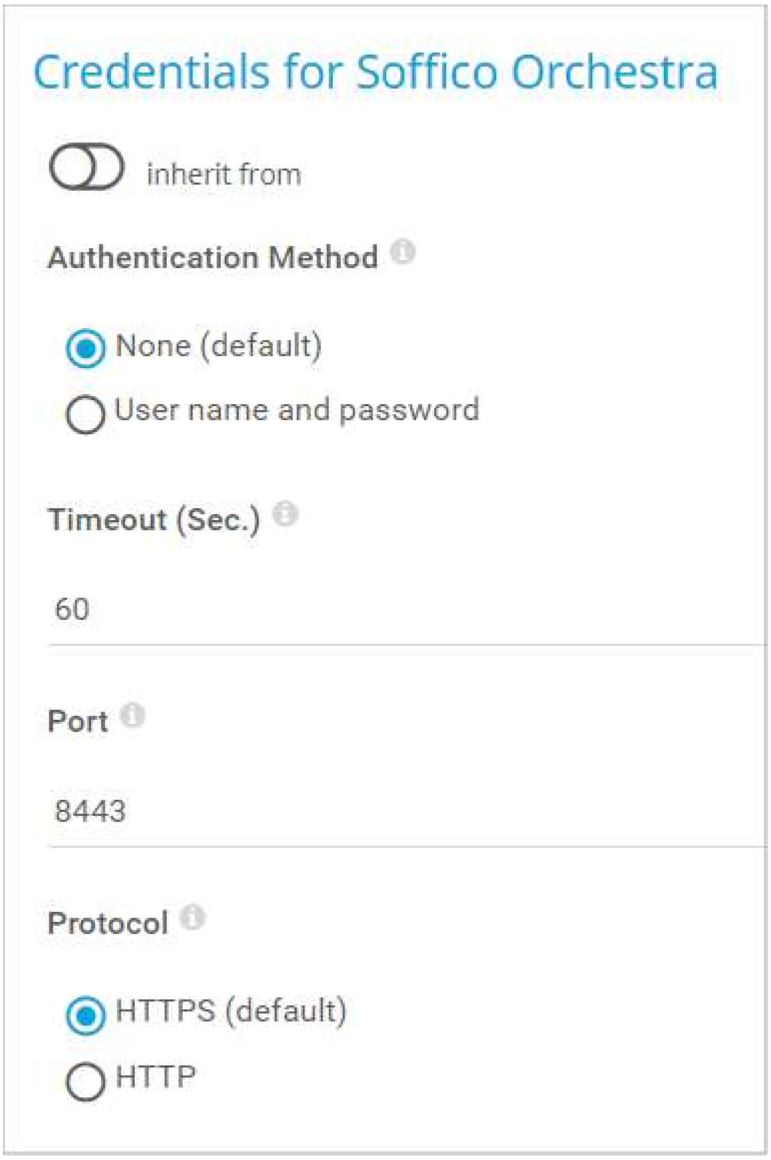
Setting	Description
	ⓘ If you select None (default) under Security Mode and use User name and password authentication, PRTG sends the unencrypted password to the OPC UA server.
User Name	This setting is only visible if you select User name and password above. Enter the user name for access to the OPC UA server.
Password	This setting is only visible if you select User name and password above. Enter the password for access to the OPC UA server.

Credentials for Soffico Orchestra

Click ✓ to interrupt the inheritance 135.

ⓘ The settings you define in this section apply to the following sensor:

- Soffico Orchestra Channel Health



Credentials for Soffico Orchestra

inherit from

Authentication Method

● None (default)

○ User name and password

Timeout (Sec.)

60

Port

8443

Protocol

● HTTPS (default)

○ HTTP

Credentials for Soffico Orchestra

Setting	Description
Authentication Method	Select if you want to connect without credentials or define credentials for access to the Orchestra platform: ▪ None (default): Connect without credentials. ▪ User name and password: Define credentials for the connection.
User Name	This setting is only visible if you select User name and password above. Enter the user name for access to the Orchestra platform.
Password	This setting is only visible if you select User name and password above. Enter the password for access to the Orchestra platform.

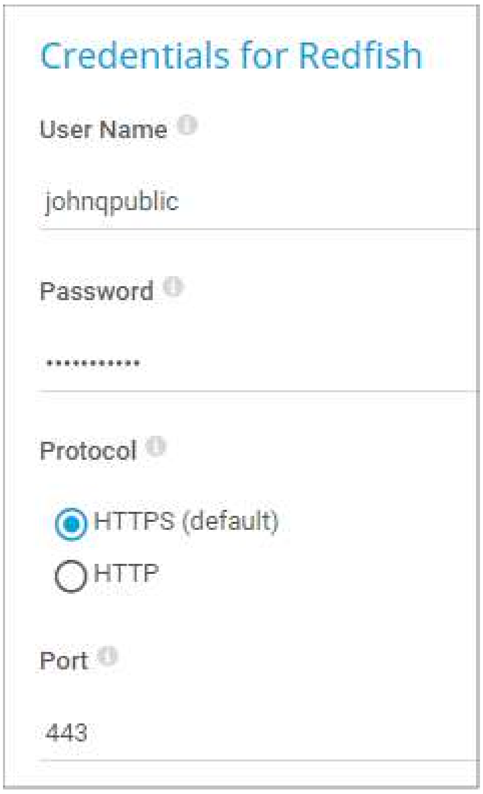
Setting	Description
Timeout (Sec.)	Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is 300 seconds (5 minutes).
Port	Enter the port for the connection to the Orchestra platform. The default port for secure connections is 8443 and the default port for unsecure connections is 8019.
Protocol	Select the protocol that you want to use for the connection to the Orchestra platform: ▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection. ▪ HTTP: Use an unsecure connection.

Credentials for Redfish

Click ✓ to interrupt the inheritance[135].

ⓘ The settings you define in this section apply to the following sensors:

- Redfish Power Supply
- Redfish System Health
- Redfish Virtual Disk



Credentials for Redfish

User Name ⓘ

johnqpublic

Password ⓘ

•••••••••••

Protocol ⓘ

● HTTPS (default)

○ HTTP

Port ⓘ

443

Credentials for Redfish

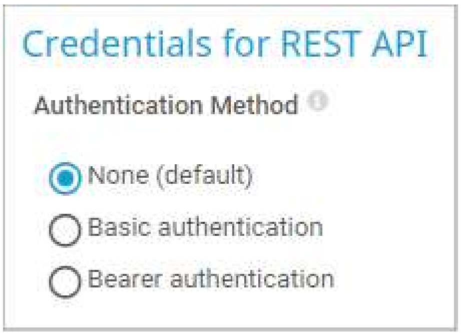
Setting	Description
User Name	Enter the user name for access to the Redfish system.
Password	Enter the password for access to the Redfish system.
Protocol	Select the protocol that you want to use for the connection to the Redfish system. Choose between: ▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection. ▪ HTTP: Use an unsecure connection.
Port	Enter the port for the connection to the Redfish system. The default port for secure connections is 443.

Credentials for REST API

Click ✓ to interrupt the inheritance 135.

ⓘ The settings you define in this section apply to the following sensor:

- REST Custom v2



Credentials for REST API

Authentication Method

● None (default)
○ Basic authentication
○ Bearer authentication

Credentials for REST API

Setting	Description
Authentication Method	Select the authentication method for access to the Representational State Transfer (REST) application programming interface (API): ▪ None (default): Use no authentication. ▪ Basic authentication: Use basic authentication. ▪ Bearer authentication: Use an OAuth2 bearer token.
User Name	This setting is only visible if you select Basic authentication above. Enter the user name for access to the REST API.
Password	This setting is only visible if you select Basic authentication above. Enter the password for access to the REST API.
Bearer Token	This setting is only visible if you select Bearer authentication above. Enter a bearer token for access to the REST API.
Placeholder 1 Description	Enter a description for Placeholder 1, for example information about the purpose or content of the placeholder.
Placeholder 1	Enter a value for the placeholder. PRTG inserts the value for the REST API request if you add %restplaceholder1 in the Request URL, POST Body, and Custom Headers fields of the REST Custom v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 2 Description	Enter a description for Placeholder 2, for example information about the purpose or content of the placeholder.
Placeholder 2	Enter a value for the placeholder. PRTG inserts the value for the REST API request if you add %restplaceholder2 in the Request URL, POST Body, and Custom Headers fields of the REST Custom v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.

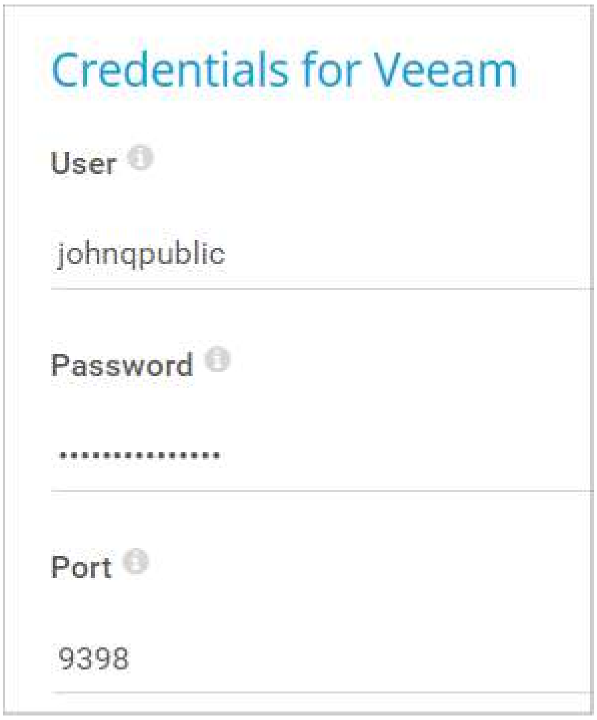
Setting	Description
Placeholder 3 Description	Enter a description for Placeholder 3, for example information about the purpose or content of the placeholder.
Placeholder 3	Enter a value for the placeholder. PRTG inserts the value for the REST API request if you add %restplaceholder3 in the Request URL, POST Body, and Custom Headers fields of the REST Custom v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 4 Description	Enter a description for Placeholder 4, for example information about the purpose or content of the placeholder.
Placeholder 4	Enter a value for the placeholder. PRTG inserts the value for the REST API request if you add %restplaceholder4 in the Request URL, POST Body, and Custom Headers fields of the REST Custom v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 5 Description	Enter a description for Placeholder 5, for example information about the purpose or content of the placeholder.
Placeholder 5	Enter a value for the placeholder. PRTG inserts the value for the REST API request if you add %restplaceholder5 in the Request URL, POST Body, and Custom Headers fields of the REST Custom v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.

Credentials for Veeam

Click ✓ to interrupt the inheritance 135.

ⓘ The settings you define in this section apply to the following sensors:

- Veeam Backup Job Status
- Veeam Backup Job Status Advanced



Credentials for Veeam

User ⓘ

johnqpublic

Password ⓘ

•••••••••••••••

Port ⓘ

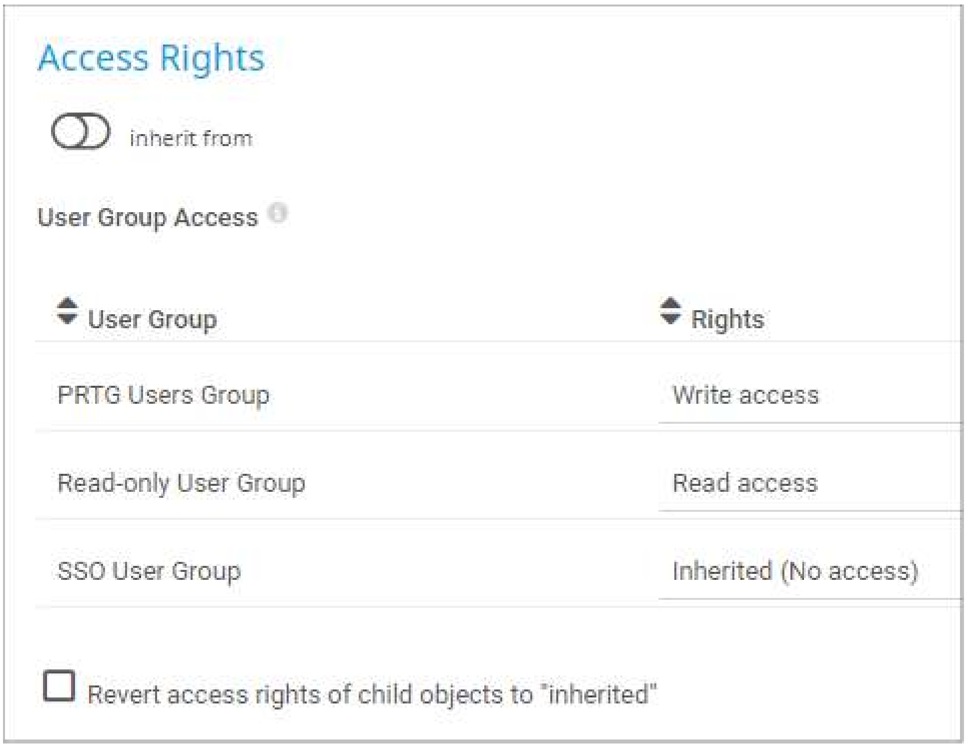
9398

Credentials for Veeam

Setting	Description
User Name	Enter the user name for access to the Veeam Backup Enterprise Manager.
Password	Enter the password for access to the Veeam Backup Enterprise Manager.
Port	Enter the port for the connection to the Veeam Backup Enterprise Manager. The default port for secure connections is 9398.

Access Rights

Click ✓ to interrupt the inheritance 135.



Access Rights

○ inherit from

User Group Access

User Group	Rights
PRTG Users Group	Write access
Read-only User Group	Read access
SSO User Group	Inherited (No access)

□ Revert access rights of child objects to "inherited"

Access Rights

Setting	Description
User Group Access	Select the user groups 3346 that have access to the object. You see a table with user groups and group access rights. The table contains all user groups in your setup. For each user group, you can choose from the following group access rights: ▪ Inherited: Inherit the access rights settings of the parent object. ▪ No access: Users in this user group cannot see or edit the object. The object neither shows up in lists nor in the device tree. ⓘ There is one exception: If a user in this user group has access to a child object, the parent object is visible in the device tree but users in this user group cannot access it. ▪ Read access: Users in this group can see the object and view its monitoring results. They cannot edit any settings. ▪ Write access: Users in this group can see the object, view its monitoring results, and edit its settings. They cannot edit its access rights settings. ▪ Full access: Users in this group can see the object, view its monitoring results, edit its settings, and edit its access rights settings. To automatically set all child objects to inherit this object's access rights, enable the Revert access rights of child objects to "inherited" option. For more details on access rights, see section Access Rights Management 144.

ⓘ Click OK to save your settings. If you close the dialog without saving, all changes to the settings are lost.

More

■ KNOWLEDGE BASE

What security features does PRTG include?

- https://kb.paessler.com/en/topic/61108

How do I set permissions for the Amazon Web Services (AWS) API key to use certain sensors in PRTG?

- https://kb.paessler.com/en/topic/38083

Where can I find the Web Services API (WSAPI) port for the connection to the HPE 3PAR system?

- https://kb.paessler.com/en/topic/89717

How do I obtain credentials and set permissions for the Microsoft 365 Service Status sensors?

- https://kb.paessler.com/en/topic/88462

How do I obtain credentials and create custom roles for the Microsoft Azure sensors?

- https://kb.paessler.com/en/topic/88625

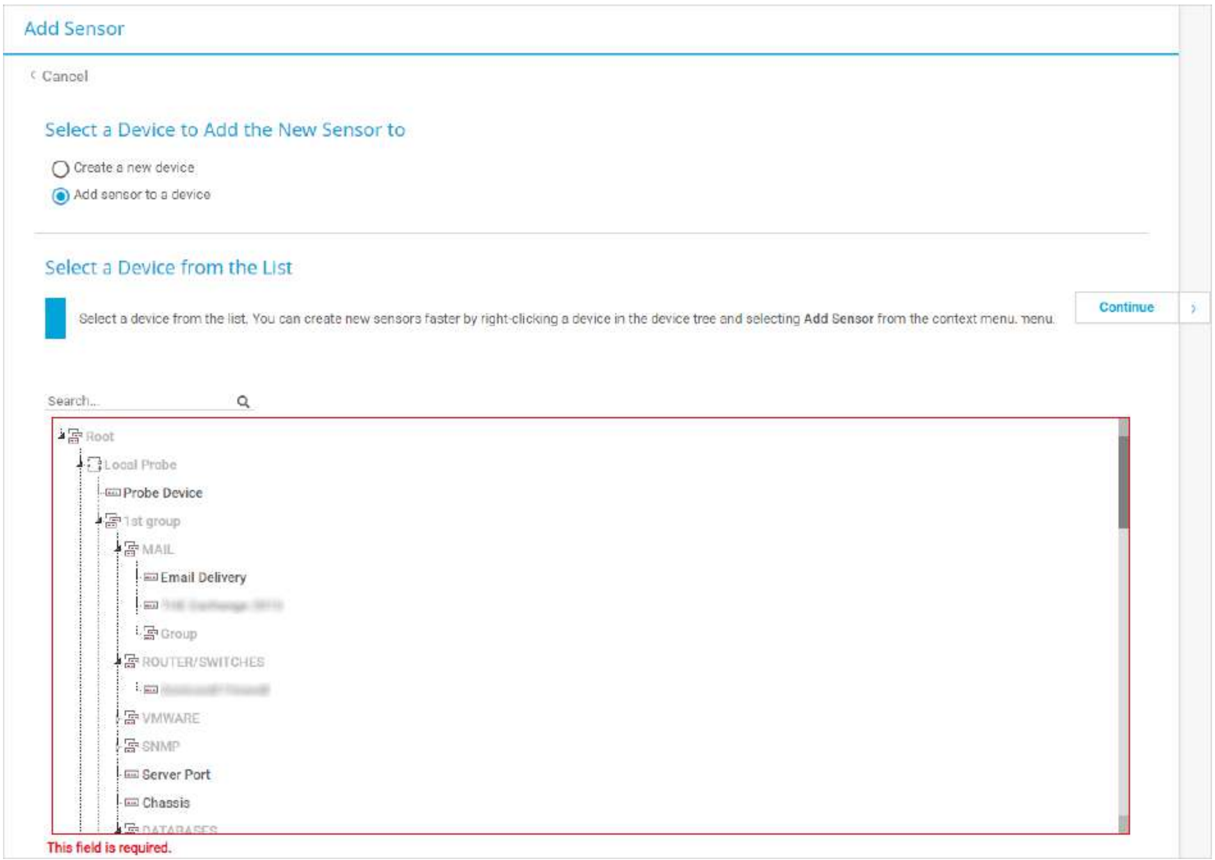
7.2.4 Add a Sensor

There are several ways to manually add a sensor:

- Select Sensors | Add Sensor from the main menu bar 251. A dialog appears that guides you through the process of adding a new sensor.
- Hover over ⊕ and select Add Sensor from the menu.
- Select Add Sensor from the context menu 234 of a device to which you want to add the new sensor. This skips step 1 and leads you directly to step 2 415.
- Click the Add Sensor button at the end of a device's sensor list on the device tree screen or above the geographical map on the right.

ⓘ This documentation refers to an administrator that accesses the PRTG web interface on a master node. Other user accounts, interfaces, or failover nodes might not have all of the options in the way described here. In a cluster, note that failover nodes are read-only by default.

Preparation: Select a Device



Add Sensor

‹ Cancel

Select a Device to Add the New Sensor to

○ Create a new device
● Add sensor to a device

Select a Device from the List

Select a device from the list. You can create new sensors faster by right-clicking a device in the device tree and selecting **Add Sensor** from the context menu. menu.

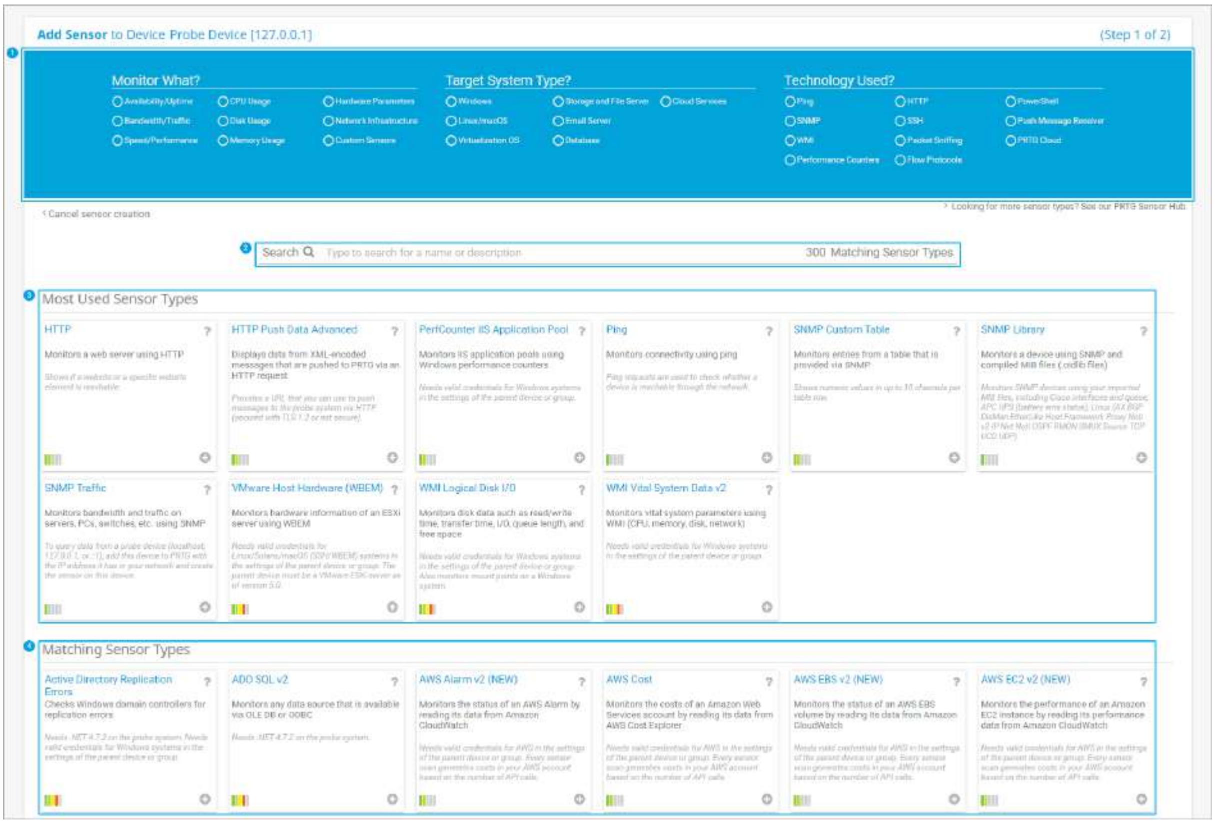
This field is required.

Add Sensor Assistant

- Select Add sensor to a device.
- Select the device you want to add the new sensor to.
- Click Continue.

The Add Sensor dialog appears.

Step 1: Choose Sensor



Add Sensor to Device Probe Device [127.0.0.1] (Step 1 of 2)

Monitor What?
○ Availability/Uptime ○ CPU Usage ○ Hardware Parameters
○ Bandwidth/Traffic ○ Disk Usage ○ Network Infrastructure
○ Speed/Performance ○ Memory Usage ○ Custom Sensors

Target System Type?
○ Windows ○ Storage and File Server ○ Cloud Services
○ Linux/macOS ○ Email Server
○ Virtualization OS ○ Database

Technology Used?
○ Ping ○ HTTP ○ PowerShell
○ SNMP ○ SSH ○ Push Message Receiver
○ WMI ○ Packet Sniffing ○ PRTG Cloud
○ Performance Counters ○ Flow Protocols

‹ Cancel sensor creation

› Looking for more sensor types? See our PRTG Sensor Hub

Search Type to search for a name or description 300 Matching Sensor Types

Most Used Sensor Types

HTTP
Monitors a web server using HTTP
Shows if a website or a specific website element is reachable.

HTTP Push Data Advanced
Displays data from XML-encoded messages that are pushed to PRTG via an HTTP request
Provides a URL that you can use to push messages to the probe system via HTTP (secured with TLS 1.2 or not secure).

PerfCounter IIS Application Pool
Monitors IIS application pools using Windows performance counters
Needs valid credentials for Windows systems in the settings of the parent device or group.

Ping
Monitors connectivity using ping
Ping requests are used to check whether a device is reachable through the network.

SNMP Custom Table
Monitors entries from a table that is provided via SNMP
Shows numeric values in up to 10 channels per table row.

SNMP Library
Monitors a device using SNMP and compiled MIB files (.oidlib files)
Monitors SNMP devices using your imported MIB files, including Cisco interfaces and queue, APC UPS (battery and status), Linux (AX BGP DisMan EtherLike Host Framework Proxy Notif v2 IP Net Mgt OSPF RMON SMUX Source TCP UCD UDP)

SNMP Traffic
Monitors bandwidth and traffic on servers, PCs, switches, etc. using SNMP
To query data from a probe device (localhost, 127.0.0.1, or ::1), add this device to PRTG with the IP address it has in your network and create the sensor on this device.

VMware Host Hardware (WBEM)
Monitors hardware information of an ESXi server using WBEM
Needs valid credentials for Linux/Solaris/macOS (SSH/WBEM) systems in the settings of the parent device or group. The parent device must be a VMware ESXi server as of version 5.0.

WMI Logical Disk I/O
Monitors disk data such as read/write time, transfer time, I/O, queue length, and free space
Needs valid credentials for Windows systems in the settings of the parent device or group. Also monitors mount points on a Windows system.

WMI Vital System Data v2
Monitors vital system parameters using WMI (CPU, memory, disk, network)
Needs valid credentials for Windows systems in the settings of the parent device or group.

Matching Sensor Types

Active Directory Replication Errors
Checks Windows domain controllers for replication errors
Needs .NET 4.7.2 on the probe system. Needs valid credentials for Windows systems in the settings of the parent device or group.

ADO SQL v2
Monitors any data source that is available via OLE DB or ODBC
Needs .NET 4.7.2 on the probe system.

AWS Alarm v2 (NEW)
Monitors the status of an AWS Alarm by reading its data from Amazon CloudWatch
Needs valid credentials for AWS in the settings of the parent device or group. Every sensor scan generates costs in your AWS account based on the number of API calls.

AWS Cost
Monitors the costs of an Amazon Web Services account by reading its data from AWS Cost Explorer
Needs valid credentials for AWS in the settings of the parent device or group. Every sensor scan generates costs in your AWS account based on the number of API calls.

AWS EBS v2 (NEW)
Monitors the status of an AWS EBS volume by reading its data from Amazon CloudWatch
Needs valid credentials for AWS in the settings of the parent device or group. Every sensor scan generates costs in your AWS account based on the number of API calls.

AWS EC2 v2 (NEW)
Monitors the performance of an Amazon EC2 instance by reading its performance data from Amazon CloudWatch
Needs valid credentials for AWS in the settings of the parent device or group. Every sensor scan generates costs in your AWS account based on the number of API calls.

Add Sensor Dialog

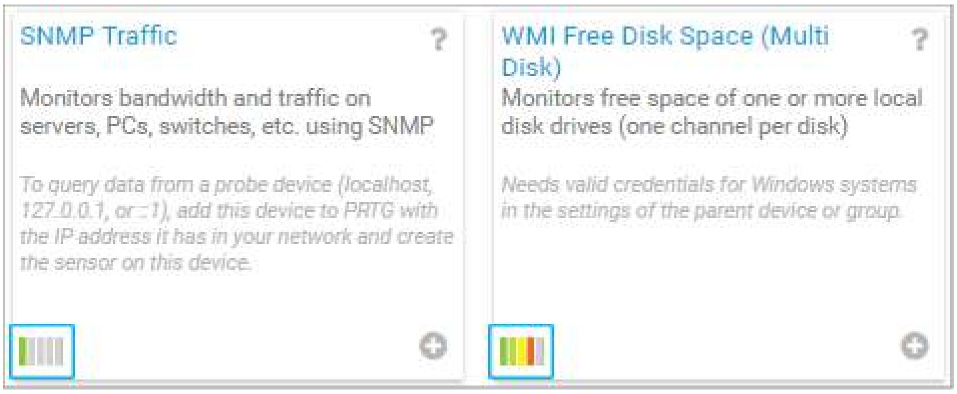
In the Add Sensor dialog, you can:

- 1 Choose appropriate criteria to filter the sensors.
  - Select the type of parameter that you want to monitor via Monitor What?
  - Specify the type of target system that you want to monitor and see what sensors are available for this type of hardware via Target System Type?
  - Select the technology that you want to use for monitoring (for example SNMP or WMI) via Technology Used?
- 2 Enter (parts of) the name into the search box.
- 3 Go through the list of the most used sensor types.
  ⓘ PRTG suggests sensors for the selected device. This recommendation is automatically calculated based on the current user's sensor usage. It shows the ten most commonly used sensors if there are already enough sensors for the recommendation to use.
- 4 Go through the list of all matching sensor types.
  If you cannot find a suitable sensor, search for custom sensors in our PRTG Sensor Hub. To do so, click Looking for more sensor types? above the search box or below the list of sensors.
  For more information, see section List of Available Sensor Types 3729, section PRTG Sensor Hub.
- Click the sensor box to select the sensor.

ⓘ If you are unsure which sensor provides the information that you need, we recommend that you use the filter categories to reduce the amount of matching sensor types.

ⓘ Also consider whether a sensor's performance impact 3385 is high or low. To do so, check the bar in the lower-left corner of the sensor box. For further information, see the Knowledge Base: How can I speed up PRTG—especially for large installations? (especially section 4 - Sensor Type and Monitoring).

For an overview list of all sensors, including their performance impact, see section List of Available Sensor Types 3683.



SNMP Traffic ?

Monitors bandwidth and traffic on servers, PCs, switches, etc. using SNMP

To query data from a probe device (localhost, 127.0.0.1, or ::1), add this device to PRTG with the IP address it has in your network and create the sensor on this device.

WMI Free Disk Space (Multi Disk) ?

Monitors free space of one or more local disk drives (one channel per disk)

Needs valid credentials for Windows systems in the settings of the parent device or group.

Sensor with Very Low Performance Impact and with High Performance Impact

For more information about a sensor, click ? to see the section of the respective sensor.

Step 2: Define Sensor Settings

The Add Sensor 413 dialog appears when you manually add a new sensor to a device. It only shows the settings that are required to create the sensor. You can change nearly all settings on the sensor's Settings tab after creation.

ⓘ Enable check boxes in front of the respective lines to select the items. Use the check box in the table header to select all items or to cancel the selection. In large tables, use the search function in the upper-right corner.

Then, the sensor settings dialog opens where you can define the sensor settings and create the sensor.

ⓘ The settings that you select during sensor creation are valid for all sensors that you create when you finish the dialog.

More

KNOWLEDGE BASE

How can I change the number of entries in most used sensor types?

- https://kb.paessler.com/en/topic/59788

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

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

PAESSLER WEBSITE

You can find useful scripts for sensors in the PRTG Sensor Hub

- https://www.paessler.com/sensor-hub

7.3 Manage Device Tree

In the device tree, click the Management tab to enter a different view of your devices and sensors. While in this view, you can move monitoring objects via drag-and-drop. You can also select objects to view and edit their settings. Any changes that you make in this view immediately take effect. To arrange objects in the tree, you have the following options.

Move or Clone a Sensor

You can change the position of a sensor on the same device or you can clone a sensor to a different device.

- On the same device, drag any sensor and drop it where you want it. The sensor moves to this position and the other sensors line up underneath it.
- Drag any sensor from a device and drop it on a different device to clone a sensor. This creates the same sensor with the same settings on the new device. The original sensor does not change.
  ⓘ Cloned sensors initially show the Paused status 224 to give you the chance to change any settings before monitoring starts. Check the settings and resume 224 monitoring.

ⓘ You cannot clone fixed objects such as the root group, a probe device, or PRTG system-internal sensors.

ⓘ To clone entire groups or devices, use the clone object 3154 feature in the object's context menu 226.

Move a Group or Device

You can change the position of a group or a device via drag-and-drop.

- On the same probe or group, drag any group or device and move it up or down the device tree. A small red arrow appears that shows the future position. When you drop the group or device, it moves to this position and the other probes, groups, and devices line up underneath it.
- Drag any group or device from one probe or group and drop it on a different probe or group. A small red arrow appears that shows the future position. When you drop the group or device, it moves to the new probe or group and the other groups and devices line up underneath it. This way, you can change the probe that a group or device is part of or you can add groups or devices to other groups.

ⓘ You cannot move the local probe, the hosted probe, or remote probes.

Multi-Edit Object Settings

You can use multi-edit for object settings:

- Hold down the Ctrl key and select multiple objects of the same type, for example, multiple groups, devices, or sensors.
- In the dialog that appears, select the properties that you want to edit, change the respective settings, and click Save. The changes are applied to all selected objects.

The dialog is the same as described in section Multi-Edit 3159.

Related Topics

For other ways to arrange objects, see

- Arrange Objects 3152
- Create Device Template 3163
- Clone Object 3154

7.4 Root Group Settings

The root group is the highest instance in the object hierarchy and it is the parent to most other objects. Therefore, most objects inherit settings from the root group. So, before you create your own sensors, it is a good idea to review the root group's settings to make sure that they suit your needs.

ⓘ If necessary, you can override every setting for every single child object. To do so, disable the respective inherit from option of an object.

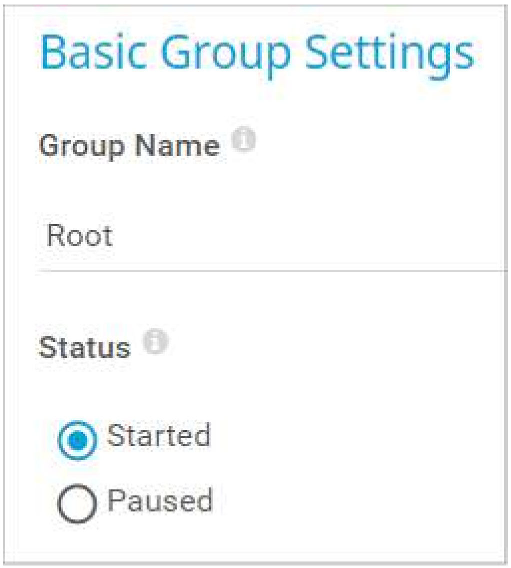
Root Group Settings

The following settings are available on the Settings tab. All of the settings that you define here can be inherited to all other objects in your setup.

ⓘ This documentation refers to an administrator that accesses the PRTG web interface on a master node. Other user accounts, interfaces, or failover nodes might not have all of the options in the way described here. In a cluster, note that failover nodes are read-only by default.

In this section:

Basic Group Settings


Basic Group Settings

Group Name ⓘ

Root

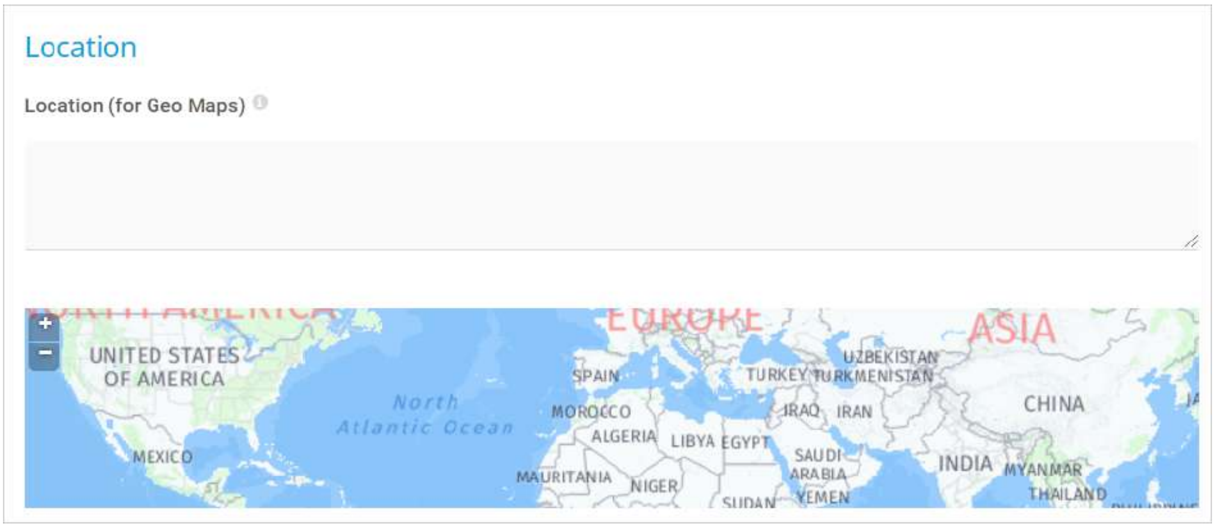
Status ⓘ

● Started
○ Paused

Basic Group Settings

Setting	Description
Group Name	Enter a name to identify the group. By default, PRTG displays it in the device tree 164. ⓘ If the name contains angle brackets (<>), PRTG replaces them with braces ({}) for security reasons. For more information, see the Knowledge Base: What security features does PRTG include?
Status	Select the monitoring status of the group: ▪ Started: Monitor the group. ▪ Paused: Pause monitoring for the group. All sensors on all devices in the group are in the Paused status 224 until you change this setting.

Location



Location

Location (for Geo Maps)

Location

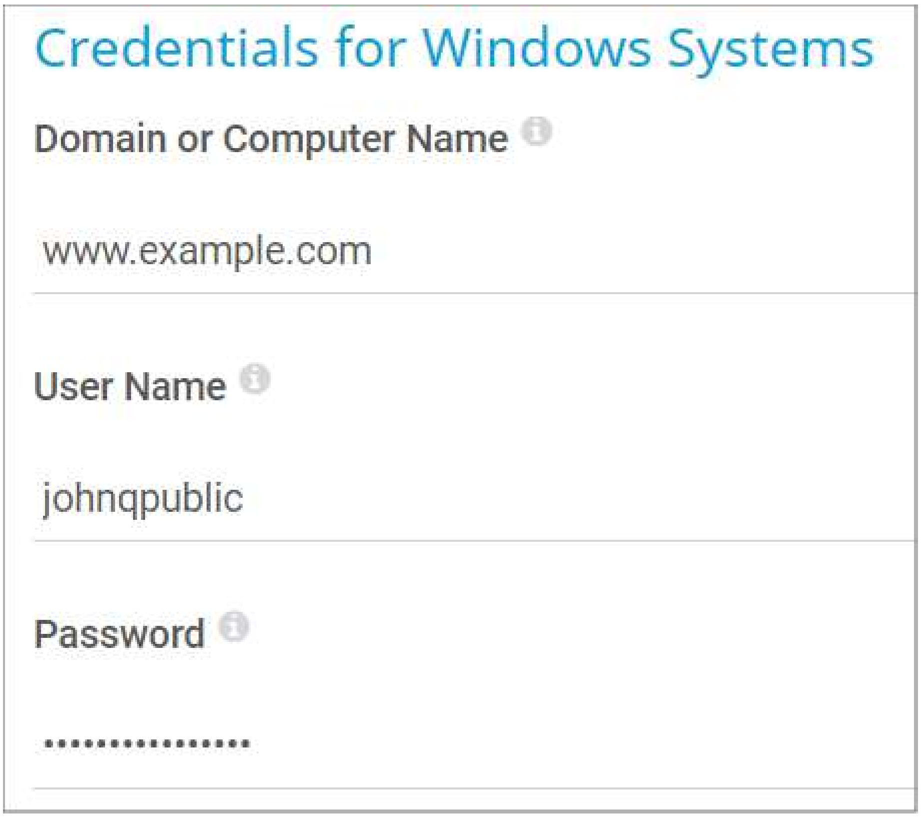
Setting	Description
Location (for Geo Maps)	If you want to use Geo Maps 3169, enter a location in the first line. Geographical maps then display objects like devices or groups with a status icon using a color code similar to the sensor status icons 179 (green–yellow–orange–red). You can enter a full postal address, city and country only, or latitude and longitude. It is possible to enter any text before, between, and after the coordinates, as PRTG automatically parses latitude and longitude, for example, enter 49.452778 11.077778, or enter 49.452778 any 11.077778 text. A minus sign (-) in the first line hides an object from a geographical map. 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 the coordinates in the second line. This geographical marker then shows the object with the label in the geographical map. ⓘ The preview map always has a road map layout regardless of the map layout you set in User Interface 3297.

Credentials for Windows Systems

ⓘ The settings you define in this section apply to the following sensors:

- Active Directory Replication Errors
- Event Log (Windows API)
- Windows IIS 6.0 SMTP Sent
- Windows IIS Application
- Windows MSMQ Queue Length
- WMI Memory
- WMI Microsoft SQL Server 2005 (Deprecated)

- Exchange Backup (PowerShell)
- Exchange Database (PowerShell)
- Exchange Database DAG (PowerShell)
- Exchange Mail Queue (PowerShell)
- Exchange Mailbox (PowerShell)
- Exchange Public Folder (PowerShell)
- File
- File Content
- Folder
- Hyper-V Cluster Shared Volume Disk Free
- Hyper-V Host Server
- Hyper-V Virtual Machine
- Hyper-V Virtual Network Adapter
- Hyper-V Virtual Storage Device
- PerfCounter Custom
- PerfCounter IIS Application Pool
- Share Disk Free
- Windows CPU Load
- Windows IIS 6.0 SMTP Received
- Windows Network Card
- Windows Pagefile
- Windows Physical Disk I/O
- Windows Print Queue
- Windows Process
- Windows System Uptime
- Windows Updates Status (PowerShell)
- WMI Battery
- WMI Custom
- WMI Custom String
- WMI Disk Health
- WMI Event Log
- WMI Exchange Server
- WMI Exchange Transport Queue
- WMI File
- WMI Free Disk Space (Multi Disk)
- WMI HDD Health
- WMI Logical Disk I/O
- WMI Microsoft SQL Server 2008
- WMI Microsoft SQL Server 2012
- WMI Microsoft SQL Server 2014
- WMI Microsoft SQL Server 2016
- WMI Microsoft SQL Server 2017
- WMI Microsoft SQL Server 2019
- WMI Remote Ping
- WMI Security Center
- WMI Service
- WMI Share
- WMI SharePoint Process
- WMI Storage Pool
- WMI Terminal Services (Windows 2008+)
- WMI Terminal Services (Windows XP/Vista/2003)
- WMI UTC Time
- WMI Vital System Data v2
- WMI Volume
- WSUS Statistics



Credentials for Windows Systems

Domain or Computer Name

www.example.com

User Name

johnqpublic

Password

••••••••••••••••

Credentials for Window s Systems

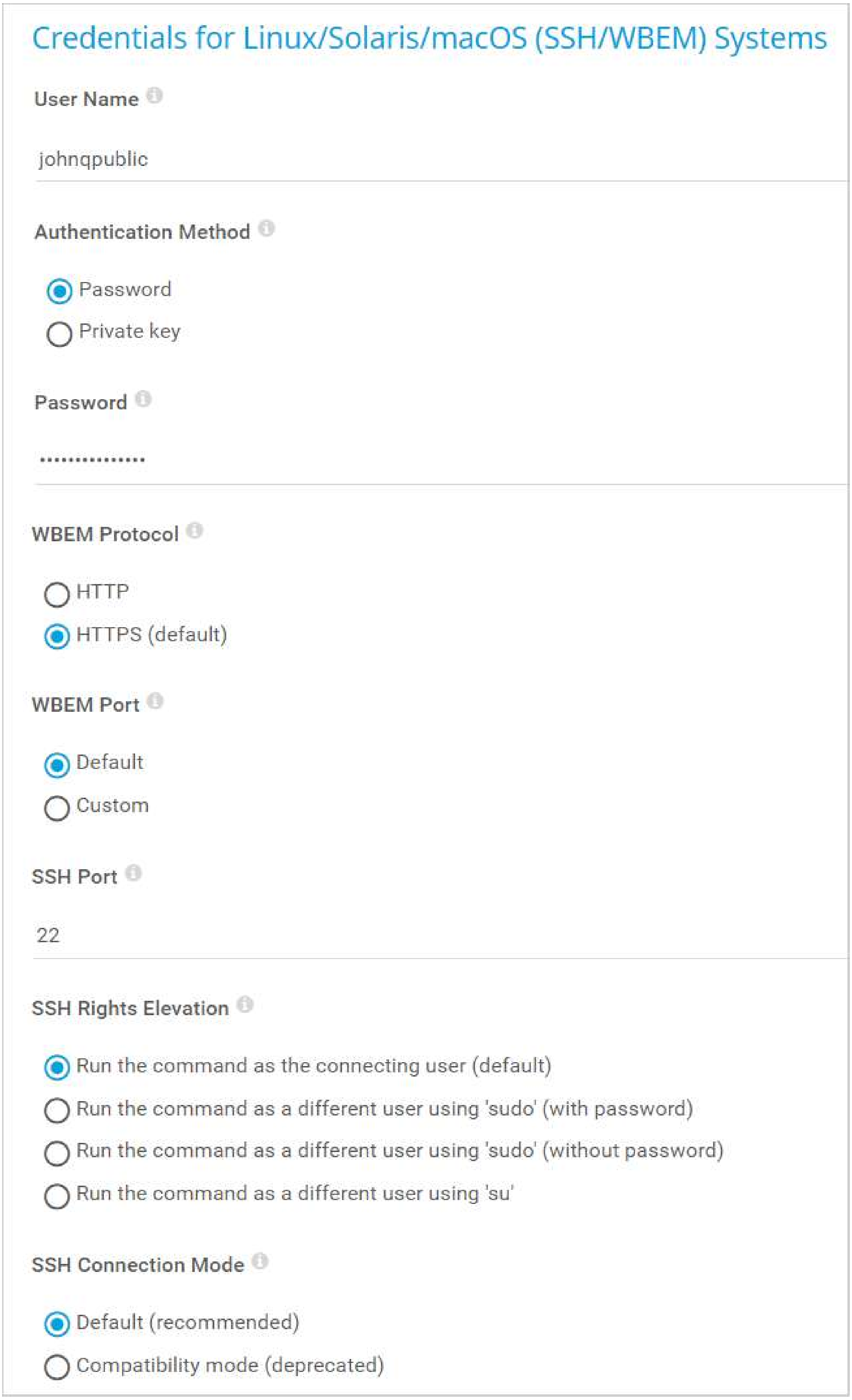
Setting	Description
Domain or Computer Name	Enter the domain or computer name of the user account with which you want to access the Windows system. PRTG uses this account for Windows Management Instrumentation (WMI) sensors and other Windows sensors. If you want to use a Windows local user account on the target device, enter the computer name. If you want to use a Windows domain user account (recommended), enter the domain name. PRTG automatically adds a prefix to use the NT LAN Manager (NTLM) protocol if you do not explicitly define it. Do not leave this field empty.
User Name	Enter the user name for access to the Windows system. Usually, you use credentials with administrator rights.
Password	Enter the password for access to the Windows system. Usually, you use credentials with administrator rights.

Credentials for Linux/Solaris/macOS (SSH/WBEM) Systems

ⓘ The settings you define in this section apply to the following sensors:

- SFTP Secure File Transfer Protocol

- SSH Disk Free
- SSH INodes Free
- SSH Load Average
- SSH Meminfo
- SSH Remote Ping
- SSH SAN Enclosure
- SSH SAN Logical Disk
- SSH SAN Physical Disk
- SSH SAN System Health
- SSH Script
- SSH Script Advanced
- VMware Host Hardware (WBEM)



Credentials for Linux/Solaris/macOS (SSH/WBEM) Systems

User Name

johnqpublic

Authentication Method

● Password
○ Private key

Password

•••••••••••••••

WBEM Protocol

○ HTTP
● HTTPS (default)

WBEM Port

● Default
○ Custom

SSH Port

22

SSH Rights Elevation

● Run the command as the connecting user (default)
○ Run the command as a different user using 'sudo' (with password)
○ Run the command as a different user using 'sudo' (without password)
○ Run the command as a different user using 'su'

SSH Connection Mode

● Default (recommended)
○ Compatibility mode (deprecated)

Setting	Description
User Name	Enter the user name for access to the Linux/Solaris/macOS system via Secure Shell (SSH) and Web-based Enterprise Management (WBEM). Usually, you use credentials with administrator rights.
Authentication Method	Select the authentication method for the login: ▪ Password: Provide the password for the login. ▪ Private key: Provide an RSA private key for authentication. ⓘ PRTG can only handle keys in the OpenSSH format that are not encrypted. You cannot use password-protected keys. ⓘ PRTG only supports RSA keys. It does not support DSA keys. 🟦 For details, see section Monitoring via SSH 3437.
Password	This setting is only visible if you select Password above. Enter a password for access to the Linux/Solaris/macOS system via SSH and WBEM. Usually, you use credentials with administrator rights.
Private Key	This setting is only visible if you select Private key above. Paste the entire RSA private key, including the BEGIN and END lines. Make sure that a corresponding public key exists on the target device. ⓘ PRTG can only handle keys in the OpenSSH format that are not encrypted. You cannot use password-protected keys. ⓘ PRTG only supports RSA keys. It does not support DSA keys. 🟦 For details, see section Monitoring via SSH 3437. ⓘ If you do not insert a private key for the first time but if you want to change the private key, you need to restart the PRTG core server service 3352 for the private key change to take effect.
WBEM Protocol	Select the protocol that you want to use for the connection to the system via WBEM: ▪ HTTP: Use an unsecure connection for WBEM. ▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection for WBEM. ⓘ This setting is only relevant if you use WBEM sensors.
WBEM Port	Select if you want to use one of the default ports for the connection to the system via WBEM or if you want to set a custom port: ▪ Default: Use one of the default ports. The default port for unsecure connections is 5988 and the default port for secure connections is 5989. ▪ Custom: Use a custom port.

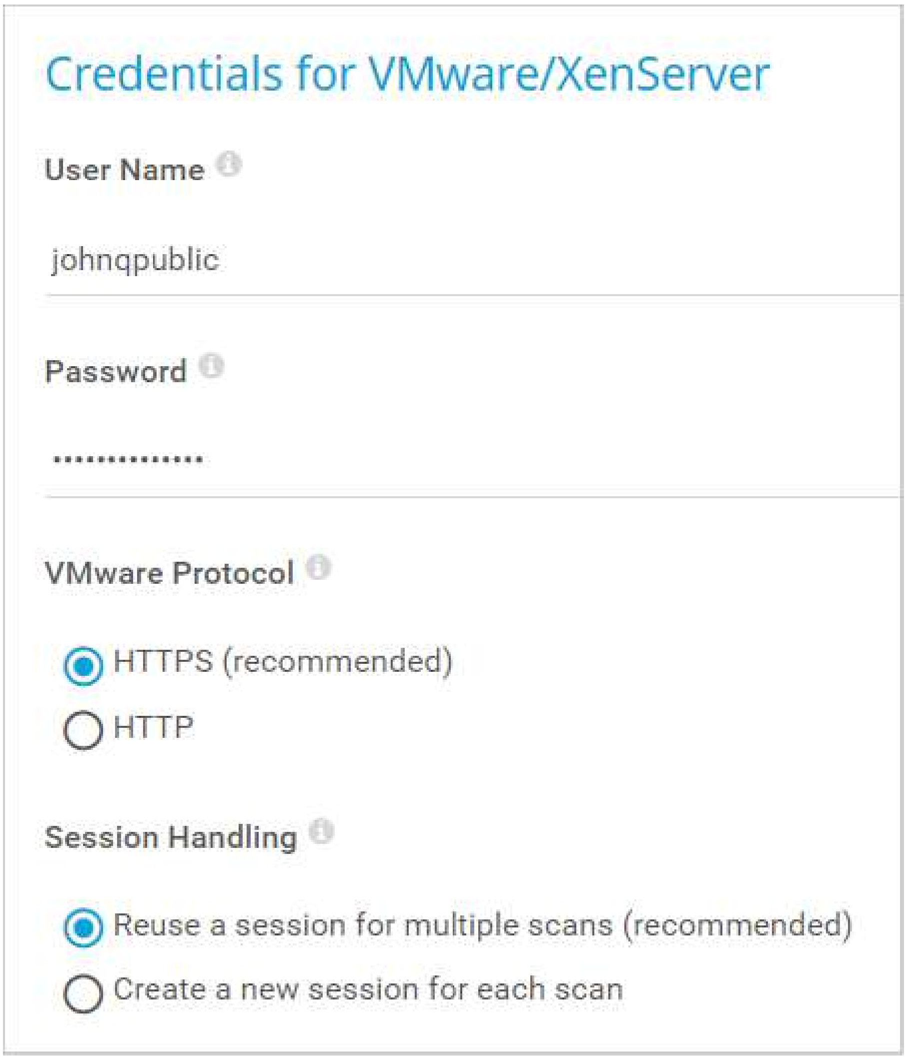
Setting	Description
	ⓘ This setting is only relevant if you use WBEM sensors.
Custom WBEM Port	This setting is only visible if you select Custom above. Enter a custom WBEM port. Enter an integer.
SSH Port	Enter the port for SSH connections. Enter an integer. The default port is 22. ⓘ By default, PRTG automatically uses this setting for all SSH sensors 3683 unless you define a different port number in the sensor settings.
SSH Rights Elevation	Select the rights that you want to use to run the command on the target system: ▪ Run the command as the connecting user (default): Use the rights of the user who establishes the SSH connection. ▪ Run the command as a different user using 'sudo' (with password): Use the rights of a different user with a password required for sudo to run commands on the target system, for example, as a root user. ▪ Run the command as a different user using 'sudo' (without password): Use the rights of a different user without a password required for sudo to run commands on the target system, for example, as a root user. ▪ Run the command as a different user using 'su': Use the rights of a different user with su to run commands on the target system.
Target System User Name	This setting is only visible if you select an option that includes sudo or su above. Enter a user name to run the specified command on the target system as a different user than the root user. If you leave this field empty, you run the command as a root user. Make sure that you set the Linux password even if you use a public key or a private key for authentication. This is not necessary if the user is allowed to run the command without a password.
Password	This setting is only visible if you select an option that includes sudo or su with password above. Enter the password to run the sudo command or the su command.
SSH Connection Mode	Select the connection mode that you want to use to access data with SSH sensors 3437: ▪ Default (recommended): This is the default connection mode for SSH sensors. It provides the best performance and security. ▪ Compatibility mode (deprecated): Use this only if the default connection mode does not work on the target system. The compatibility mode is the connection mode that PRTG used in previous versions and it is deprecated.

Setting	Description
	ⓘ We strongly recommend that you use the default connection mode. ⓘ You can also individually select the connection mode for each SSH sensor in the sensor settings.

Credentials for VMware/XenServer

ⓘ The settings you define in this section apply to the following sensors:

- Citrix XenServer Host
- Citrix XenServer Virtual Machine
- VMware Datastore (SOAP)
- VMware Host Hardware (WBEM)
- VMware Host Hardware Status (SOAP)
- VMware Host Performance (SOAP)
- VMware Virtual Machine (SOAP)



Credentials for VMware/XenServer

User Name

johnqpublic

Password

••••••••••••••

VMware Protocol

● HTTPS (recommended)
○ HTTP

Session Handling

● Reuse a session for multiple scans (recommended)
○ Create a new session for each scan

Credentials for VMw are/XenServer

Setting	Description
User Name	Enter the user name for access to VMware ESXi, vCenter Server, or Citrix XenServer. Usually, you use credentials with administrator rights.
Password	Enter the password for access to VMware ESXi, vCenter Server, or Citrix XenServer. Usually, you use credentials with administrator rights. ⓘ Single sign-on (SSO) passwords for vSphere do not support special characters. For details, see the VMware sensors sections.
VMware Protocol	Select the protocol for the connection to VMware ESXi, vCenter Server, or Citrix XenServer: ▪ HTTPS (recommended): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection. ▪ HTTP: Use an unsecure connection.

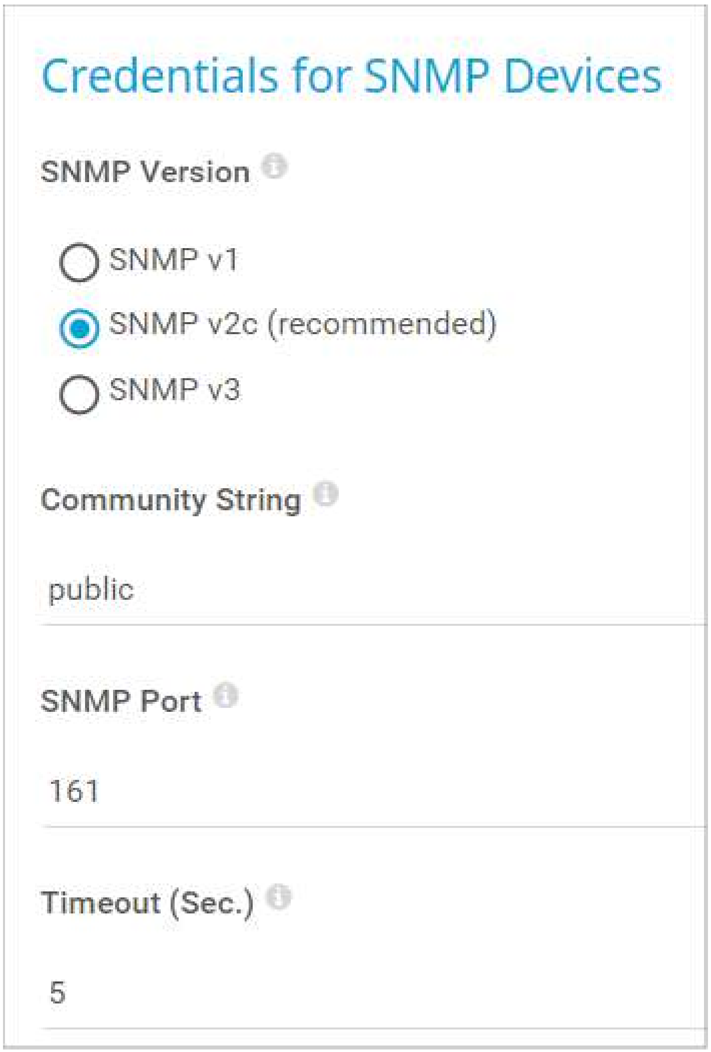
Setting	Description
Session Handling	Select if you want to reuse a session for VMware sensors: ▪ Reuse a session for multiple scans (recommended): Select this option if you want a VMware sensor to reuse a single session for multiple sensor scans to query data. With this option, the sensor does not need to log in and out for each sensor scan. We recommend that you use this option because it reduces network load and log entries on the target device. This can increase performance. ▪ Create a new session for each scan: If you select this option, PRTG does not reuse a session and a VMware sensor has to log in and out for each sensor scan. This can decrease performance.

Credentials for SNMP Devices

ⓘ The settings you define in this section apply to the following sensors:

- Cisco IP SLA
- SNMP APC Hardware
- SNMP Buffalo TS System Health
- SNMP Cisco ADSL
- SNMP Cisco ASA VPN Connections
- SNMP Cisco ASA VPN Traffic
- SNMP Cisco ASA VPN Users
- SNMP Cisco CBQoS
- SNMP Cisco System Health
- SNMP Cisco UCS Blade
- SNMP Cisco UCS Chassis
- SNMP Cisco UCS Physical Disk
- SNMP Cisco UCS System Health
- SNMP CPU Load
- SNMP Custom
- SNMP Custom Advanced
- SNMP Custom String
- SNMP Fujitsu System Health v2
- SNMP Hardware Status
- SNMP HP LaserJet Hardware
- SNMP HPE BladeSystem Blade
- SNMP HPE BladeSystem Enclosure System Health
- SNMP HPE ProLiant Logical Disk
- SNMP HPE ProLiant Memory Controller
- SNMP HPE ProLiant Network Interface
- SNMP HPE ProLiant Physical Disk
- SNMP HPE ProLiant System Health
- SNMP IBM System X Logical Disk
- SNMP IBM System X Physical Disk
- SNMP IBM System X Physical Memory
- SNMP NetApp Enclosure
- SNMP NetApp I/O
- SNMP NetApp License
- SNMP NetApp Logical Unit
- SNMP NetApp Network Interface
- SNMP NetApp System Health
- SNMP Nutanix Cluster Health
- SNMP Nutanix Hypervisor
- SNMP Poseidon Environment
- SNMP Printer
- SNMP QNAP Logical Disk
- SNMP QNAP Physical Disk
- SNMP QNAP System Health
- SNMP Rittal CMC III Hardware Status
- SNMP RMON
- SNMP SonicWall System Health
- SNMP SonicWall VPN Traffic
- SNMP Synology Logical Disk

- SNMP Custom String Lookup
- SNMP Custom Table
- SNMP Dell EqualLogic Logical Disk
- SNMP Dell EqualLogic Member Health
- SNMP Dell EqualLogic Physical Disk
- SNMP Dell Hardware
- SNMP Dell PowerEdge Physical Disk
- SNMP Dell PowerEdge System Health
- SNMP Disk Free
- SNMP IBM System X System Health
- SNMP interSeptor Pro Environment
- SNMP Juniper NS System Health
- SNMP LenovoEMC Physical Disk
- SNMP LenovoEMC System Health
- SNMP Library
- SNMP Linux Disk Free
- SNMP Linux Load Average
- SNMP Linux Meminfo
- SNMP Linux Physical Disk
- SNMP Memory
- SNMP NetApp Disk Free
- SNMP Synology Physical Disk
- SNMP Synology System Health
- SNMP System Uptime
- SNMP Traffic
- SNMP Trap Receiver
- SNMP Windows Service



Credentials for SNMP Devices

SNMP Version

○ SNMP v1
● SNMP v2c (recommended)
○ SNMP v3

Community String: public

SNMP Port: 161

Timeout (Sec.): 5

Credentials for SNMP Devices

Setting	Description
SNMP Version	Select the Simple Network Management Protocol (SNMP) version for the connection to the target SNMP device: ▪ SNMP v1: Use SNMP v1 for the connection. SNMP v1 only offers clear-text data transmission. ⓘ SNMP v1 does not support 64-bit counters. This might result in invalid data when you monitor traffic via SNMP. ▪ SNMP v2c (recommended): Use SNMP v2c for the connection. SNMP v2c also only offers clear-text data transmission but it supports 64-bit counters.

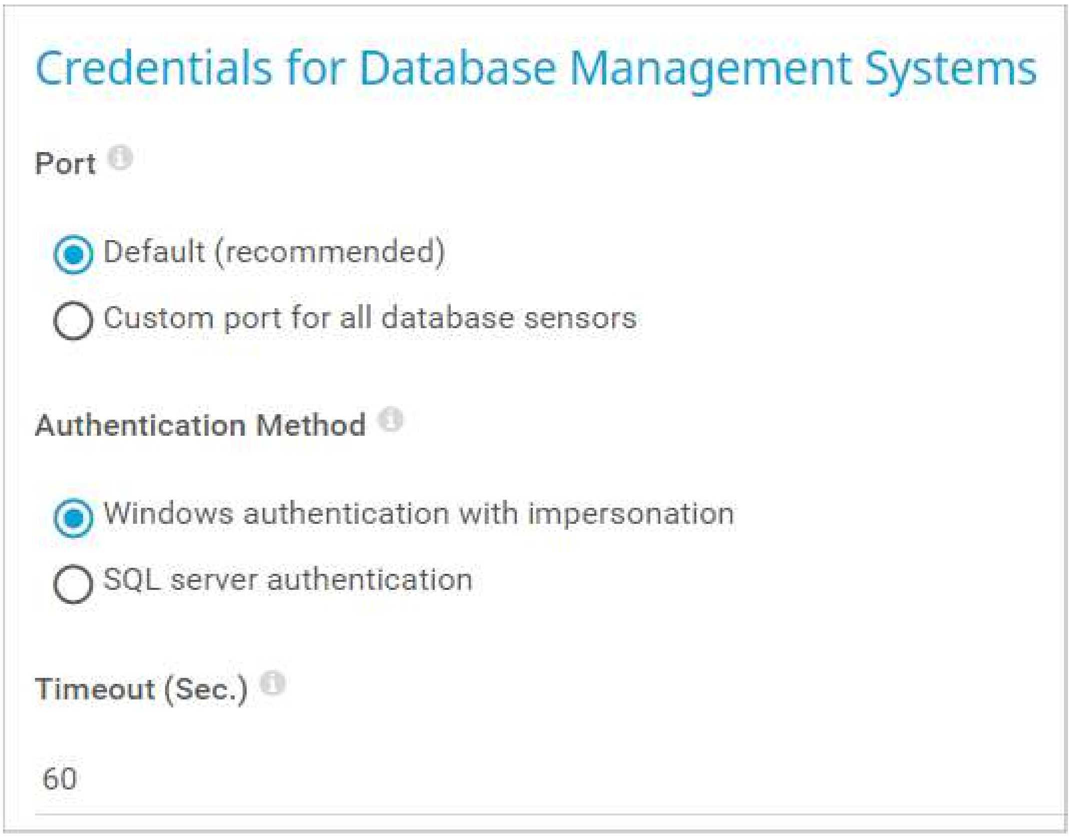
Setting	Description
	▪ SNMP v3: Use SNMP v3 for the connection. SNMP v3 provides secure authentication and data encryption. ⓘ SNMP v3 has performance limitations because of the use of encryption. The main limiting factor is CPU power. Also keep in mind that SNMP v3, unlike SNMP v1 and v2c, does not scale with more CPU power. Because of this limitation, PRTG can only handle a limited number of requests per second so that you can use only a limited number of sensors using SNMP v3. If you see an increase in Interval Delay or Open Requests with the Probe Health sensor, distribute the load over multiple probes 3621. SNMP v1 and SNMP v2c do not have this limitation.
Community String	This setting is only visible if you select SNMP v1 or SNMP v2c (recommended) above. Enter the community string of your device. This is like a clear-text password for simple authentication. ⓘ We recommend that you use the default value.
Authentication Method	This setting is only visible if you select SNMP v3 above. Select the authentication method: ▪ MD5: Use message-digest algorithm 5 (MD5) for authentication. ▪ SHA: Use Secure Hash Algorithm (SHA) for authentication. ▪ SHA-224: Use SHA-224 for authentication. ▪ SHA-256: Use SHA-256 for authentication. ▪ SHA-384: Use SHA-384 for authentication. ▪ SHA-512: Use SHA-512 for authentication. ⓘ If you do not want to use authentication but you need SNMP v3, for example, because your device requires context, you can leave the Password field empty. In this case, PRTG uses SNMP_SEC_LEVEL_NOAUTH and it entirely deactivates authentication. ⓘ The authentication method you select must match the authentication method of your device.
User Name	This setting is only visible if you select SNMP v3 above. Enter the user name for access to the target SNMP device. ⓘ The user name that you enter must match the user name of your device.
Password	This setting is only visible if you select SNMP v3 above. Enter the password for access to the target SNMP device. ⓘ The password that you enter must match the password of your device.

Setting	Description
Encryption Type	This setting is only visible if you select SNMP v3 above. Select an encryption type: ▪ DES: Use Data Encryption Standard (DES) as the encryption algorithm. ▪ AES: Use Advanced Encryption Standard (AES) as the encryption algorithm. ▪ AES-192: Use AES-192 as the encryption algorithm. ▪ AES-256: Use AES-256 as the encryption algorithm. ⓘ The encryption type that you select must match the encryption type of your device.
Encryption Key	This setting is only visible if you select SNMP v3 above. Enter an encryption key. If you provide a key, PRTG encrypts SNMP data packets with the encryption algorithm that you selected above. Enter a string or leave the field empty. ⓘ The encryption key that you enter must match the encryption key of your device. If the encryption keys do not match, you do not get an error message.
Context Name	This setting is only visible if you select SNMP v3 above. Enter a context name only if the configuration of the device requires it. Context is a collection of management information that is accessible by an SNMP device. Enter a string.
SNMP Port	Enter the port for the connection to the SNMP target device. Enter an integer. The default port is 161. ⓘ We recommend that you use the default value.
Timeout (Sec.)	Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is 300 seconds (5 minutes).

Credentials for Database Management Systems

ⓘ The settings you define in this section apply to the following sensors:

- ADO SQL v2
- Microsoft SQL v2
- MySQL v2
- Oracle SQL v2
- PostgreSQL



Credentials for Database Management Systems

Port

● Default (recommended)
○ Custom port for all database sensors

Authentication Method

● Windows authentication with impersonation
○ SQL server authentication

Timeout (Sec.)

60

Credentials for Database Management Systems

Setting	Description
Port	Select the port that PRTG uses for connections to the monitored databases: ▪ Default (recommended): PRTG automatically determines the type of the database and uses the corresponding default port to connect. PRTG uses the following default ports: ▫ Microsoft SQL: 1433 ▫ MySQL: 3306 ▫ Oracle SQL: 1521 ▫ PostgreSQL: 5432 ▪ Custom port for all database sensors: Select this option if your database management systems do not use the default ports. Enter a custom port for database connections below. ⓘ PRTG uses this custom port for all database sensors and for connections to all your databases.
Custom Port	Enter a custom port for database connections. Enter an integer.

Setting	Description
	ⓘ PRTG uses this custom port for all database sensors and for connections to all your databases.
Authentication Method	Select the authentication method for the connection to the Structured Query Language (SQL) database: ▪ Windows authentication with impersonation: PRTG uses the Windows credentials that you define in settings that are higher in the object hierarchy 131, for example, in the settings of the parent device; for the database connection. ⓘ The user whose credentials PRTG uses needs to have permission to log in to the probe system with a database sensor. This is necessary for the impersonation. ▪ SQL server authentication: Use explicit credentials for database connections. Enter a user name and password below.
User Name	This setting is only visible if you select SQL server authentication above. Enter the user name for the database connection.
Password	This setting 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. Enter an integer. The maximum timeout value is 300 seconds (5 minutes).

Credentials for AWS

ⓘ The settings you define in this section apply to the following sensors:

- AWS Alarm v2
- AWS Cost
- AWS EBS v2
- AWS EC2 v2
- AWS ELB v2
- AWS RDS v2

For more information about the permissions that are necessary to query the AWS API, see the Knowledge Base: How do I set permissions for the Amazon Web Services (AWS) API key to use certain sensors in PRTG?

Credentials for AWS

Access Key

Secret Key

Credentials for AWS

Setting	Description
Access Key	Enter the Amazon Web Services (AWS) access key.
Secret Key	Enter the AWS secret key.

Credentials for Microsoft 365

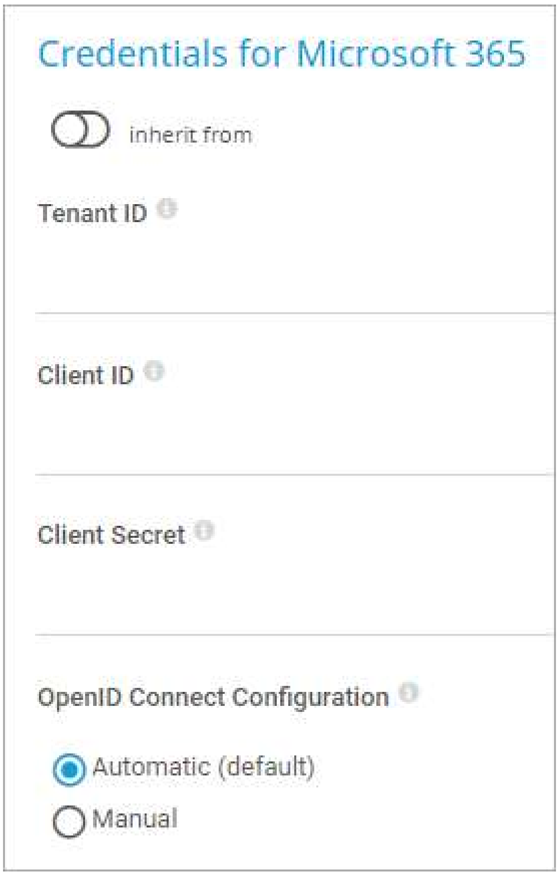
ⓘ The settings you define in this section apply to the following sensors:

- Microsoft 365 Mailbox
- Microsoft 365 Service Status
- Microsoft 365 Service Status Advanced

The sensors use the credentials to authenticate with Azure Active Directory (Azure AD).

For more information about the credentials and the permissions that are necessary to use the Microsoft 365 Service Status sensor and the Microsoft 365 Service Status Advanced sensor, see the Knowledge Base: How do I obtain credentials and set permissions for the Microsoft 365 Service Status sensors?

For more information about the credentials and the permissions that are necessary to use the Microsoft 365 Mailbox sensor, see the Knowledge Base: How do I obtain credentials and set permissions for the Microsoft 365 Mailbox sensor?



Credentials for Microsoft 365

inherit from

Tenant ID

Client ID

Client Secret

OpenID Connect Configuration

● Automatic (default)
○ Manual

Credentials for Microsoft 365

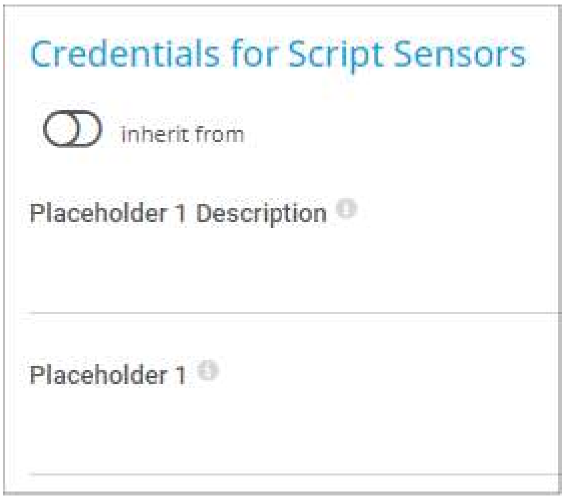
Setting	Description
Tenant ID	Enter the Azure AD tenant ID. ⓘ A tenant ID must be a 32-digit sequence in hexadecimal notation.
Client ID	Enter the Azure AD client ID.
Client Secret	Enter the Azure AD client secret.
OpenID Connect Configuration	Select if you want to manually enter the authorization endpoint URL and token endpoint URL that PRTG uses to access Microsoft Graph. Choose between: ▪ Automatic (default): PRTG automatically determines the authorization endpoint URL and the token endpoint URL. ▪ Manual: Manually enter the authorization endpoint URL and the token endpoint URL.
Authorization Endpoint	Enter the authorization endpoint URL including the server. Authorization endpoint URL example:

Setting	Description
	`https://login.microsoftonline.com/<tenant-ID>/oauth2/v2.0/authorize` ⓘ Make sure to replace <tenant-ID> with the directory (tenant) ID from Azure AD.
Token Endpoint	Enter the token endpoint URL including the server. Token endpoint URL example: `https://login.microsoftonline.com/<tenant-ID>/oauth2/v2.0/token` ⓘ Make sure to replace <tenant-ID> with the directory (tenant) ID from Azure AD.

Credentials for Script Sensors

ⓘ The settings you define in this section apply to the following sensors:

- EXE/Script
- EXE/Script Advanced
- Python Script Advanced
- SSH Script
- SSH Script Advanced



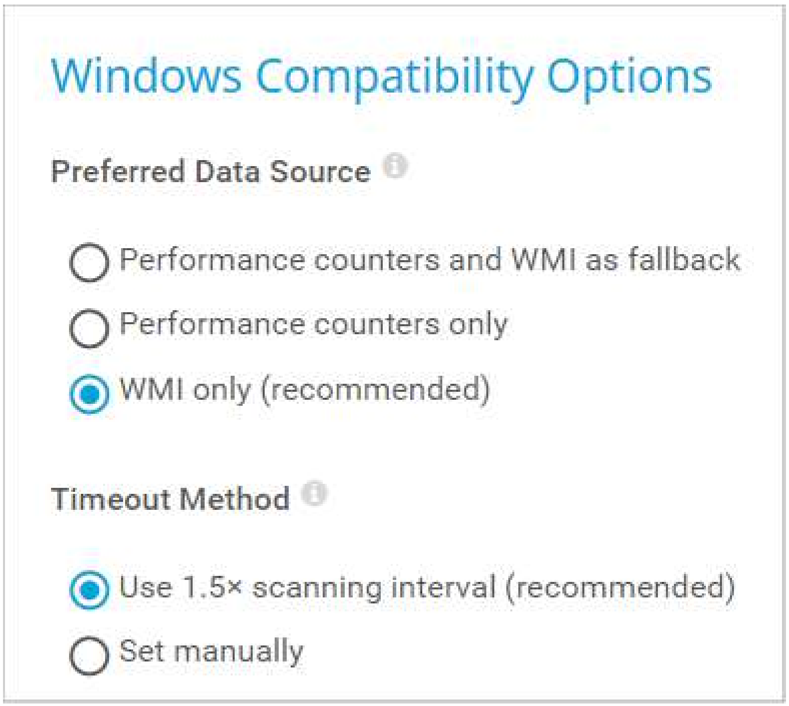
Credentials for Script Sensors

Setting	Description
Placeholder 1 Description	Enter a description for Placeholder 1, for example information about the purpose or content of the placeholder.

Setting	Description
Placeholder 1	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add %scriptplaceholder1 in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 2 Description	Enter a description for Placeholder 2, for example information about the purpose or content of the placeholder.
Placeholder 2	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add %scriptplaceholder2 in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 3 Description	Enter a description for Placeholder 3, for example information about the purpose or content of the placeholder.
Placeholder 3	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add %scriptplaceholder3 in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 4 Description	Enter a description for Placeholder 4, for example information about the purpose or content of the placeholder.
Placeholder 4	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add %scriptplaceholder4 in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 5 Description	Enter a description for Placeholder 5, for example information about the purpose or content of the placeholder.
Placeholder 5	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add %scriptplaceholder5 in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.

Windows Compatibility Options

If you experience problems when you monitor via Windows sensors, use the following compatibility options for troubleshooting.



Windows Compatibility Options

Preferred Data Source

○ Performance counters and WMI as fallback
○ Performance counters only
● WMI only (recommended)

Timeout Method

● Use 1.5× scanning interval (recommended)
○ Set manually

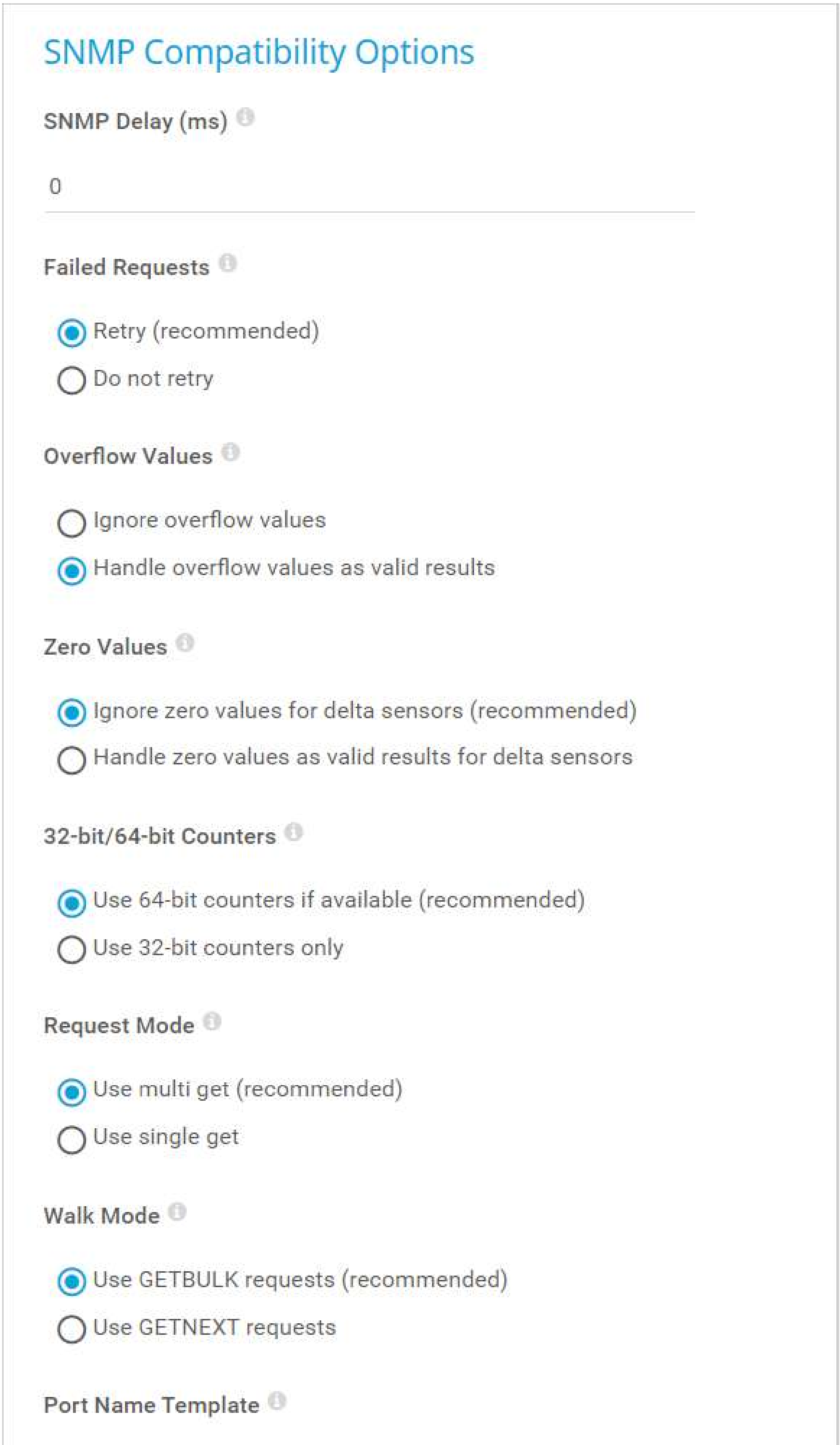
Window s Compatibility Options

Setting	Description
Preferred Data Source	ⓘ This setting only applies to hybrid sensors that use both performance counters and Windows Management Instrumentation (WMI). The setting does not apply to other sensors. Define the method that Windows sensors use to query data: ▪ Performance counters and WMI as fallback: 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, the sensor returns no data. ▪ WMI only (recommended): Query data via WMI only. If this is not possible, the sensor returns no data. We recommend that you use this option.
Timeout Method	Select the time that the sensor waits for the return of the WMI query before the sensor cancels the query and shows an error message: ▪ Use 1.5× scanning interval (recommended): Multiply the scanning interval of the sensor by 1.5 and use the resulting value. ▪ Set manually: Manually enter a timeout value. ⓘ We recommend that you use the default value. ⓘ If you experience ongoing timeout errors, try increasing the timeout value.

Setting	Description
Timeout (Sec.)	This setting is only visible if you select Set manually above. Enter the time the sensor waits for the return of its WMI query before it cancels it and shows an error message. Enter an integer. The maximum timeout value is 900 seconds (15 minutes).

SNMP Compatibility Options

If you experience problems when you monitor via Simple Network Management Protocol (SNMP) sensors, use the following compatibility options for troubleshooting.



SNMP Compatibility Options

SNMP Delay (ms)

0

Failed Requests

● Retry (recommended)

○ Do not retry

Overflow Values

○ Ignore overflow values

● Handle overflow values as valid results

Zero Values

● Ignore zero values for delta sensors (recommended)

○ Handle zero values as valid results for delta sensors

32-bit/64-bit Counters

● Use 64-bit counters if available (recommended)

○ Use 32-bit counters only

Request Mode

● Use multi get (recommended)

○ Use single get

Walk Mode

● Use GETBULK requests (recommended)

○ Use GETNEXT requests

Port Name Template

Setting	Description
SNMP Delay (ms)	Enter the time in milliseconds (ms) that PRTG waits between two SNMP requests. This can increase device compatibility. Enter an integer. You can define a delay between 0 and 100. PRTG does not support higher delays. ⓘ We recommend that you use the default value. ⓘ If you experience SNMP connection failures, try increasing the delay.
Failed Requests	Select if an SNMP sensor tries again after a request fails: ▪ Retry (recommended): Try again if an SNMP request fails. This can prevent false error messages because of temporary timeout failures. ▪ Do not retry: Do not retry if an SNMP request fails. If you select this option, an SNMP sensor shows a Down status earlier.
Overflow Values	Select how PRTG handles overflow values. Some devices do not correctly handle internal buffer overflows. This can cause false peaks. ▪ Ignore (default): Ignore overflow values and do not include them in the monitoring data. We recommend that you use this option. ▪ Handle overflow values as valid results: Regard all overflow values as regular data and include them in the monitoring data. ⓘ If you experience problems because of strange peaks in your data graphs, change this option. Peaks might indicate that the target device resets counters without an overflow. PRTG interprets such behavior as overflow that results in data peaks. Select the option Ignore (default) in this case. For more details, see the Knowledge Base: What is the Overflow Values setting in the SNMP Compatibility Options?
Zero Values	Select how PRTG handles zero values. Some devices send incorrect zero values. This can cause false peaks. ▪ Ignore (recommended): Ignore zero values and do not include them in the monitoring data. We recommend that you use this option. ⓘ If you experience problems, try changing this option. ▪ Handle zero values as valid results for delta sensors: Regard all zero values as regular data and include them in the monitoring data.
32-bit/64-bit Counters	Select the type of traffic counters that PRTG searches for on a device: ▪ Use 64-bit counters if available (recommended): The interface scan uses 64-bit traffic counters, if available. This can avoid buffer overflows in the devices ⓘ We recommend that you use the default value. ⓘ If you experience problems, try changing this option.

Setting	Description
	▪ Use 32-bit counters only: The interface scan always uses 32-bit traffic counters, even if 64-bit counters are available. This can make monitoring more reliable for some devices.
Request Mode	Select the request method that PRTG uses for SNMP sensors: ▪ Use multi get (recommended): Bundle multiple SNMP requests into one request. We recommend that you use this option. ⓘ If you experience problems, try changing this option. ▪ Use single get: Use one request for each SNMP value. This can increase compatibility with older devices. ⓘ PRTG uses paging for SNMP requests. This means that if a sensor has to query more than 20 object identifiers (OID), it automatically polls the OIDs in packages of 20 OIDs each.
Walk Mode	Select the kind of SNMP walk that PRTG uses for SNMP sensors: ▪ Use GETBULK requests (recommended): Request the next x OIDs in one SNMP request. The default value is 10. It is dynamic based on the response size. ⓘ This option only works with devices that support SNMP as of version v2c. Make sure that you set the correct SNMP Version in the Credentials for SNMP Devices settings of the parent device or inherit it from objects that are higher in the object hierarchy 131. ▪ Use GETNEXT requests: Request one OID at a time. This can increase compatibility with older devices or with devices that have insufficient SNMP BULKWALK support.
Port Name Template	Select how PRTG displays the name of SNMP sensors. Enter a template that uses several variables. When you add new sensors, PRTG scans the interface for available counters at certain OIDs. At each OID, several fields with interface descriptions are usually available. They are different for every device and OID. PRTG uses the information in these fields to name the sensors. If a field is empty or if it is not available, PRTG adds an empty string to the name. By default, the port name template is ([port]) [ifalias] [ifsensor], which creates a name like (001) Ethernet1 Traffic. You can use and combine any field names that are available at an OID of your device, for example: ▪ [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 target device or interface, for example, manufacturer, product name, or version.

Setting	Description
	▪ [ifspeed]: An estimate of the monitored interface's current bandwidth (Kbit/s). ▪ [ifsensor]: The type of the sensor, this is Traffic or RMON. This helps to differentiate between SNMP Traffic and SNMP RMON sensors. 🟦 For more information about SNMP sensor names, see the Knowledge Base: How can I change the defaults for names automatically generated for new SNMP sensors?
Port Name Update	Select how PRTG reacts if you change the names of ports in your physical device (for example, a switch or router): ▪ 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 manually change names in PRTG. ▪ Automatically update sensor names if port names change in the device: If PRTG detects port name changes in your physical device, it tries to automatically adjust the sensor names accordingly. 🟦 For more information about automatic name updates, see the Knowledge Base: Automatically update port name and number for SNMP Traffic sensors when the device changes them.
Port Identification	Select the field that PRTG uses for SNMP interface identification: ▪ Automatic identification (recommended): Try the ifAlias field first to identify an SNMP interface and then try ifDescr. ⓘ PRTG does not automatically try ifName. ▪ Use ifAlias: For most devices, ifAlias is the best field to use for unique interface names. ▪ Use ifDescr: Use this option if the port order of your device changes after a restart, and if no ifAlias field is available. For example, this is the best option for Cisco ASA devices. ⓘ If you use 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 no unique ifAlias is available. ⓘ If you use this option, it is important that your device returns unique interface names in the ifName field. ▪ Do not update ports: Use this option to disable the automatic port identification.
Start Interface Index	ⓘ This setting only applies to SNMP Traffic sensors and to Cisco IP SLA sensors. Enter the index at which PRTG starts to query the interface range during sensor creation. Enter 0 for the automatic mode.

Setting	Description
	ⓘ We recommend that you use the default value.
End Interface Index	ⓘ This setting only applies to SNMP Traffic sensors and to Cisco IP SLA sensors. Enter the index at which PRTG stops querying the interface range during sensor creation. Enter 0 for the automatic mode. ⓘ We recommend that you use the default value.

Proxy Settings for HTTP Sensors

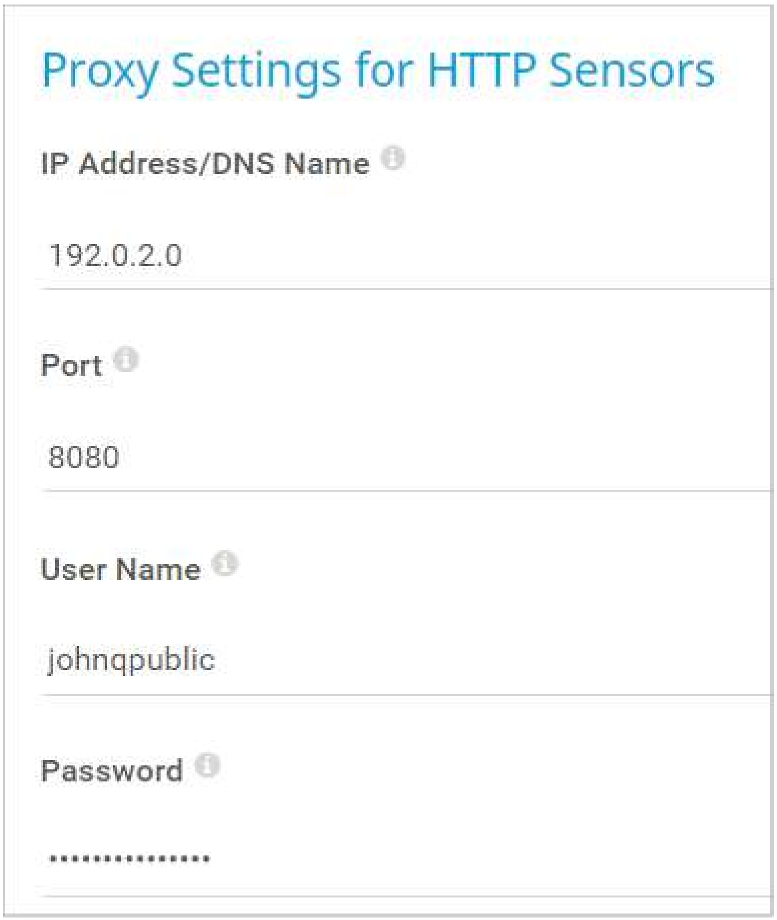
ⓘ The settings you define in this section apply to the following sensors:

- HTTP
- HTTP Advanced
- HTTP Apache ModStatus PerfStats
- HTTP Apache ModStatus Totals
- HTTP Content
- HTTP Data Advanced
- HTTP Transaction
- REST Custom

The proxy settings determine how a sensor connects to a URL. You can enter data for an HTTP proxy server that sensors use when they connect via HTTP or HTTPS.

ⓘ This setting only applies to HTTP sensors and how they monitor. To change the proxy settings for the PRTG core server, see section Core & Probes 3325.

ⓘ The SSL Certificate sensor and the SSL Security Check sensor do not support HTTP proxies but you can configure connections via SOCKS proxies in the sensors' settings:



Proxy Settings for HTTP Sensors

IP Address/DNS Name ⓘ

192.0.2.0

Port ⓘ

8080

User Name ⓘ

johnqpublic

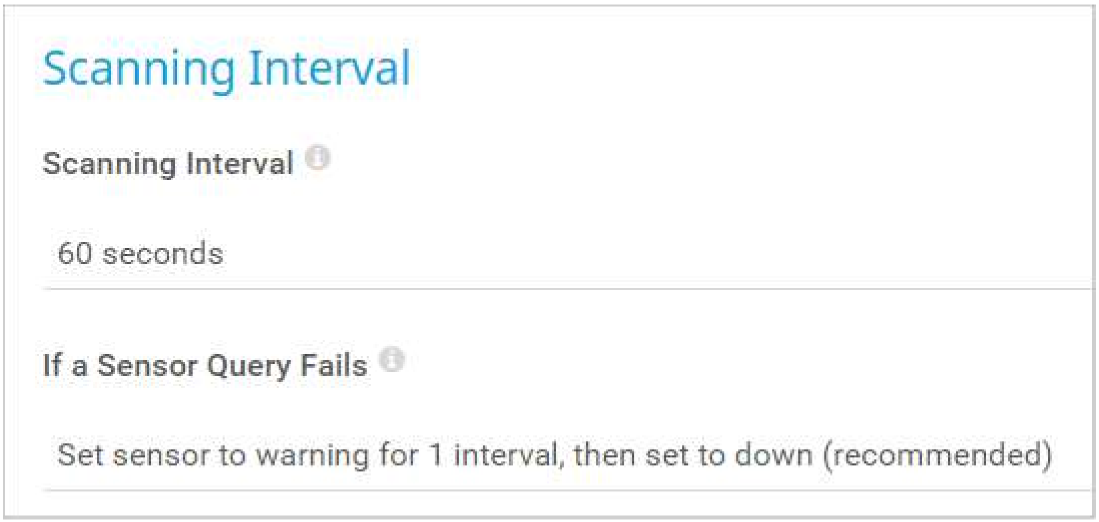
Password ⓘ

•••••••••••••••

Proxy Settings for HTTP Sensors

Setting	Description
IP Address/DNS Name	Enter the IP address or Domain Name System (DNS) name of the proxy server. If you leave this field empty, HTTP sensors do not use a proxy.
Port	Enter the port number of the proxy. The default port is 8080. Enter an integer.
User Name	If the proxy requires authentication, enter the user name for the proxy login. ⓘ Only basic authentication is available. 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. Enter a string or leave the field empty.

Scanning Interval



Scanning Interval

Scanning Interval

60 seconds

If a Sensor Query Fails

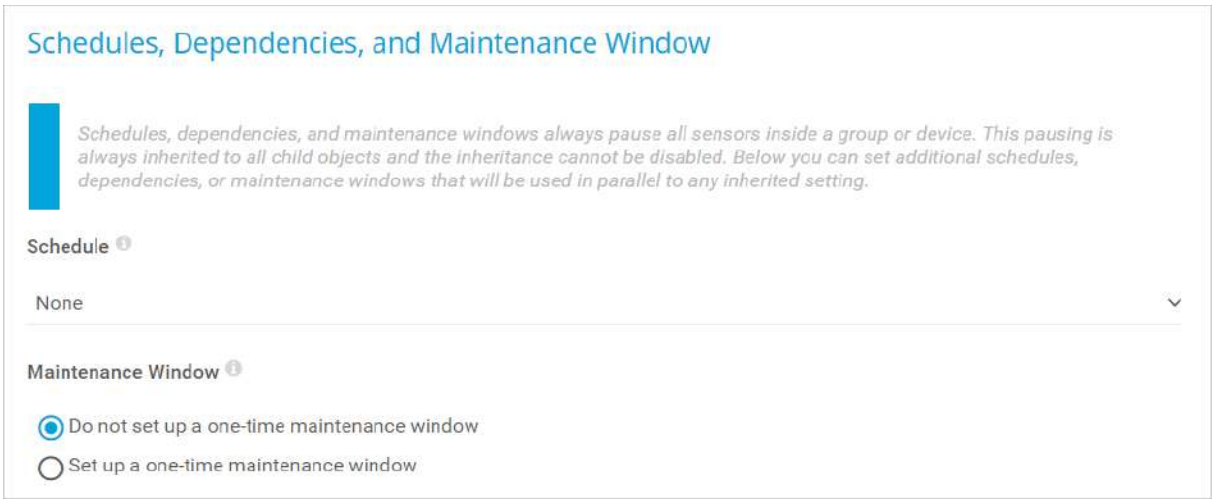
Set sensor to warning for 1 interval, then set to down (recommended)

Scanning Interval

Setting	Description
Scanning Interval	Select a scanning interval from the dropdown list. The scanning interval determines the amount of time that the sensor waits between two scans. Choose from: ▪ 30 seconds ▪ 60 seconds ▪ 5 minutes ▪ 10 minutes ▪ 15 minutes ▪ 30 minutes ▪ 1 hour ▪ 4 hours ▪ 6 hours ▪ 12 hours ▪ 24 hours ⓘ You can change the available intervals in the system administration 3307 of PRTG Network Monitor.

Setting	Description
If a Sensor Query Fails	Select the number of scanning intervals that the sensor has time to reach and to check a device again if a sensor query fails. Depending on the option that you select, the sensor can try to reach and to check a device again several times before the sensor shows the Down status 179. This can avoid false alarms if the target device only has temporary issues. For previous scanning intervals with failed requests, the sensor shows the Warning status. Choose from: ▪ Set sensor to down status immediately: Set the sensor to the Down status immediately after the first request fails. ▪ Set sensor to warning status for 1 interval, then set to down status (recommended): Set the sensor to the Warning status after the first request fails. If the second request also fails, the sensor shows the Down status. ▪ Set sensor to warning status for 2 intervals, then set to down status: Set the sensor to the Down status only after the third request fails. ▪ Set sensor to warning status for 3 intervals, then set to down status: Set the sensor to the Down status only after the fourth request fails. ▪ Set sensor to warning status for 4 intervals, then set to down status: Set the sensor to the Down status only after the fifth request fails. ▪ Set sensor to warning status for 5 intervals, then set to down status: Set the sensor to the Down status only after the sixth request fails. ⓘ Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval before they show the Down status. It is not possible to immediately set a WMI sensor to the Down status, so the first option does not apply to these sensors. All other options can apply. ⓘ If you define error limits for a sensor's channels, the sensor immediately shows the Down status. None of the interval options apply. ⓘ If a channel uses lookup 3604 values, the sensor immediately shows the Down status. None of the interval options apply.

Schedules, Dependencies, and Maintenance Window



Schedules, Dependencies, and Maintenance Window

Schedules, dependencies, and maintenance windows always pause all sensors inside a group or device. This pausing is always inherited to all child objects and the inheritance cannot be disabled. Below you can set additional schedules, dependencies, or maintenance windows that will be used in parallel to any inherited setting.

Schedule

None

Maintenance Window

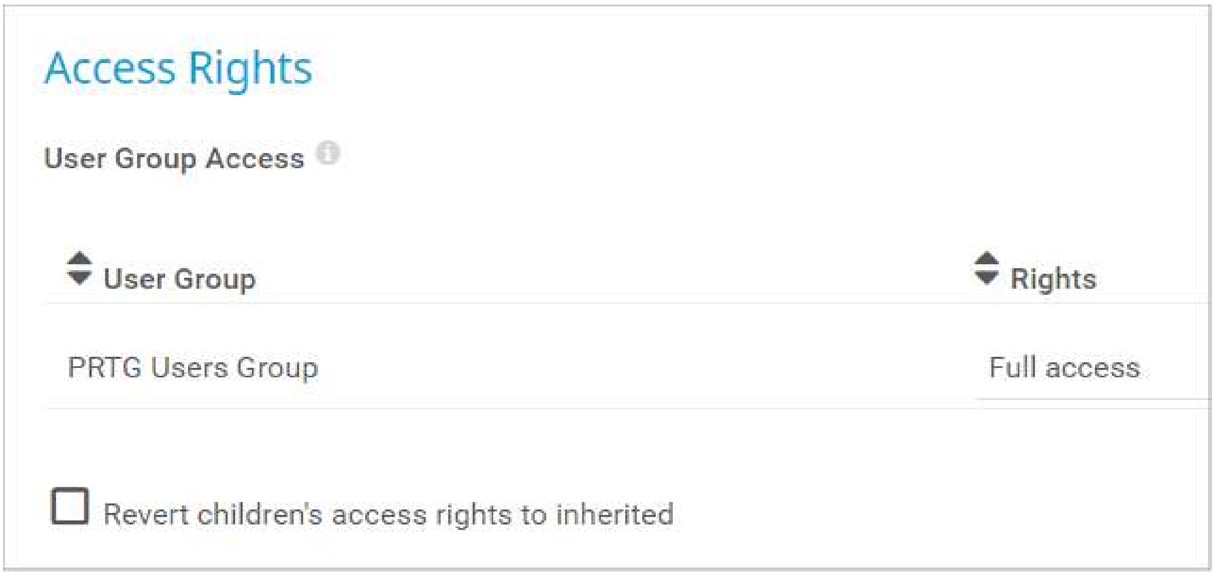
● Do not set up a one-time maintenance window
○ Set up a one-time maintenance window

Schedules, Dependencies, and Maintenance Window

Setting	Description
Schedule	Select a schedule from the list. You can use schedules to monitor during a certain time span (days or hours) every week. Choose from: ▪ None ▪ Saturdays ▪ Sundays ▪ Weekdays ▪ Weekdays Eight-To-Eight (08:00 - 20:00) ▪ Weekdays Nights (17:00 - 09:00) ▪ Weekdays Nights (20:00 - 08:00) ▪ Weekdays Nine-To-Five (09:00 - 17:00) ▪ Weekends ⓘ You can create schedules, edit schedules, or pause monitoring for a specific time span. For more information, see section Schedules 3286.
Maintenance Window	Select if you want to set up a one-time maintenance window. During a maintenance window, monitoring stops for the selected object and all child objects. They show the Paused status instead. Choose between: ▪ Do not set up a one-time maintenance window: Do not set up a one-time maintenance window. Monitoring is always active. ▪ Set up a one-time maintenance window: Set up a one-time maintenance window and pause monitoring. You can define a time span for the pause below.

Setting	Description
	ⓘ To close an active one-time maintenance window before the end date, select Do not set up a one-time maintenance window.
Maintenance Begins	This setting is only visible if you enable Set up a one-time maintenance window above. Use the date time picker to enter the start date and time of the one-time maintenance window.
Maintenance Ends	This setting is only visible if you enable Set up a one-time maintenance window above. Use the date time picker to enter the end date and time of the one-time maintenance window.

Access Rights



Access Rights

User Group Access

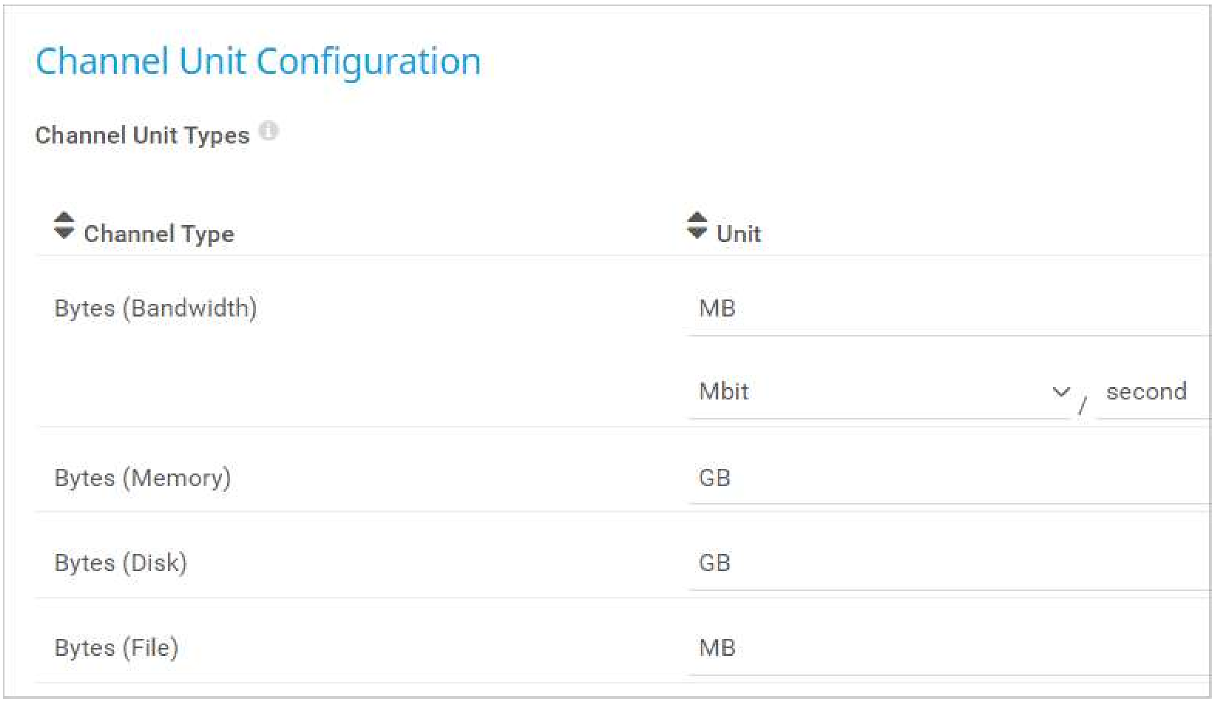
User Group	Rights
PRTG Users Group	Full access

□ Revert children's access rights to inherited

Access Rights

Setting	Description
User Group Access	Select the user groups 3346 that have access to the object. You see a table with user groups and group access rights. The table contains all user groups in your setup. For each user group, you can choose from the following group access rights: ▪ Inherited: Inherit the access rights settings of the parent object. ▪ No access: Users in this user group cannot see or edit the object. The object neither shows up in lists nor in the device tree. ⓘ There is one exception: If a user in this user group has access to a child object, the parent object is visible in the device tree but users in this user group cannot access it. ▪ Read access: Users in this group can see the object and view its monitoring results. They cannot edit any settings. ▪ Write access: Users in this group can see the object, view its monitoring results, and edit its settings. They cannot edit its access rights settings. ▪ Full access: Users in this group can see the object, view its monitoring results, edit its settings, and edit its access rights settings. To automatically set all child objects to inherit this object's access rights, enable the Revert access rights of child objects to "inherited" option. For more details on access rights, see section Access Rights Management 144.

Channel Unit Configuration



Channel Unit Configuration

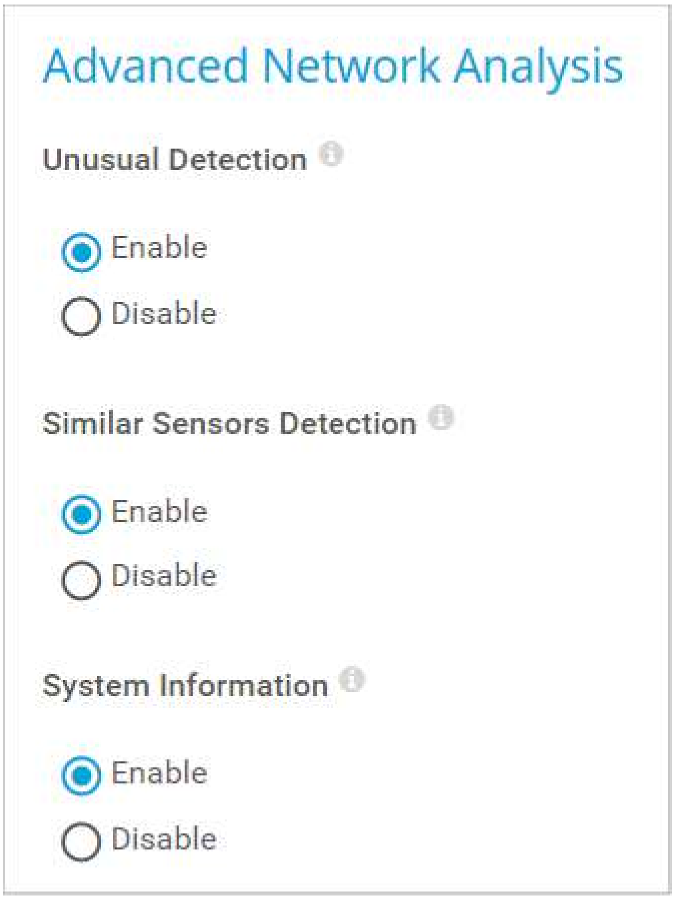
Channel Unit Types

Channel Type	Unit
Bytes (Bandwidth)	MB Mbit / second
Bytes (Memory)	GB
Bytes (Disk)	GB
Bytes (File)	MB

Channel Unit Configuration

Setting	Description
Channel Unit Types	For each type of channel, select the unit in which PRTG displays the data. If you define this setting on probe, group, or device level, you can inherit these settings to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom ⓘ Custom channel types are only available on sensor level. ⓘ Which channel units are available depends on the sensor type and the available parameters. If no configurable channels are available, this field shows No configurable channels.

Advanced Network Analysis



Advanced Network Analysis

Unusual Detection

● Enable
○ Disable

Similar Sensors Detection

● Enable
○ Disable

System Information

● Enable
○ Disable

Advanced Network Analysis

Setting	Description
Unusual Detection	Select if you want to use the unusual detection 3309 for sensors: ▪ Enabled: Activates the unusual detection for this object and, by default, for all objects underneath in the object hierarchy 131. Sensors that are affected by this setting show the Unusual status if PRTG detects unusual activity. ▪ Disabled: Does not activate the unusual detection. PRTG ignores unusual values for sensors that are affected by this setting. These sensors do not show the Unusual status. ⓘ You can configure the behavior of the unusual detection or completely disable it in the system settings 3309.
Similar Sensors Detection	Select if you want to activate the similar sensors 189 analysis: ▪ Enabled: Activates the similar sensors detection for this object and, by default, for all objects underneath in the object hierarchy. PRTG considers all sensors that are affected by this setting during the similarity analysis. ▪ Disabled: Does not activate the similar sensors detection. PRTG does not consider sensors that are affected by this setting during the similarity analysis. ⓘ You can configure the depth of the analysis of the similar sensors detection or completely disable it in the system settings 3311.
System Information	Select if you want to retrieve and show system information 202 for your devices: ▪ Enabled: Activates the system information feature for this object and, by default, for all objects underneath in the hierarchy. ▪ Disabled: Does not activate the system information feature. ⓘ The System Information feature is enabled by default. To retrieve the data, PRTG automatically uses the credentials for Windows systems 596 and the credentials for SNMP devices 603 that you entered in the device settings or that the device inherits 131 from a parent object like the root group. Consider this when you monitor devices that are outside of your local network, especially when you use SNMP v1 or SNMP v2c, which do not provide encryption. ☁ This setting is not available on the hosted probe of a PRTG Hosted Monitor instance.

ⓘ Save your settings. If you change tabs or use the main menu without saving, all changes to the settings are lost.

More

■ KNOWLEDGE BASE

What security features does PRTG include?

- https://kb.paessler.com/en/topic/61108

How do I set permissions for the Amazon Web Services (AWS) API key to use certain sensors in PRTG?

- https://kb.paessler.com/en/topic/38083

What is the Overflow Values setting in the SNMP Compatibility Options?

- https://kb.paessler.com/en/topic/43503

How can I change the defaults for names automatically generated for new SNMP sensors?

- https://kb.paessler.com/en/topic/7363

Automatically update port name and number for SNMP Traffic sensors when the device changes them

- https://kb.paessler.com/en/topic/25893

7.5 Probe Settings

The following settings are available on the Settings tab of a probe.

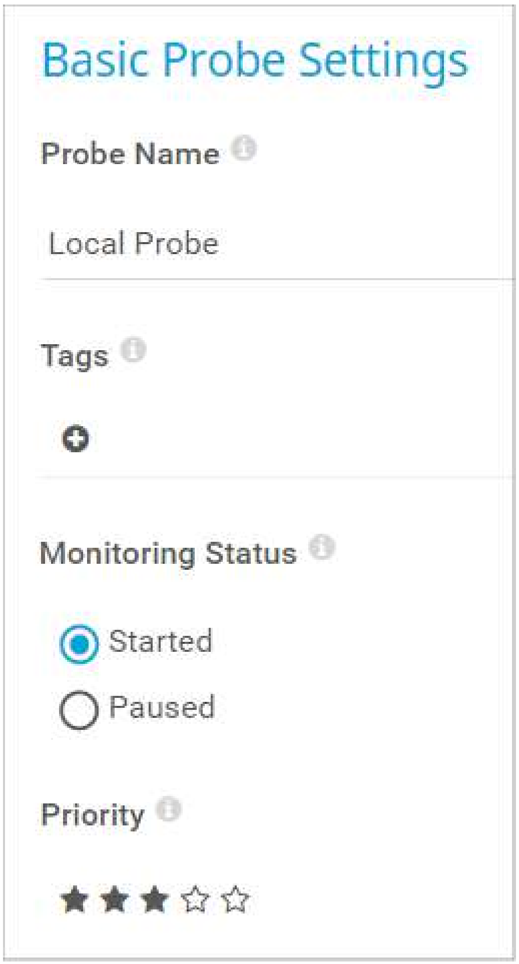
ⓘ We recommend that you define as many settings as possible in the root group settings 419 so that you can inherit them to all other objects in the object hierarchy 131.

ⓘ This documentation refers to an administrator that accesses the PRTG web interface on a master node. Other user accounts, interfaces, or failover nodes might not have all of the options in the way described here. In a cluster, note that failover nodes are read-only by default.

In this section:

- Scanning Interval 507
- Schedules, Dependencies, and Maintenance Window 509
- Access Rights 511
- Channel Unit Configuration 512
- Advanced Network Analysis 514
- Administrative Probe Settings 515
- Scheduled Restart Settings 517

Basic Probe Settings



Basic Probe Settings

Probe Name

Local Probe

Tags

Monitoring Status

● Started
○ Paused

Priority

★★★☆☆

Basic Probe Settings

Setting	Description
Probe Name	Enter a name to identify the probe. By default, PRTG shows this name in the device tree 164, as well as in alarms 199, logs 208, notifications 3173, reports 3192, maps 3214, libraries 3176, and tickets 211.

Setting	Description
	ⓘ If the name contains angle brackets (<>), PRTG replaces them with braces ({}) for security reasons. For more information, see the Knowledge Base: What security features does PRTG include?
Tags	Enter one or more tags. Confirm each tag with the Spacebar key, a comma, or the 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 137. ⓘ It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with parentheses (()) or angle brackets (<>). ⓘ For performance reasons, it can take some minutes until you can filter for new tags that you added.
Monitoring Status	Select the monitoring status of the probe: ▪ Started: Monitor the probe. ▪ Paused: Pause monitoring for the probe. All sensors on all devices on the probe are in the Paused status 224 until you change this setting.
Priority	Select a priority 221 for the probe. This setting determines the position of the probe in lists. The highest priority is at the top of a list. You can choose from the lowest priority (★☆☆☆☆) to the highest priority (★★★★★).

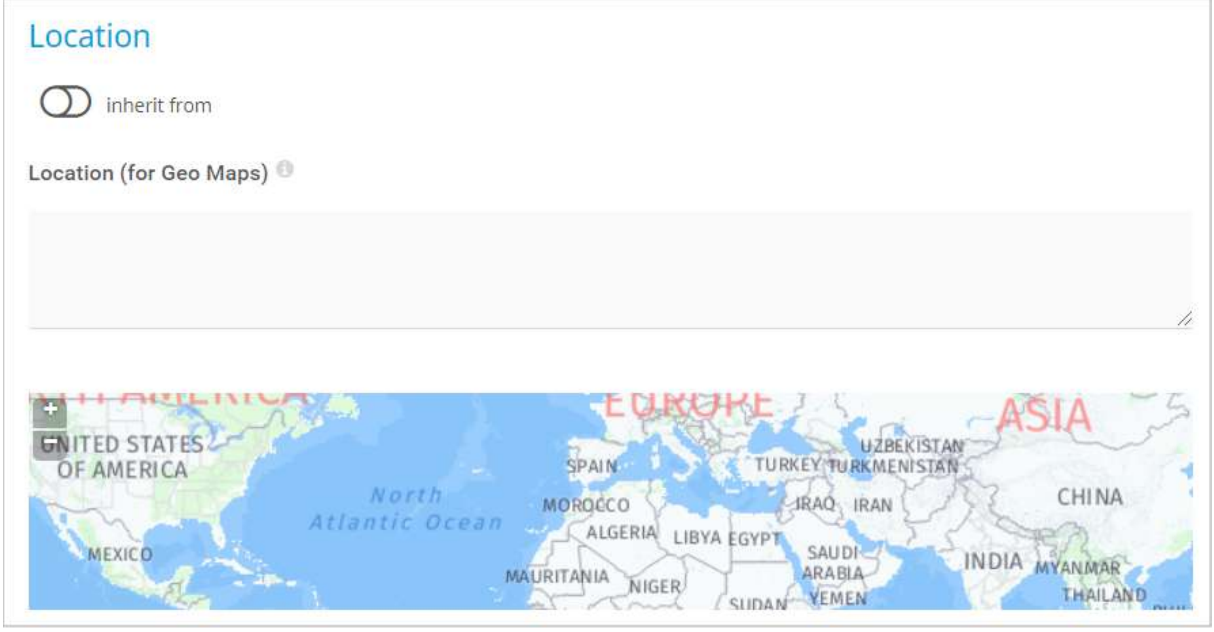
Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the root group settings 419 if necessary. To change a setting for this object only, click ◉ under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section Inheritance of Settings 135.

Location

Click ◉ to interrupt the inheritance 135.



Location

○ inherit from

Location (for Geo Maps)

Location

Setting	Description
Location (for Geo Maps)	If you want to use Geo Maps 3169, enter a location in the first line. Geographical maps then display objects like devices or groups with a status icon using a color code similar to the sensor status icons 179 (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, as PRTG automatically parses latitude and longitude, for example, enter 49.452778 11.077778, or enter 49.452778 any 11.077778 text. A minus sign (-) in the first line hides an object from a geographical map. 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 the coordinates in the second line. This geographical marker then shows the object with the label in the geographical map. ⓘ The preview map always has a road map layout regardless of the map layout you set in User Interface 3297.

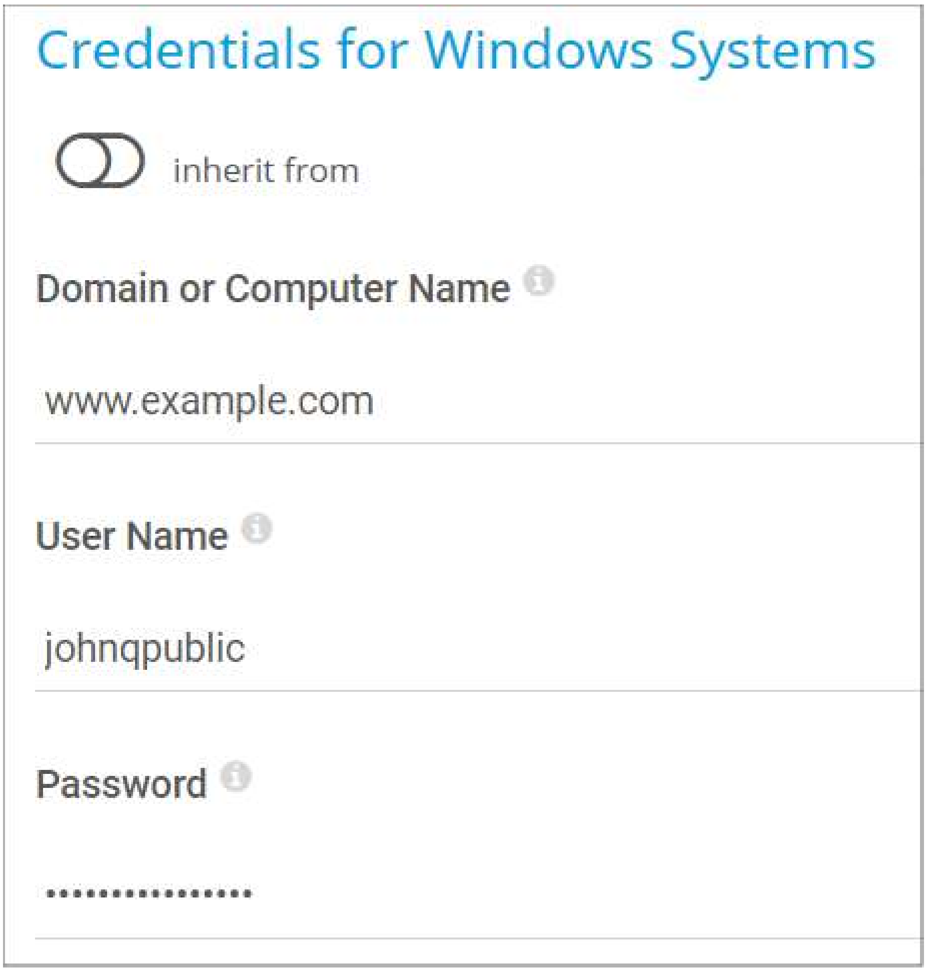
Credentials for Windows Systems

Click ● to interrupt the inheritance 135.

ⓘ The settings you define in this section apply to the following sensors:

▪ Active Directory Replication Errors	▪ Windows IIS 6.0 SMTP Sent	▪ WMI Memory

- Event Log (Windows API)
- Exchange Backup (PowerShell)
- Exchange Database (PowerShell)
- Exchange Database DAG (PowerShell)
- Exchange Mail Queue (PowerShell)
- Exchange Mailbox (PowerShell)
- Exchange Public Folder (PowerShell)
- File
- File Content
- Folder
- Hyper-V Cluster Shared Volume Disk Free
- Hyper-V Host Server
- Hyper-V Virtual Machine
- Hyper-V Virtual Network Adapter
- Hyper-V Virtual Storage Device
- PerfCounter Custom
- PerfCounter IIS Application Pool
- Share Disk Free
- Windows CPU Load
- Windows IIS 6.0 SMTP Received
- Windows IIS Application
- Windows MSMQ Queue Length
- Windows Network Card
- Windows Pagefile
- Windows Physical Disk I/O
- Windows Print Queue
- Windows Process
- Windows System Uptime
- Windows Updates Status (PowerShell)
- WMI Battery
- WMI Custom
- WMI Custom String
- WMI Disk Health
- WMI Event Log
- WMI Exchange Server
- WMI Exchange Transport Queue
- WMI File
- WMI Free Disk Space (Multi Disk)
- WMI HDD Health
- WMI Logical Disk I/O
- WMI Microsoft SQL Server 2005 (Deprecated)
- WMI Microsoft SQL Server 2008
- WMI Microsoft SQL Server 2012
- WMI Microsoft SQL Server 2014
- WMI Microsoft SQL Server 2016
- WMI Microsoft SQL Server 2017
- WMI Microsoft SQL Server 2019
- WMI Remote Ping
- WMI Security Center
- WMI Service
- WMI Share
- WMI SharePoint Process
- WMI Storage Pool
- WMI Terminal Services (Windows 2008+)
- WMI Terminal Services (Windows XP/Vista/2003)
- WMI UTC Time
- WMI Vital System Data v2
- WMI Volume
- WSUS Statistics



Credentials for Windows Systems

○ inherit from

Domain or Computer Name

www.example.com

User Name

johnqpublic

Password

•••••••••••••••

Credentials for Window s Systems

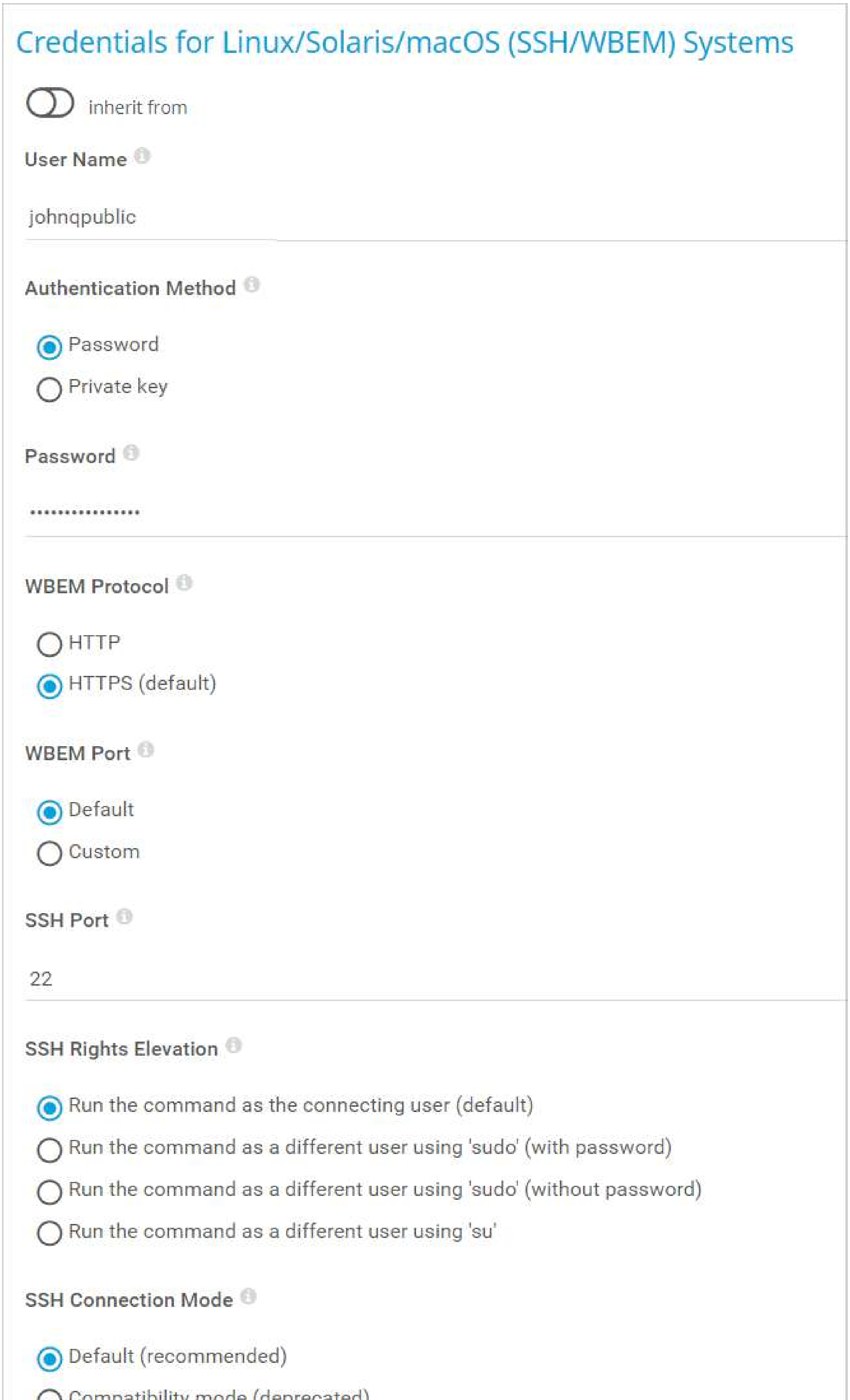
Setting	Description
Domain or Computer Name	Enter the domain or computer name of the user account with which you want to access the Windows system. PRTG uses this account for Windows Management Instrumentation (WMI) sensors and other Windows sensors. If you want to use a Windows local user account on the target device, enter the computer name. If you want to use a Windows domain user account (recommended), enter the domain name. PRTG automatically adds a prefix to use the NT LAN Manager (NTLM) protocol if you do not explicitly define it. Do not leave this field empty.
User Name	Enter the user name for access to the Windows system. Usually, you use credentials with administrator rights.
Password	Enter the password for access to the Windows system. Usually, you use credentials with administrator rights.

Credentials for Linux/Solaris/macOS (SSH/WBEM) Systems

Click ✓ to interrupt the inheritance 135.

ⓘ The settings you define in this section apply to the following sensors:

- SFTP Secure File Transfer Protocol
- SSH Disk Free
- SSH INodes Free
- SSH Load Average
- SSH Meminfo
- SSH Remote Ping
- SSH SAN Enclosure
- SSH SAN Logical Disk
- SSH SAN Physical Disk
- SSH SAN System Health
- SSH Script
- SSH Script Advanced
- VMware Host Hardware (WBEM)



Credentials for Linux/Solaris/macOS (SSH/WBEM) Systems

○ inherit from

User Name

johnqpublic

Authentication Method

- ● Password
- ○ Private key

Password

•••••••••••••••

WBEM Protocol

- ○ HTTP
- ● HTTPS (default)

WBEM Port

- ● Default
- ○ Custom

SSH Port

22

SSH Rights Elevation

- ● Run the command as the connecting user (default)
- ○ Run the command as a different user using 'sudo' (with password)
- ○ Run the command as a different user using 'sudo' (without password)
- ○ Run the command as a different user using 'su'

SSH Connection Mode

- ● Default (recommended)
- ○ Compatibility mode (deprecated)

Setting	Description
User Name	Enter the user name for access to the Linux/Solaris/macOS system via Secure Shell (SSH) and Web-based Enterprise Management (WBEM). Usually, you use credentials with administrator rights.
Authentication Method	Select the authentication method for the login: ▪ Password: Provide the password for the login. ▪ Private key: Provide an RSA private key for authentication. ⓘ PRTG can only handle keys in the OpenSSH format that are not encrypted. You cannot use password-protected keys. ⓘ PRTG only supports RSA keys. It does not support DSA keys. 🟦 For details, see section Monitoring via SSH 3437.
Password	This setting is only visible if you select Password above. Enter a password for access to the Linux/Solaris/macOS system via SSH and WBEM. Usually, you use credentials with administrator rights.
Private Key	This setting is only visible if you select Private key above. Paste the entire RSA private key, including the BEGIN and END lines. Make sure that a corresponding public key exists on the target device. ⓘ PRTG can only handle keys in the OpenSSH format that are not encrypted. You cannot use password-protected keys. ⓘ PRTG only supports RSA keys. It does not support DSA keys. 🟦 For details, see section Monitoring via SSH 3437. ⓘ If you do not insert a private key for the first time but if you want to change the private key, you need to restart the PRTG core server service 3352 for the private key change to take effect.
WBEM Protocol	Select the protocol that you want to use for the connection to the system via WBEM: ▪ HTTP: Use an unsecure connection for WBEM. ▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection for WBEM. ⓘ This setting is only relevant if you use WBEM sensors.
WBEM Port	Select if you want to use one of the default ports for the connection to the system via WBEM or if you want to set a custom port: ▪ Default: Use one of the default ports. The default port for unsecure connections is 5988 and the default port for secure connections is 5989. ▪ Custom: Use a custom port.

Setting	Description
	ⓘ This setting is only relevant if you use WBEM sensors.
Custom WBEM Port	This setting is only visible if you select Custom above. Enter a custom WBEM port. Enter an integer.
SSH Port	Enter the port for SSH connections. Enter an integer. The default port is 22. ⓘ By default, PRTG automatically uses this setting for all SSH sensors 3683 unless you define a different port number in the sensor settings.
SSH Rights Elevation	Select the rights that you want to use to run the command on the target system: ▪ Run the command as the connecting user (default): Use the rights of the user who establishes the SSH connection. ▪ Run the command as a different user using 'sudo' (with password): Use the rights of a different user with a password required for sudo to run commands on the target system, for example, as a root user. ▪ Run the command as a different user using 'sudo' (without password): Use the rights of a different user without a password required for sudo to run commands on the target system, for example, as a root user. ▪ Run the command as a different user using 'su': Use the rights of a different user with su to run commands on the target system.
Target System User Name	This setting is only visible if you select an option that includes sudo or su above. Enter a user name to run the specified command on the target system as a different user than the root user. If you leave this field empty, you run the command as a root user. Make sure that you set the Linux password even if you use a public key or a private key for authentication. This is not necessary if the user is allowed to run the command without a password.
Password	This setting is only visible if you select an option that includes sudo or su with password above. Enter the password to run the sudo command or the su command.
SSH Connection Mode	Select the connection mode that you want to use to access data with SSH sensors 3437: ▪ Default (recommended): This is the default connection mode for SSH sensors. It provides the best performance and security. ▪ Compatibility mode (deprecated): Use this only if the default connection mode does not work on the target system. The compatibility mode is the connection mode that PRTG used in previous versions and it is deprecated.

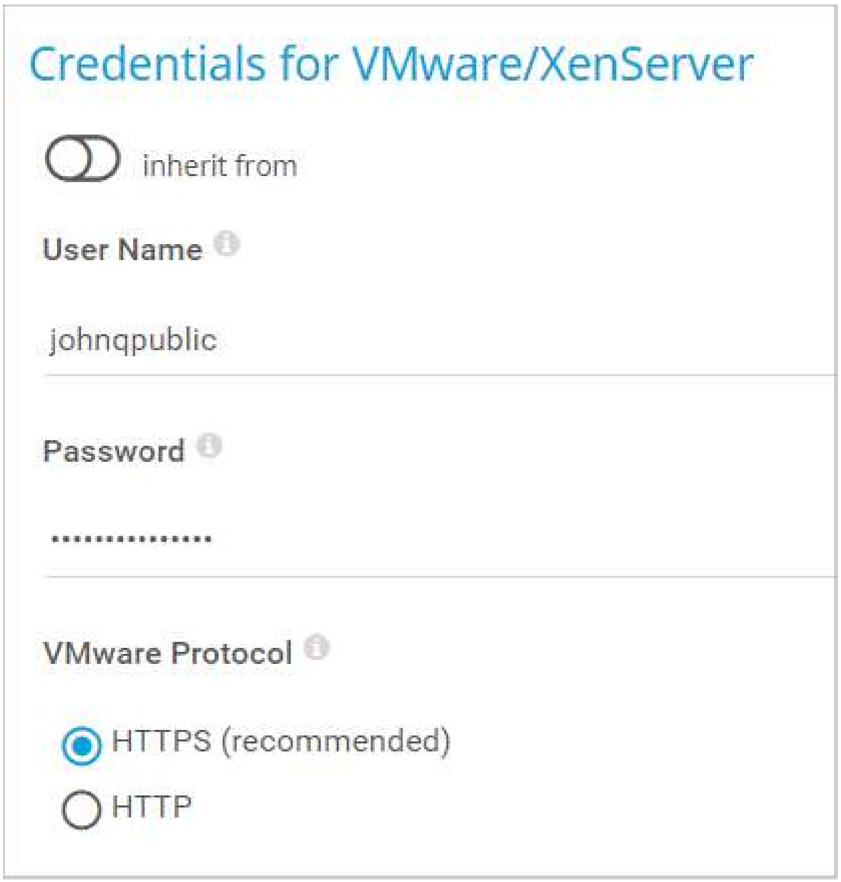
Setting	Description
	ⓘ We strongly recommend that you use the default connection mode. ⓘ You can also individually select the connection mode for each SSH sensor in the sensor settings.

Credentials for VMware/XenServer

Click ● to interrupt the inheritance 135.

ⓘ The settings you define in this section apply to the following sensors:

- Citrix XenServer Host
- Citrix XenServer Virtual Machine
- VMware Datastore (SOAP)
- VMware Host Hardware (WBEM)
- VMware Host Hardware Status (SOAP)
- VMware Host Performance (SOAP)
- VMware Virtual Machine (SOAP)



Credentials for VMware/XenServer

○ inherit from

User Name: johnqpublic

Password: •••••••••••••••

VMware Protocol

● HTTPS (recommended)

○ HTTP

Credentials for VMw are/XenServer

Setting	Description
User Name	Enter the user name for access to VMware ESXi, vCenter Server, or Citrix XenServer. Usually, you use credentials with administrator rights.
Password	Enter the password for access to VMware ESXi, vCenter Server, or Citrix XenServer. Usually, you use credentials with administrator rights. ⓘ Single sign-on (SSO) passwords for vSphere do not support special characters. For details, see the VMware sensors sections.
VMware Protocol	Select the protocol for the connection to VMware ESXi, vCenter Server, or Citrix XenServer: ▪ HTTPS (recommended): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection. ▪ HTTP: Use an unsecure connection.
Session Handling	Select if you want to reuse a session for VMware sensors: ▪ Reuse a session for multiple scans (recommended): Select this option if you want a VMware sensor to reuse a single session for multiple sensor scans to query data. With this option, the sensor does not need to log in and out for each sensor scan. We recommend that you use this option because it reduces network load and log entries on the target device. This can increase performance. ▪ Create a new session for each scan: If you select this option, PRTG does not reuse a session and a VMware sensor has to log in and out for each sensor scan. This can decrease performance.

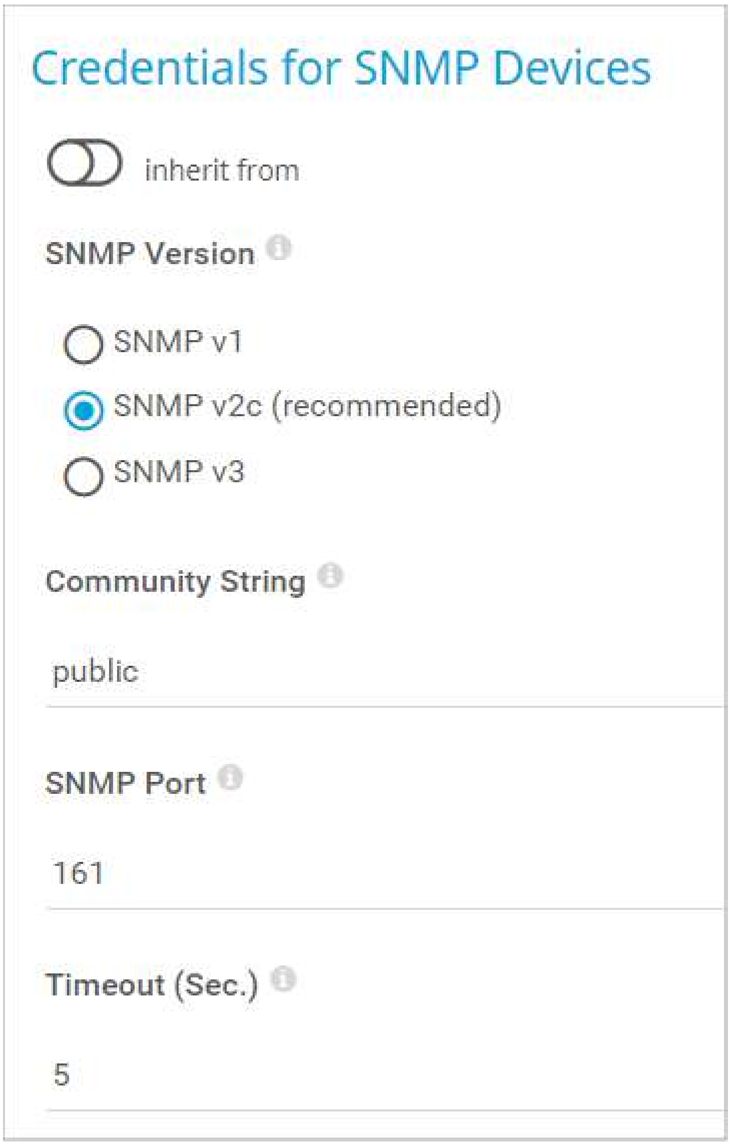
Credentials for SNMP Devices

Click ☑ to interrupt the inheritance 135.

ⓘ The settings you define in this section apply to the following sensors:

- Cisco IP SLA
- SNMP APC Hardware
- SNMP Buffalo TS System Health
- SNMP Cisco ADSL
- SNMP Cisco ASA VPN Connections
- SNMP Cisco ASA VPN Traffic
- SNMP Fujitsu System Health v2
- SNMP Hardware Status
- SNMP HP LaserJet Hardware
- SNMP HPE BladeSystem Blade
- SNMP HPE BladeSystem Enclosure System Health
- SNMP HPE ProLiant Logical Disk
- SNMP NetApp Enclosure
- SNMP NetApp I/O
- SNMP NetApp License
- SNMP NetApp Logical Unit
- SNMP NetApp Network Interface
- SNMP NetApp System Health
- SNMP Nutanix Cluster Health

- SNMP Cisco ASA VPN Users
- SNMP Cisco CBQoS
- SNMP Cisco System Health
- SNMP Cisco UCS Blade
- SNMP Cisco UCS Chassis
- SNMP Cisco UCS Physical Disk
- SNMP Cisco UCS System Health
- SNMP CPU Load
- SNMP Custom
- SNMP Custom Advanced
- SNMP Custom String
- SNMP Custom String Lookup
- SNMP Custom Table
- SNMP Dell EqualLogic Logical Disk
- SNMP Dell EqualLogic Member Health
- SNMP Dell EqualLogic Physical Disk
- SNMP Dell Hardware
- SNMP Dell PowerEdge Physical Disk
- SNMP Dell PowerEdge System Health
- SNMP Disk Free
- SNMP HPE ProLiant Memory Controller
- SNMP HPE ProLiant Network Interface
- SNMP HPE ProLiant Physical Disk
- SNMP HPE ProLiant System Health
- SNMP IBM System X Logical Disk
- SNMP IBM System X Physical Disk
- SNMP IBM System X Physical Memory
- SNMP IBM System X System Health
- SNMP interSeptor Pro Environment
- SNMP Juniper NS System Health
- SNMP LenovoEMC Physical Disk
- SNMP LenovoEMC System Health
- SNMP Library
- SNMP Linux Disk Free
- SNMP Linux Load Average
- SNMP Linux Meminfo
- SNMP Linux Physical Disk
- SNMP Memory
- SNMP NetApp Disk Free
- SNMP Nutanix Hypervisor
- SNMP Poseidon Environment
- SNMP Printer
- SNMP QNAP Logical Disk
- SNMP QNAP Physical Disk
- SNMP QNAP System Health
- SNMP Rittal CMC III Hardware Status
- SNMP RMON
- SNMP SonicWall System Health
- SNMP SonicWall VPN Traffic
- SNMP Synology Logical Disk
- SNMP Synology Physical Disk
- SNMP Synology System Health
- SNMP System Uptime
- SNMP Traffic
- SNMP Trap Receiver
- SNMP Windows Service



Credentials for SNMP Devices

inherit from

SNMP Version

○ SNMP v1

● SNMP v2c (recommended)

○ SNMP v3

Community String

public

SNMP Port

161

Timeout (Sec.)

5

Credentials for SNMP Devices

Setting	Description
SNMP Version	Select the Simple Network Management Protocol (SNMP) version for the connection to the target SNMP device: ▪ SNMP v1: Use SNMP v1 for the connection. SNMP v1 only offers clear-text data transmission. ⓘ SNMP v1 does not support 64-bit counters. This might result in invalid data when you monitor traffic via SNMP. ▪ SNMP v2c (recommended): Use SNMP v2c for the connection. SNMP v2c also only offers clear-text data transmission but it supports 64-bit counters.

Setting	Description
	- SNMP v3: Use SNMP v3 for the connection. SNMP v3 provides secure authentication and data encryption. ⓘ SNMP v3 has performance limitations because of the use of encryption. The main limiting factor is CPU power. Also keep in mind that SNMP v3, unlike SNMP v1 and v2c, does not scale with more CPU power. Because of this limitation, PRTG can only handle a limited number of requests per second so that you can use only a limited number of sensors using SNMP v3. If you see an increase in Interval Delay or Open Requests with the Probe Health sensor, distribute the load over multiple probes 3621. SNMP v1 and SNMP v2c do not have this limitation.
Community String	This setting is only visible if you select SNMP v1 or SNMP v2c (recommended) above. Enter the community string of your device. This is like a clear-text password for simple authentication. ⓘ We recommend that you use the default value.
Authentication Method	This setting is only visible if you select SNMP v3 above. Select the authentication method: - MD5: Use message-digest algorithm 5 (MD5) for authentication. - SHA: Use Secure Hash Algorithm (SHA) for authentication. - SHA-224: Use SHA-224 for authentication. - SHA-256: Use SHA-256 for authentication. - SHA-384: Use SHA-384 for authentication. - SHA-512: Use SHA-512 for authentication. ⓘ If you do not want to use authentication but you need SNMP v3, for example, because your device requires context, you can leave the Password field empty. In this case, PRTG uses SNMP_SEC_LEVEL_NOAUTH and it entirely deactivates authentication. ⓘ The authentication method you select must match the authentication method of your device.
User Name	This setting is only visible if you select SNMP v3 above. Enter the user name for access to the target SNMP device. ⓘ The user name that you enter must match the user name of your device.
Password	This setting is only visible if you select SNMP v3 above. Enter the password for access to the target SNMP device. ⓘ The password that you enter must match the password of your device.

Setting	Description
Encryption Type	This setting is only visible if you select SNMP v3 above. Select an encryption type: ▪ DES: Use Data Encryption Standard (DES) as the encryption algorithm. ▪ AES: Use Advanced Encryption Standard (AES) as the encryption algorithm. ▪ AES-192: Use AES-192 as the encryption algorithm. ▪ AES-256: Use AES-256 as the encryption algorithm. ⓘ The encryption type that you select must match the encryption type of your device.
Encryption Key	This setting is only visible if you select SNMP v3 above. Enter an encryption key. If you provide a key, PRTG encrypts SNMP data packets with the encryption algorithm that you selected above. Enter a string or leave the field empty. ⓘ The encryption key that you enter must match the encryption key of your device. If the encryption keys do not match, you do not get an error message.
Context Name	This setting is only visible if you select SNMP v3 above. Enter a context name only if the configuration of the device requires it. Context is a collection of management information that is accessible by an SNMP device. Enter a string.
SNMP Port	Enter the port for the connection to the SNMP target device. Enter an integer. The default port is 161. ⓘ We recommend that you use the default value.
Timeout (Sec.)	Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is 300 seconds (5 minutes).

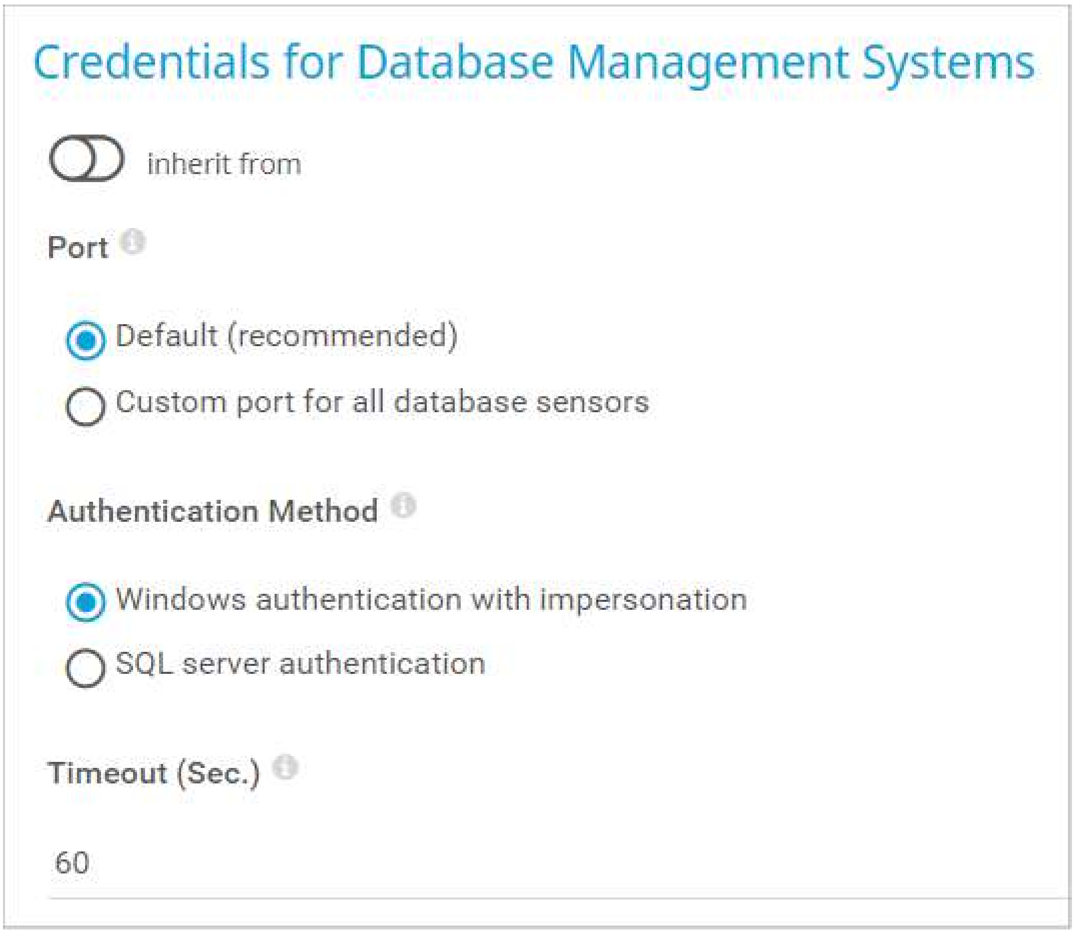
Credentials for Database Management Systems

Click ☑ to interrupt the inheritance 135.

ⓘ The settings you define in this section apply to the following sensors:

- ADO SQL v2
- Microsoft SQL v2
- MySQL v2
- Oracle SQL v2

- PostgreSQL



Credentials for Database Management Systems

○ inherit from

Port

● Default (recommended)

○ Custom port for all database sensors

Authentication Method

● Windows authentication with impersonation

○ SQL server authentication

Timeout (Sec.)

60

Credentials for Database Management Systems

Setting	Description
Port	Select the port that PRTG uses for connections to the monitored databases: - Default (recommended): PRTG automatically determines the type of the database and uses the corresponding default port to connect. PRTG uses the following default ports: - Microsoft SQL: 1433 - MySQL: 3306 - Oracle SQL: 1521 - PostgreSQL: 5432 - Custom port for all database sensors: Select this option if your database management systems do not use the default ports. Enter a custom port for database connections below. ⓘ PRTG uses this custom port for all database sensors and for connections to all your databases.

Setting	Description
Custom Port	Enter a custom port for database connections. Enter an integer. ⓘ PRTG uses this custom port for all database sensors and for connections to all your databases.
Authentication Method	Select the authentication method for the connection to the Structured Query Language (SQL) database: ▪ Windows authentication with impersonation: PRTG uses the Windows credentials that you define in settings that are higher in the object hierarchy 131, for example, in the settings of the parent device; for the database connection. ⓘ The user whose credentials PRTG uses needs to have permission to log in to the probe system with a database sensor. This is necessary for the impersonation. ▪ SQL server authentication: Use explicit credentials for database connections. Enter a user name and password below.
User Name	This setting is only visible if you select SQL server authentication above. Enter the user name for the database connection.
Password	This setting 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. Enter an integer. The maximum timeout value is 300 seconds (5 minutes).

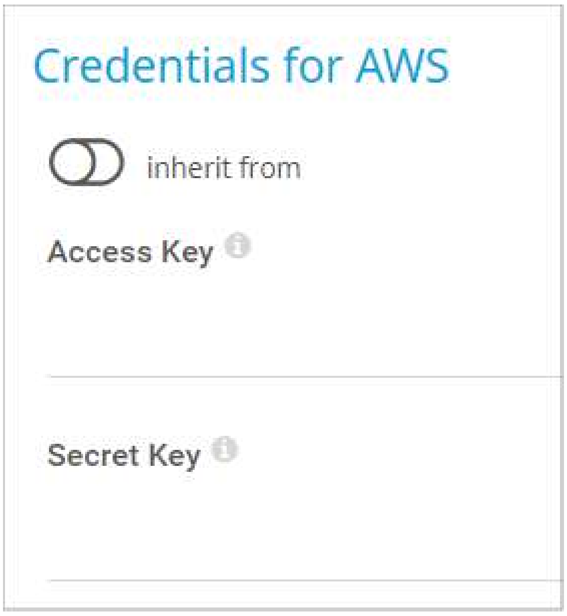
Credentials for AWS

Click ◉ to interrupt the inheritance 135.

ⓘ The settings you define in this section apply to the following sensors:

- AWS Alarm v2
- AWS Cost
- AWS EBS v2
- AWS EC2 v2
- AWS ELB v2
- AWS RDS v2

■ For more information about the permissions that are necessary to query the AWS API, see the Knowledge Base: How do I set permissions for the Amazon Web Services (AWS) API key to use certain sensors in PRTG?



Credentials for AWS

inherit from

Access Key

Secret Key

Credentials for AWS

Setting	Description
Access Key	Enter the Amazon Web Services (AWS) access key.
Secret Key	Enter the AWS secret key.

Credentials for Microsoft 365

Click ✓ to interrupt the inheritance 135.

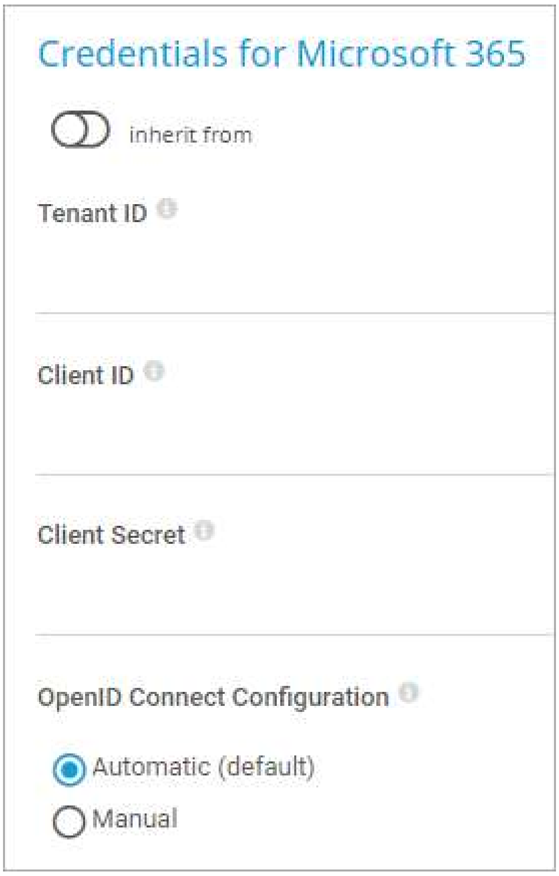
ⓘ The settings you define in this section apply to the following sensors:

- Microsoft 365 Mailbox
- Microsoft 365 Service Status
- Microsoft 365 Service Status Advanced

The sensors use the credentials to authenticate with Azure Active Directory (Azure AD).

For more information about the credentials and the permissions that are necessary to use the Microsoft 365 Service Status sensor and the Microsoft 365 Service Status Advanced sensor, see the Knowledge Base: How do I obtain credentials and set permissions for the Microsoft 365 Service Status sensors?

For more information about the credentials and the permissions that are necessary to use the Microsoft 365 Mailbox sensor, see the Knowledge Base: How do I obtain credentials and set permissions for the Microsoft 365 Mailbox sensor?



Credentials for Microsoft 365

○ inherit from

Tenant ID

Client ID

Client Secret

OpenID Connect Configuration

● Automatic (default)

○ Manual

Credentials for Microsoft 365

Setting	Description
Tenant ID	Enter the Azure AD tenant ID. ⓘ A tenant ID must be a 32-digit sequence in hexadecimal notation.
Client ID	Enter the Azure AD client ID.
Client Secret	Enter the Azure AD client secret.
OpenID Connect Configuration	Select if you want to manually enter the authorization endpoint URL and token endpoint URL that PRTG uses to access Microsoft Graph. Choose between: ▪ Automatic (default): PRTG automatically determines the authorization endpoint URL and the token endpoint URL. ▪ Manual: Manually enter the authorization endpoint URL and the token endpoint URL.
Authorization Endpoint	Enter the authorization endpoint URL including the server. Authorization endpoint URL example:

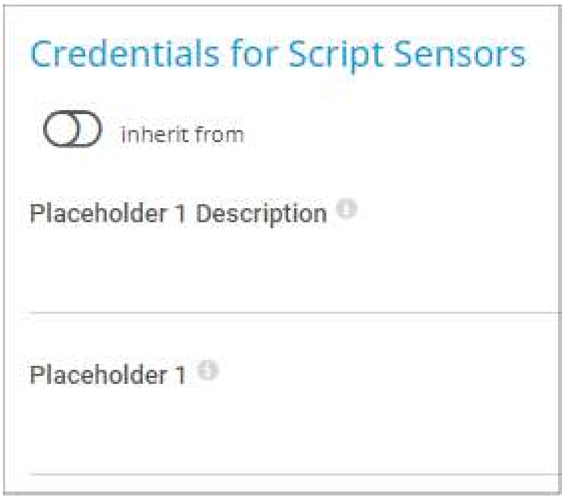
Setting	Description
	`https://login.microsoftonline.com/<tenant-ID>/oauth2/v2.0/authorize` ⓘ Make sure to replace <tenant-ID> with the directory (tenant) ID from Azure AD.
Token Endpoint	Enter the token endpoint URL including the server. Token endpoint URL example: `https://login.microsoftonline.com/<tenant-ID>/oauth2/v2.0/token` ⓘ Make sure to replace <tenant-ID> with the directory (tenant) ID from Azure AD.

Credentials for Script Sensors

Click ✓ to interrupt the inheritance 135.

ⓘ The settings you define in this section apply to the following sensors:

- EXE/Script
- EXE/Script Advanced
- Python Script Advanced
- SSH Script
- SSH Script Advanced


Credentials for Script Sensors

○ inherit from

Placeholder 1 Description

Placeholder 1

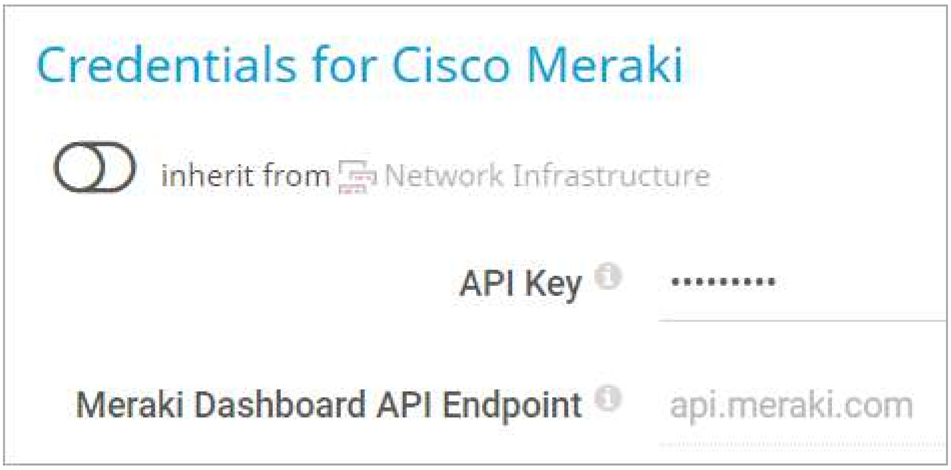
Credentials for Script Sensors

Setting	Description
Placeholder 1 Description	Enter a description for Placeholder 1, for example information about the purpose or content of the placeholder.
Placeholder 1	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add %scriptplaceholder1 in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 2 Description	Enter a description for Placeholder 2, for example information about the purpose or content of the placeholder.
Placeholder 2	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add %scriptplaceholder2 in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 3 Description	Enter a description for Placeholder 3, for example information about the purpose or content of the placeholder.
Placeholder 3	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add %scriptplaceholder3 in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 4 Description	Enter a description for Placeholder 4, for example information about the purpose or content of the placeholder.
Placeholder 4	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add %scriptplaceholder4 in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 5 Description	Enter a description for Placeholder 5, for example information about the purpose or content of the placeholder.
Placeholder 5	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add %scriptplaceholder5 in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.

Credentials for Cisco Meraki

ⓘ The settings you define in this section apply to the following sensors:

- Cisco Meraki License
- Cisco Meraki Network Health



Credentials for Cisco Meraki

inherit from Network Infrastructure

API Key ••••••••••

Meraki Dashboard API Endpoint api.meraki.com

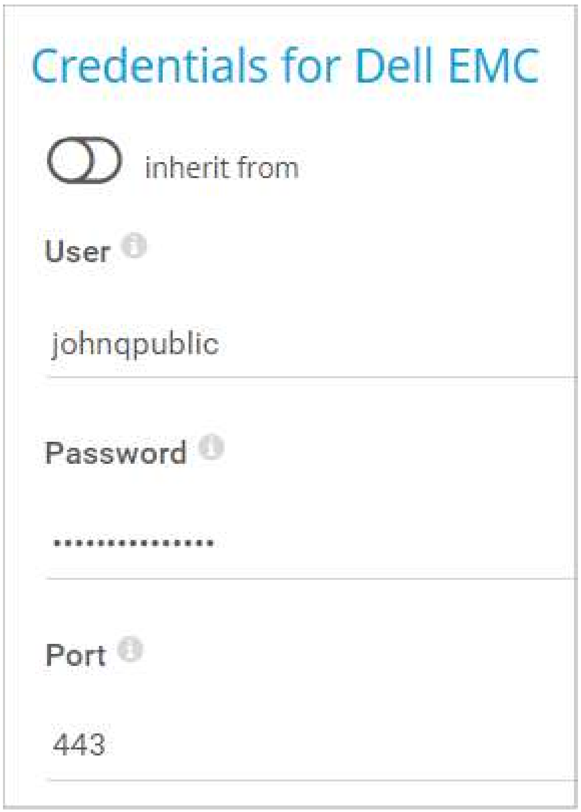
Credentials for Cisco Meraki

Setting	Description
API Key	Enter an API key that the sensor uses for authentication against the Cisco Meraki Dashboard API.
Meraki Dashboard API Endpoint	Enter the endpoint for the Cisco Meraki Dashboard API. The default api.meraki.com should be valid for most use cases. ⓘ See the Cisco Meraki Dashboard API documentation for other possible choices.

Credentials for Dell EMC

ⓘ The settings you define in this section apply to the following sensors:

- Dell EMC Unity Enclosure Health v2
- Dell EMC Unity File System v2
- Dell EMC Unity Storage Capacity v2
- Dell EMC Unity Storage LUN v2
- Dell EMC Unity Storage Pool v2
- Dell EMC Unity VMware Datastore v2



Credentials for Dell EMC

inherit from

User

johnqpublic

Password

•••••••••••••••

Port

443

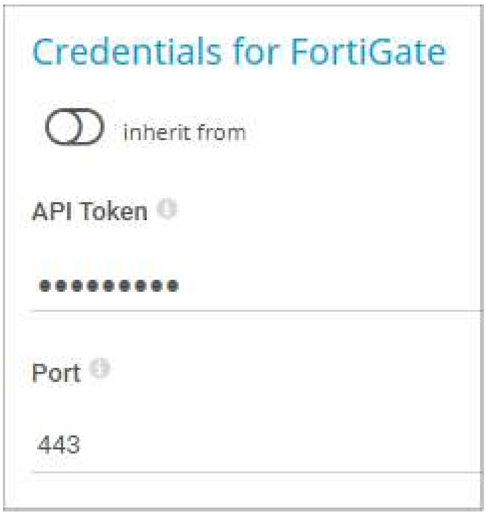
Credentials for Dell EMC

Setting	Description
User Name	Enter the user name for access to the Dell EMC system.
Password	Enter the password for access to the Dell EMC system.
Port	Enter the port for the connection to the Dell EMC system. The default port for secure connections is 443.

Credentials for FortiGate

ⓘ The settings you define in this section apply to the following sensors:

- FortiGate System Statistics
- FortiGate VPN Overview



Credentials for FortiGate

○ inherit from

API Token

●●●●●●●●●

Port

443

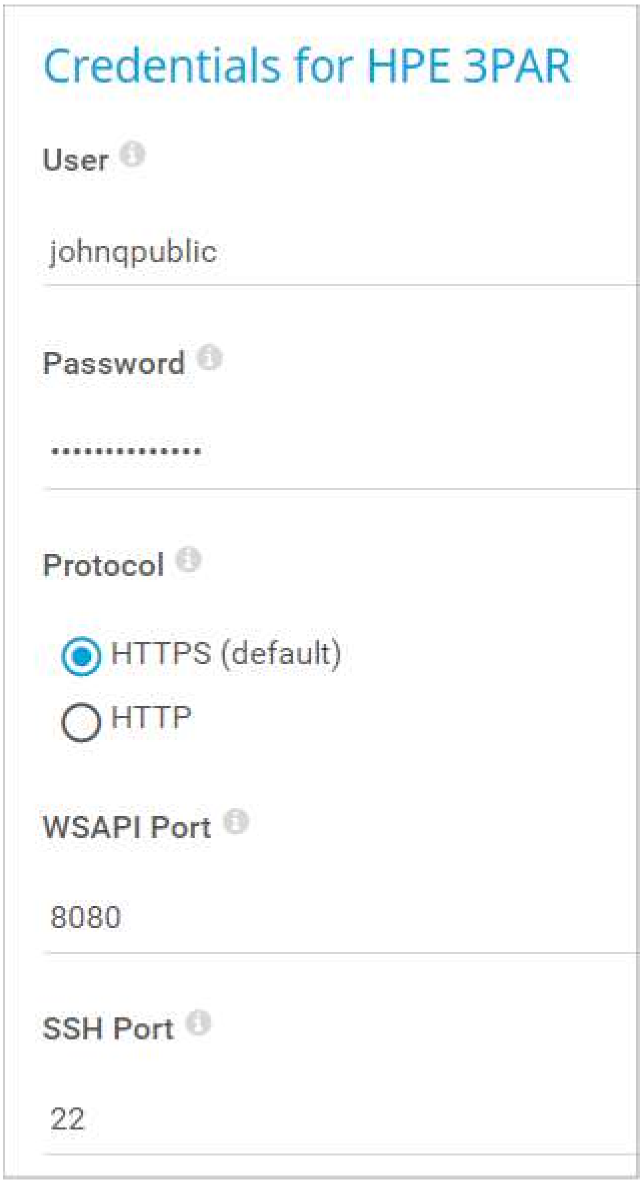
Credentials for FortiGate

Setting	Description
API Token	Enter the API token for access to the FortiGate system.
Port	Enter the port for the connection to the FortiGate system. The default port for secure connections is 443.

Credentials for HPE 3PAR

The settings you define in this section apply to the following sensors:

- HPE 3PAR Common Provisioning Group
- HPE 3PAR Drive Enclosure
- HPE 3PAR Virtual Volume



Credentials for HPE 3PAR

User

johnqpublic

Password

••••••••••••••

Protocol

● HTTPS (default)

○ HTTP

WSAPI Port

8080

SSH Port

22

Credentials for HPE 3PAR

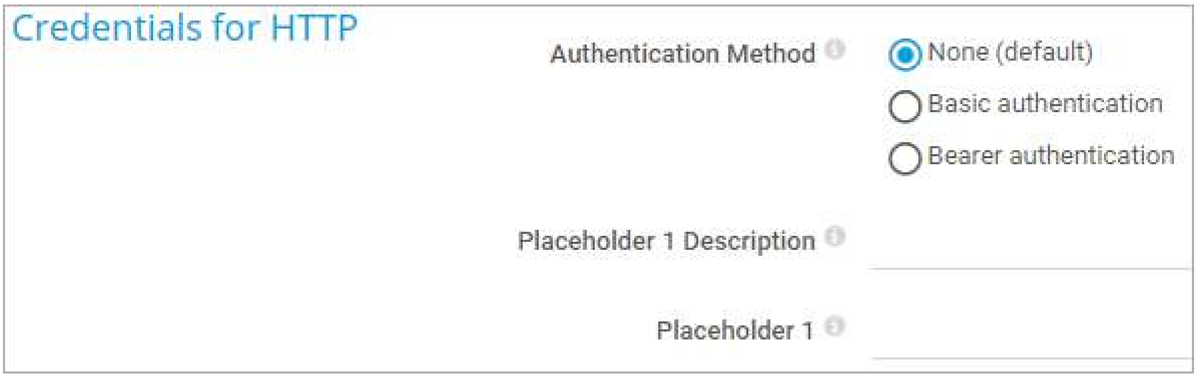
Setting	Description
User Name	Enter the user name for access to the HPE 3PAR system.
Password	Enter the password for access to the HPE 3PAR system.
Protocol	Select the protocol that you want to use for the connection to the HPE 3PAR system: ▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection. ▪ HTTP: Use an unsecure connection.

Setting	Description
WSAPI Port	Enter the Web Services API (WSAPI) port for the connection to the HPE 3PAR system. The default port for secure connections is 8080 and the default port for unsecure connections is 8008. ⓘ For more information, see the Knowledge Base: [Where can I find the Web Services API (WSAPI) port for the connection to the HPE 3PAR system?]
SSH Port	Enter the SSH port for the connection to the HPE 3PAR system. The default port for secure connections is 22.

Credentials for HTTP

ⓘ The settings you define in this section apply to the following sensor:

- HTTP v2



Credentials for HTTP

Authentication Method ● None (default) ○ Basic authentication ○ Bearer authentication

Placeholder 1 Description

Placeholder 1

Credentials for HTTP

Setting	Description
Authentication Method	Select the authentication method for access to the server. Choose between: ▪ None (default): Use no authentication. ▪ Basic authentication: Use basic authentication. ▪ Bearer authentication: Use an OAuth2 bearer token.
User Name	This setting is only visible if you select Basic authentication above. Enter the user name for access to the server.
Password	This setting is only visible if you select Basic authentication above. Enter the password for access to the server.

Setting	Description
Bearer Token	This setting is only visible if you select Bearer authentication above. Enter a bearer token for access to the server.
Placeholder 1 Description	Enter a description for Placeholder 1, for example information about the purpose or content of the placeholder.
Placeholder 1	Enter a value for the placeholder. PRTG inserts the value for the HTTP request if you add %httpplaceholder1 in the URL, POST Body, and Custom Header fields of the HTTP v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 2 Description	Enter a description for Placeholder 2, for example information about the purpose or content of the placeholder.
Placeholder 2	Enter a value for the placeholder. PRTG inserts the value for the HTTP request if you add %httpplaceholder2 in the URL, POST Body, and Custom Header fields of the HTTP v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 3 Description	Enter a description for Placeholder 3, for example information about the purpose or content of the placeholder.
Placeholder 3	Enter a value for the placeholder. PRTG inserts the value for the HTTP request if you add %httpplaceholder3 in the URL, POST Body, and Custom Header fields of the HTTP v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 4 Description	Enter a description for Placeholder 4, for example information about the purpose or content of the placeholder.
Placeholder 4	Enter a value for the placeholder. PRTG inserts the value for the HTTP request if you add %httpplaceholder4 in the URL, POST Body, and Custom Header fields of the HTTP v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 5 Description	Enter a description for Placeholder 5, for example information about the purpose or content of the placeholder.
Placeholder 5	Enter a value for the placeholder. PRTG inserts the value for the HTTP request if you add %httpplaceholder5 in the URL, POST Body, and Custom Header fields of the HTTP v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.

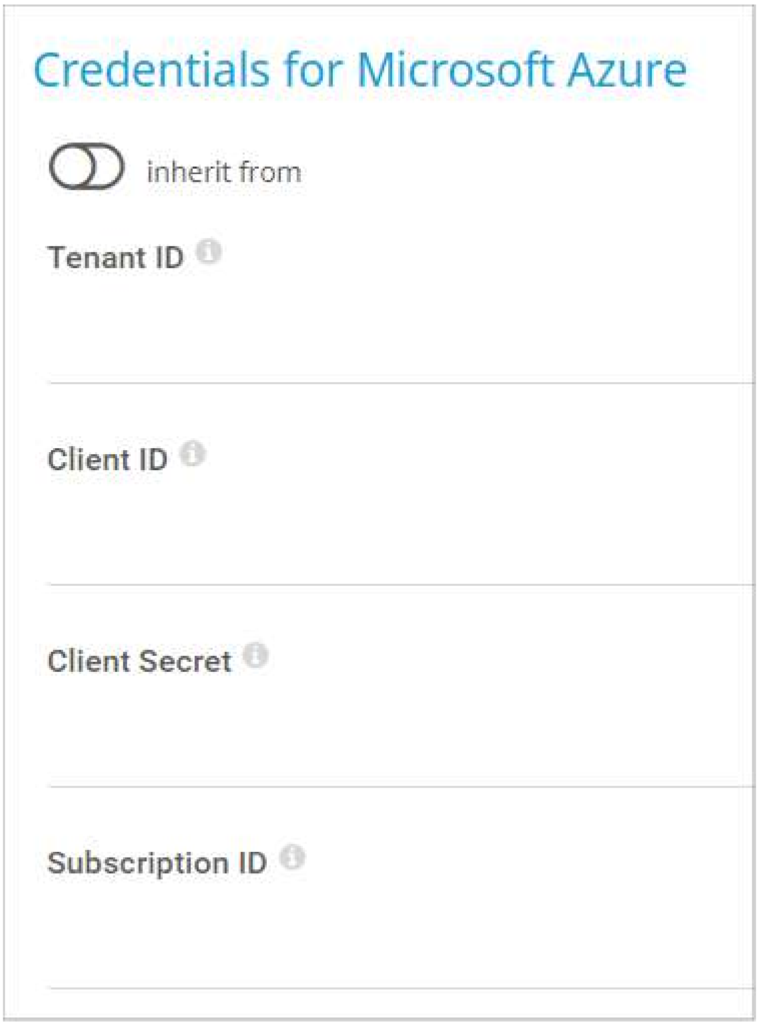
Credentials for Microsoft Azure

ⓘ The settings you define in this section apply to the following sensors:

- Microsoft Azure SQL Database
- Microsoft Azure Storage Account
- Microsoft Azure Subscription Cost
- Microsoft Azure Virtual Machine

The sensors use the credentials to authenticate with Azure Active Directory (Azure AD).

🟦 For more information about the credentials and permissions that are necessary use the Microsoft Azure sensors, see the Knowledge Base: How do I obtain credentials and create custom roles for the Microsoft Azure sensors?


Credentials for Microsoft Azure

○ inherit from

Tenant ID

Client ID

Client Secret

Subscription ID

Credentials for Microsoft Azure

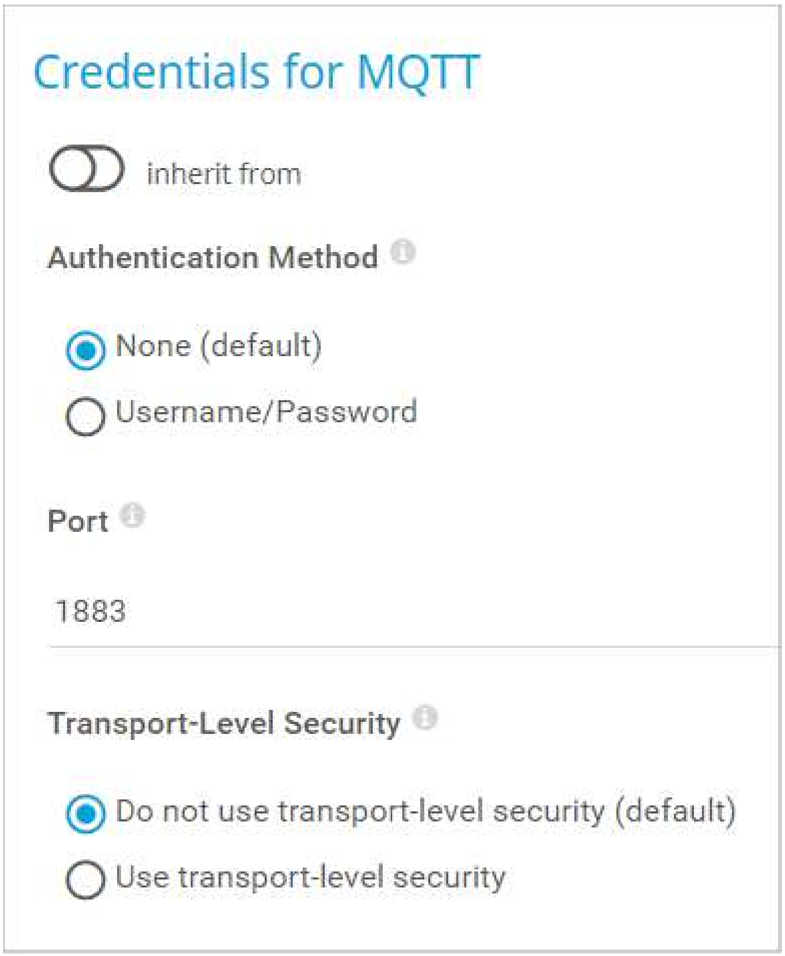
Setting	Description
Tenant ID	Enter the Azure AD tenant ID. ⓘ A tenant ID must be a 32-digit sequence in hexadecimal notation.

Setting	Description
Client ID	Enter the Azure AD client ID.
Client Secret	Enter the Azure AD client secret.
Subscription ID	Enter the Azure AD subscription ID.

Credentials for MQTT

ⓘ The settings you define in this section apply to the following sensors:

- MQTT Round Trip
- MQTT Statistics
- MQTT Subscribe Custom



Credentials for MQTT

inherit from

Authentication Method

● None (default)
○ Username/Password

Port

1883

Transport-Level Security

● Do not use transport-level security (default)
○ Use transport-level security

Credentials for MQTT

Setting	Description
Authentication Method	Select if you want to connect without credentials or define credentials for access to the MQTT broker. ▪ None (default): Connect without credentials. ▪ User name and password: Define credentials for the connection.
User Name	This setting is only visible if you select User name and password above. Enter the user name for access to the Message Queue Telemetry Transport (MQTT) broker.
Password	This setting is only visible if you select User name and password above. Enter the password for access to the MQTT broker.
Port	Enter the port for the connection to the MQTT broker. The default port for secure connections is 8883 and the default port for unsecure connections is 1883.
Transport-Level Security	Select if you want to use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection: ▪ Do not use transport-level security: Establish the connection without connection security. ▪ Use transport-level security: Establish the connection with the strongest SSL/TLS method that the target device provides.
Server Authentication	This setting is only visible if you select Use transport-level security above. Select if you want to use a certificate for server authentication. ▪ Disable (default): Do not use a certificate for server authentication. ▪ Enable: Use a certificate for server authentication.
CA Certificate	This setting is only visible if you enable Server Authentication above. Paste the certificate authority (CA) certificate for the verification of the MQTT broker. ⓘ The certificate must be in Privacy-Enhanced Mail (PEM) format.
Client Authentication	This setting is only visible if you select Use transport-level security above. Select if you want to use a certificate for client authentication. ▪ Disable (default): Do not use a certificate for client authentication. ▪ Enable: Use a certificate for client authentication.
Client Certificate	This setting is only visible if you enable Client Authentication above. Paste the certificate that you created for authenticating the sensor against the MQTT broker.

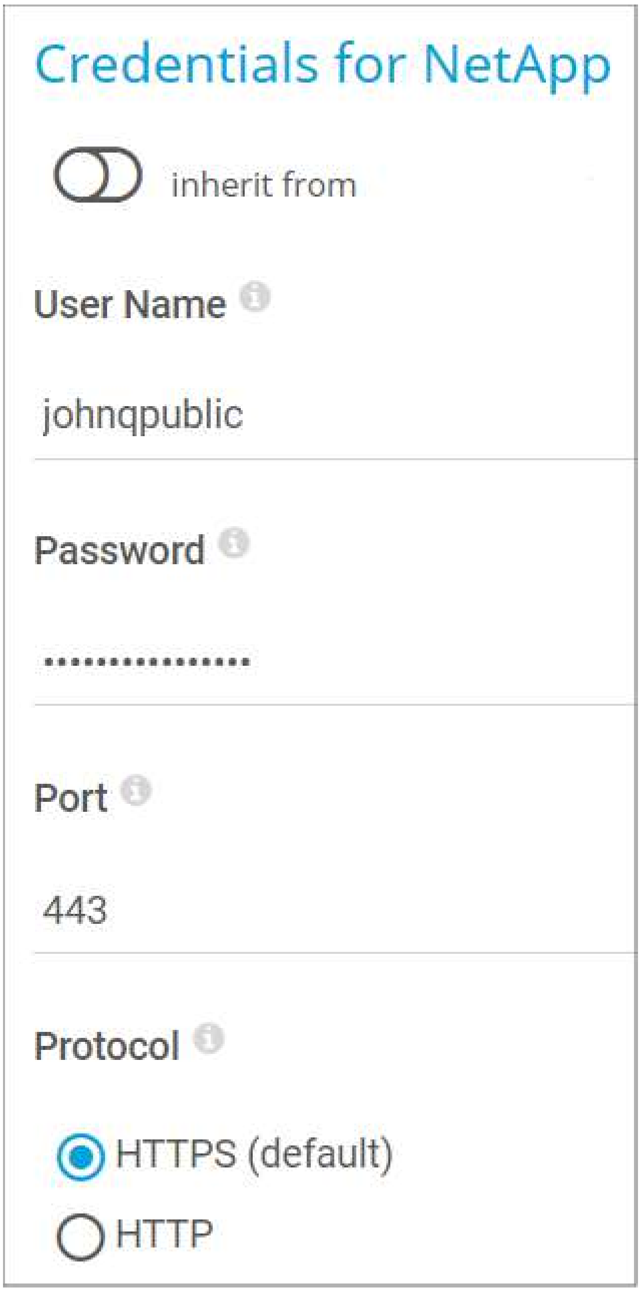
Setting	Description
	ⓘ The certificate must be in PEM format.
Client Key	This setting is only visible if you enable Client Authentication above. Enter the client key for access to the MQTT broker. ⓘ The client key must be in PEM format and it must be encrypted using the Client Key Password.
Client Key Password	This setting is only visible if you enable Client Authentication above. Enter the password for the client key.

Credentials for NetApp

ⓘ The settings you define in this section apply to the following sensors:

- NetApp Aggregate v2
- NetApp I/O v2
- NetApp LIF v2
- NetApp LUN v2
- NetApp NIC v2
- NetApp Physical Disk v2
- NetApp SnapMirror v2
- NetApp System Health v2
- NetApp Volume v2

The sensors use the credentials for access to the ONTAP System Manager.



Credentials for NetApp

inherit from

User Name

johnqpublic

Password

••••••••••••••••

Port

443

Protocol

● HTTPS (default)

○ HTTP

Credentials for NetApp

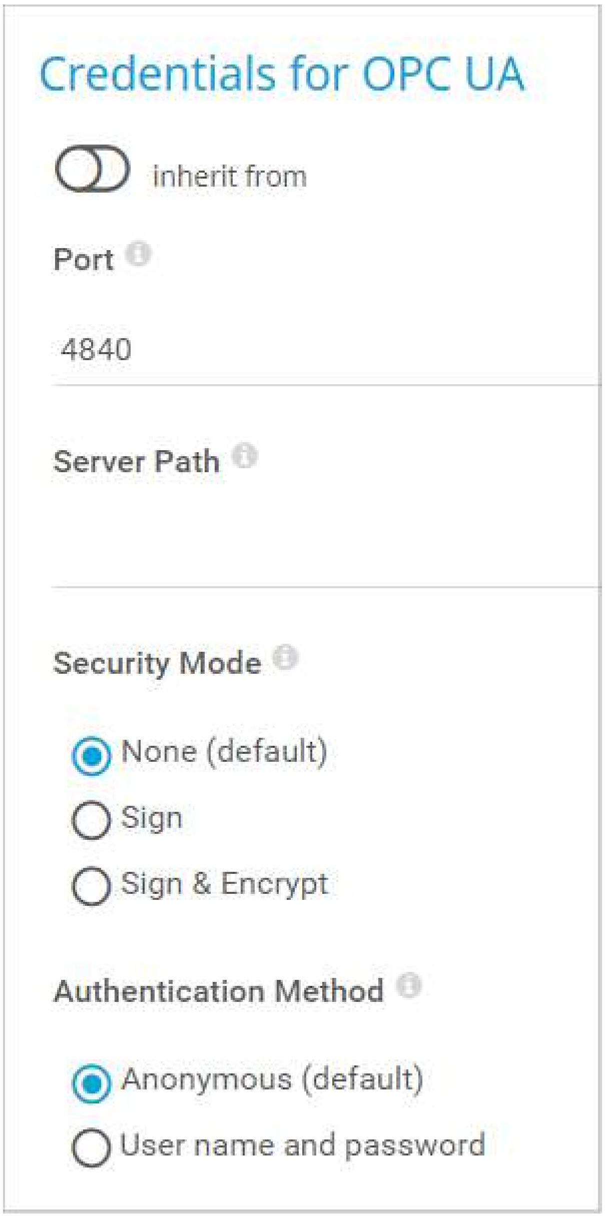
Setting	Description
User Name	Enter a user name for access to the ONTAP System Manager.
Password	Enter the password for access to the ONTAP System Manager.
Port	Enter the port for the connection to the ONTAP System Manager. The default port for secure connections is 443.

Setting	Description
Protocol	Select the protocol that you want to use for the connection to the ONTAP System Manager. Choose between: ▪ HTTPS (default) ▪ HTTP

Credentials for OPC UA

ⓘ The settings you define in this section apply to the following sensors:

- Beckhoff IPC System Health
- OPC UA Certificate
- OPC UA Custom
- OPC UA Server Status



Credentials for OPC UA

inherit from

Port

4840

Server Path

Security Mode

● None (default)
○ Sign
○ Sign & Encrypt

Authentication Method

● Anonymous (default)
○ User name and password

Credentials for OPC UA

Setting	Description
Port	Enter the port for the connection to the OPC Unified Architecture (OPC UA) server. The default port for secure connections is 4840.
Server Path	Enter the path of the OPC UA server endpoint if you run more than one server under the same IP address or DNS name.
Security Mode	Select if you want to use encryption: ▪ None (default): Do not use encryption. ▪ Sign: Sign messages between the sensor and the OPC UA server.

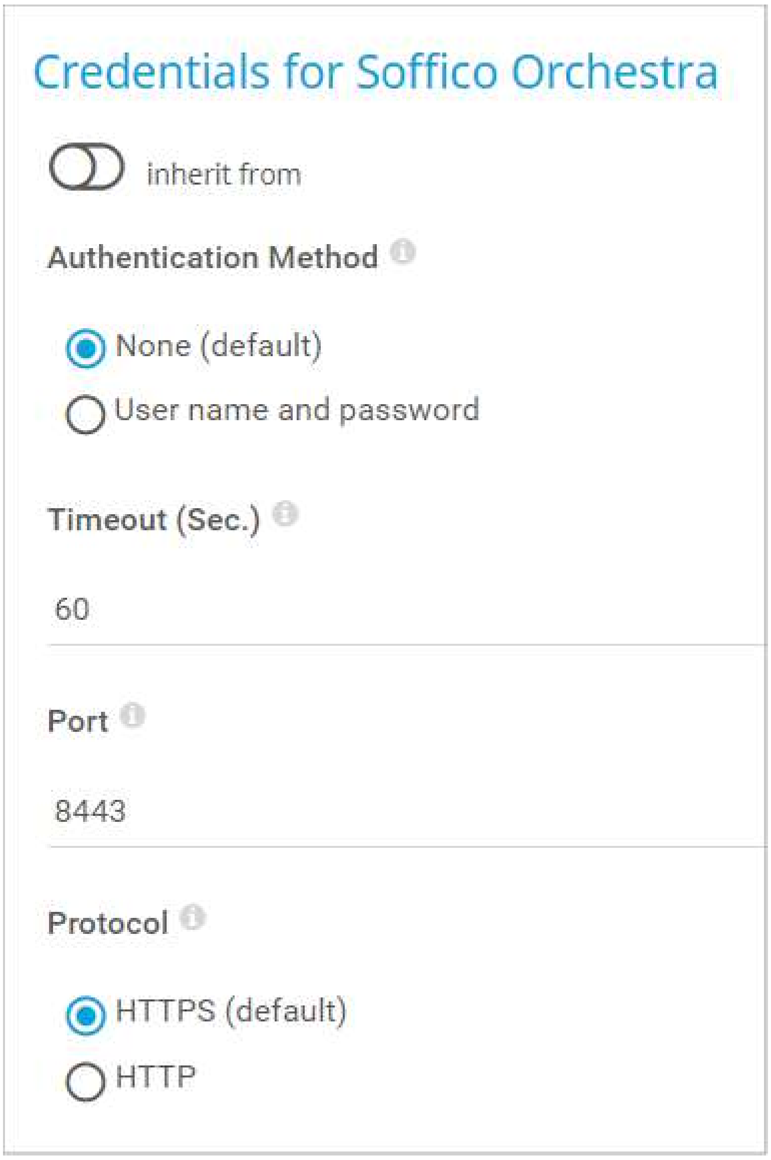
Setting	Description
	▪ Sign & Encrypt: Sign and encrypt messages between the sensor and the OPC UA server.
Security Policy	This setting is only visible if you select Sign or Sign & Encrypt above. Select if you want to use a security policy and define which policy you want to use: ▪ None (default): Do not use a security policy. ▪ Basic256Sha256: Use the Basic256Sha256 security policy. ▪ Basic256: Use the Basic256 security policy.
Client Certificate	This setting is only visible if you select Sign or Sign & Encrypt above. Enter the certificate that you created for authenticating the sensor against the OPC UA server. ⓘ The certificate must meet the following requirements: ▪ The key size must be 2048-bit. ▪ The secure hash algorithm must be SHA256. ▪ DataEncipherment must be part of the KeyUsage certificate extension. ▪ A uniform resource indicator (URI) must be set in subjectAltName. ▪ The certificate must be in Privacy-Enhanced Mail (PEM) format.
Client Key	This setting is only visible if you select Sign or Sign & Encrypt above. Enter the client key for access to the OPC UA server. ⓘ The client key must be in PEM format and it must be encrypted using the Client Key Password.
Client Key Password	This setting is only visible if you select Sign or Sign & Encrypt above. Enter the password for the client key.
Authentication Method	Select if you want to connect without credentials or define credentials for access to the OPC UA server: ▪ Anonymous (default): Connect without credentials. ▪ User name and password: Define credentials for the connection. ⓘ Most OPC UA servers do not support User name and password authentication without a client certificate. To use User name and password authentication, select Sign or Sign & Encrypt under Security Mode and Basic256Sha256 or Basic256 under Security Policy and enter the Client Certificate, Client Key, and Client Key Password that you want to use.

Setting	Description
	ⓘ If you select None (default) under Security Mode and use User name and password authentication, PRTG sends the unencrypted password to the OPC UA server.
User Name	This setting is only visible if you select User name and password above. Enter the user name for access to the OPC UA server.
Password	This setting is only visible if you select User name and password above. Enter the password for access to the OPC UA server.

Credentials for Soffico Orchestra

ⓘ The settings you define in this section apply to the following sensor:

- Soffico Orchestra Channel Health



Credentials for Soffico Orchestra

○ inherit from

Authentication Method

● None (default)

○ User name and password

Timeout (Sec.)

60

Port

8443

Protocol

● HTTPS (default)

○ HTTP

Credentials for Soffico Orchestra

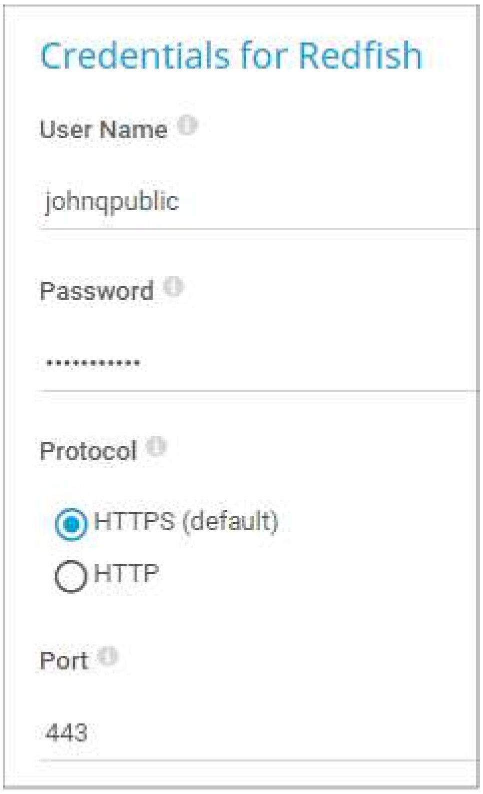
Setting	Description
Authentication Method	Select if you want to connect without credentials or define credentials for access to the Orchestra platform: ▪ None (default): Connect without credentials. ▪ User name and password: Define credentials for the connection.
User Name	This setting is only visible if you select User name and password above. Enter the user name for access to the Orchestra platform.
Password	This setting is only visible if you select User name and password above. Enter the password for access to the Orchestra platform.

Setting	Description
Timeout (Sec.)	Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is 300 seconds (5 minutes).
Port	Enter the port for the connection to the Orchestra platform. The default port for secure connections is 8443 and the default port for unsecure connections is 8019.
Protocol	Select the protocol that you want to use for the connection to the Orchestra platform: ▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection. ▪ HTTP: Use an unsecure connection.

Credentials for Redfish

ⓘ The settings you define in this section apply to the following sensors:

- Redfish Power Supply
- Redfish System Health
- Redfish Virtual Disk



Credentials for Redfish

User Name: johnqpublic

Password: ***********

Protocol

● HTTPS (default)
○ HTTP

Port: 443

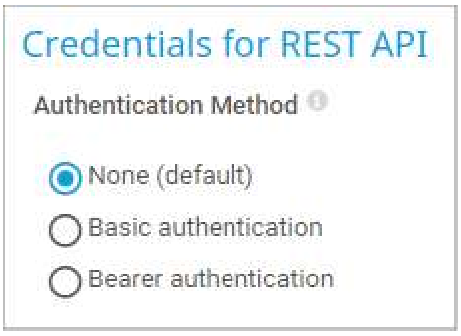
Credentials for Redfish

Setting	Description
User Name	Enter the user name for access to the Redfish system.
Password	Enter the password for access to the Redfish system.
Protocol	Select the protocol that you want to use for the connection to the Redfish system. Choose between: ▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection. ▪ HTTP: Use an unsecure connection.
Port	Enter the port for the connection to the Redfish system. The default port for secure connections is 443.

Credentials for REST API

The settings you define in this section apply to the following sensor:

- REST Custom v2



Credentials for REST API

Authentication Method

● None (default)
○ Basic authentication
○ Bearer authentication

Credentials for REST API

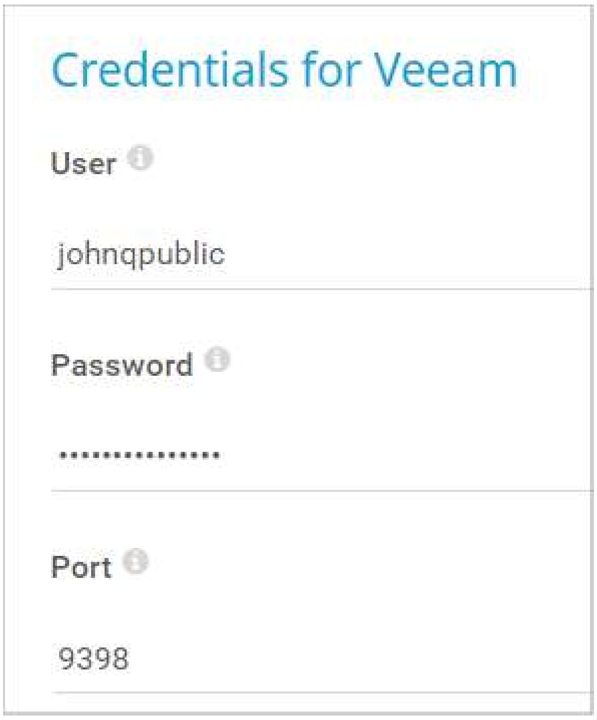
Setting	Description
Authentication Method	Select the authentication method for access to the Representational State Transfer (REST) application programming interface (API): ▪ None (default): Use no authentication. ▪ Basic authentication: Use basic authentication. ▪ Bearer authentication: Use an OAuth2 bearer token.
User Name	This setting is only visible if you select Basic authentication above. Enter the user name for access to the REST API.

Setting	Description
Password	This setting is only visible if you select Basic authentication above. Enter the password for access to the REST API.
Bearer Token	This setting is only visible if you select Bearer authentication above. Enter a bearer token for access to the REST API.
Placeholder 1 Description	Enter a description for Placeholder 1, for example information about the purpose or content of the placeholder.
Placeholder 1	Enter a value for the placeholder. PRTG inserts the value for the REST API request if you add %restplaceholder1 in the Request URL, POST Body, and Custom Headers fields of the REST Custom v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 2 Description	Enter a description for Placeholder 2, for example information about the purpose or content of the placeholder.
Placeholder 2	Enter a value for the placeholder. PRTG inserts the value for the REST API request if you add %restplaceholder2 in the Request URL, POST Body, and Custom Headers fields of the REST Custom v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 3 Description	Enter a description for Placeholder 3, for example information about the purpose or content of the placeholder.
Placeholder 3	Enter a value for the placeholder. PRTG inserts the value for the REST API request if you add %restplaceholder3 in the Request URL, POST Body, and Custom Headers fields of the REST Custom v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 4 Description	Enter a description for Placeholder 4, for example information about the purpose or content of the placeholder.
Placeholder 4	Enter a value for the placeholder. PRTG inserts the value for the REST API request if you add %restplaceholder4 in the Request URL, POST Body, and Custom Headers fields of the REST Custom v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 5 Description	Enter a description for Placeholder 5, for example information about the purpose or content of the placeholder.
Placeholder 5	Enter a value for the placeholder. PRTG inserts the value for the REST API request if you add %restplaceholder5 in the Request URL, POST Body, and Custom Headers fields of the REST Custom v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.

Credentials for Veeam

ⓘ The settings you define in this section apply to the following sensors:

- Veeam Backup Job Status
- Veeam Backup Job Status Advanced



Credentials for Veeam

User ⓘ

johnqpublic

Password ⓘ

•••••••••••••••

Port ⓘ

9398

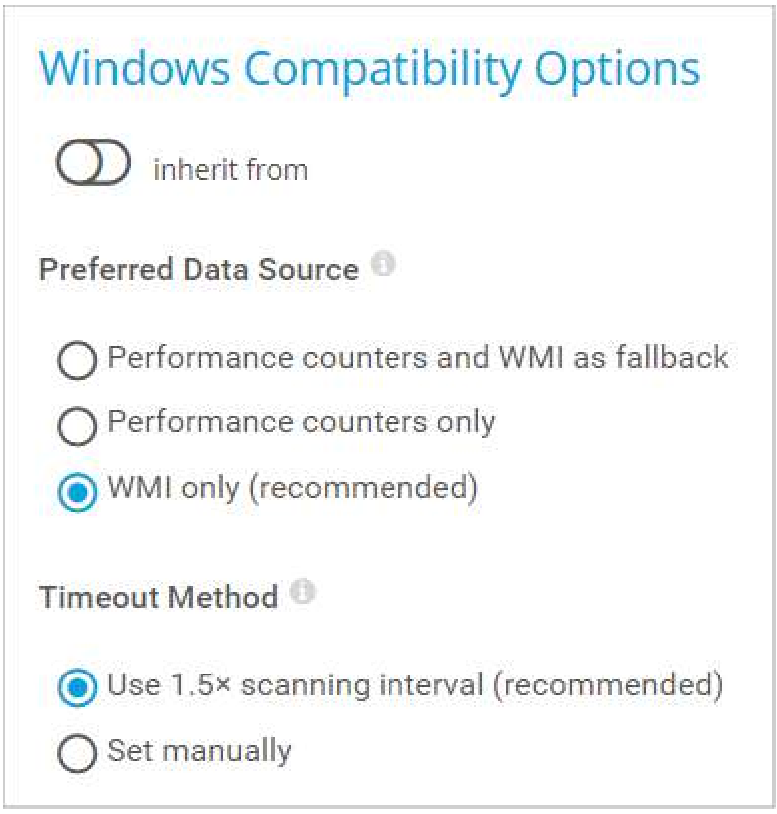
Credentials for Veeam

Setting	Description
User Name	Enter the user name for access to the Veeam Backup Enterprise Manager.
Password	Enter the password for access to the Veeam Backup Enterprise Manager.
Port	Enter the port for the connection to the Veeam Backup Enterprise Manager. The default port for secure connections is 9398.

Windows Compatibility Options

Click ✓ to interrupt the inheritance 135.

If you experience problems when you monitor via Windows sensors, use the following compatibility options for troubleshooting.



Windows Compatibility Options

inherit from

Preferred Data Source

○ Performance counters and WMI as fallback
○ Performance counters only
● WMI only (recommended)

Timeout Method

● Use 1.5× scanning interval (recommended)
○ Set manually

Window s Compatibility Options

Setting	Description
Preferred Data Source	ⓘ This setting only applies to hybrid sensors that use both performance counters and Windows Management Instrumentation (WMI). The setting does not apply to other sensors. Define the method that Windows sensors use to query data: ▪ Performance counters and WMI as fallback: 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, the sensor returns no data. ▪ WMI only (recommended): Query data via WMI only. If this is not possible, the sensor returns no data. We recommend that you use this option.
Timeout Method	Select the time that the sensor waits for the return of the WMI query before the sensor cancels the query and shows an error message: ▪ Use 1.5× scanning interval (recommended): Multiply the scanning interval of the sensor by 1.5 and use the resulting value. ▪ Set manually: Manually enter a timeout value.

Setting	Description
	ⓘ We recommend that you use the default value. ⓘ If you experience ongoing timeout errors, try increasing the timeout value.
Timeout (Sec.)	This setting is only visible if you select Set manually above. Enter the time the sensor waits for the return of its WMI query before it cancels it and shows an error message. Enter an integer. The maximum timeout value is 900 seconds (15 minutes).

SNMP Compatibility Options

Click ✓ to interrupt the inheritance 135.

If you experience problems when you monitor via Simple Network Management Protocol (SNMP) sensors, use the following compatibility options for troubleshooting.