

## SNMP Compatibility Options

☒ inherit from

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

Setting	Description
SNMP Delay (ms)	<p>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.</p> <p><b>i</b> We recommend that you use the default value.</p> <p><b>i</b> If you experience SNMP connection failures, try increasing the delay.</p>
Failed Requests	<p>Select if an SNMP sensor tries again after a request fails:</p> <ul style="list-style-type: none"> <li>▪ <b>Retry (recommended):</b> Try again if an SNMP request fails. This can prevent false error messages because of temporary timeout failures.</li> <li>▪ <b>Do not retry:</b> Do not retry if an SNMP request fails. If you select this option, an SNMP sensor shows a Down status earlier.</li> </ul>
Overflow Values	<p>Select how PRTG handles overflow values. Some devices do not correctly handle internal buffer overflows. This can cause false peaks.</p> <ul style="list-style-type: none"> <li>▪ <b>Ignore (default):</b> Ignore overflow values and do not include them in the monitoring data. We recommend that you use this option.</li> <li>▪ <b>Handle overflow values as valid results:</b> Regard all overflow values as regular data and include them in the monitoring data.</li> </ul> <p><b>i</b> 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: <a href="#">What is the Overflow Values setting in the SNMP Compatibility Options?</a></p>
Zero Values	<p>Select how PRTG handles zero values. Some devices send incorrect zero values. This can cause false peaks.</p> <ul style="list-style-type: none"> <li>▪ <b>Ignore (recommended):</b> Ignore zero values and do not include them in the monitoring data. We recommend that you use this option.</li> <li>▪ <b>Handle zero values as valid results for delta sensors:</b> Regard all zero values as regular data and include them in the monitoring data.</li> </ul> <p><b>i</b> If you experience problems, try changing this option.</p>
32-bit/64-bit Counters	<p>Select the type of traffic counters that PRTG searches for on a device:</p> <ul style="list-style-type: none"> <li>▪ <b>Use 64-bit counters if available (recommended):</b> The interface scan uses 64-bit traffic counters, if available. This can avoid buffer overflows in the devices</li> </ul> <p><b>i</b> We recommend that you use the default value.</p> <p><b>i</b> If you experience problems, try changing this option.</p>

Setting	Description
	<ul style="list-style-type: none"> <li>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.</li> </ul>
Request Mode	<p>Select the request method that PRTG uses for SNMP sensors:</p> <ul style="list-style-type: none"> <li>Use multi get (recommended): Bundle multiple SNMP requests into one request. We recommend that you use this option. <ul style="list-style-type: none"> <li>❗ If you experience problems, try changing this option.</li> </ul> </li> <li>Use single get: Use one request for each SNMP value. This can increase compatibility with older devices.</li> </ul> <p>❗ PRTG uses <a href="#">paging</a> 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.</p>
Walk Mode	<p>Select the kind of SNMP walk that PRTG uses for SNMP sensors:</p> <ul style="list-style-type: none"> <li>Use GETBULK requests (recommended): Request the next <a href="#">x</a> OIDs in one SNMP request. The default value is <a href="#">10</a>. It is dynamic based on the response size. <ul style="list-style-type: none"> <li>❗ 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 <a href="#">object hierarchy</a><sup>[13]</sup>.</li> </ul> </li> <li>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.</li> </ul>
Port Name Template	<p>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 <a href="#">([port]) [ifalias] [ifsensor]</a>, which creates a name like <a href="#">(001) Ethernet1 Traffic</a>. You can use and combine any field names that are available at an OID of your device, for example:</p> <ul style="list-style-type: none"> <li>[port]: The port number of the monitored interface.</li> <li>[ifalias]: The 'alias' name for the monitored interface as specified by a network manager, providing a non-volatile handling.</li> <li>[ifname]: The textual name of the monitored interface as assigned by the local device.</li> <li>[ifdescr]: A textual string containing information about the target device or interface, for example, manufacturer, product name, or version.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ [ifspeed]: An estimate of the monitored interface's current bandwidth (Kbit/s).</li> <li>▪ [ifsensor]: The type of the sensor, this is <a href="#">Traffic</a> or <a href="#">RMON</a>. This helps to differentiate between <a href="#">SNMP Traffic</a> and <a href="#">SNMP RMON</a> sensors.</li> </ul> <p> For more information about SNMP sensor names, see the Knowledge Base: <a href="#">How can I change the defaults for names automatically generated for new SNMP sensors?</a></p>
Port Name Update	<p>Select how PRTG reacts if you change the names of ports in your physical device (for example, a switch or router):</p> <ul style="list-style-type: none"> <li>▪ 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.</li> <li>▪ 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.</li> </ul> <p> For more information about automatic name updates, see the Knowledge Base: <a href="#">Automatically update port name and number for SNMP Traffic sensors when the device changes them.</a></p>
Port Identification	<p>Select the field that PRTG uses for SNMP interface identification:</p> <ul style="list-style-type: none"> <li>▪ Automatic identification (recommended): Try the ifAlias field first to identify an SNMP interface and then try ifDescr.  PRTG does not automatically try ifName.</li> <li>▪ Use ifAlias: For most devices, ifAlias is the best field to use for unique interface names.</li> <li>▪ 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.</li> <li>▪ 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.</li> <li>▪ Do not update ports: Use this option to disable the automatic port identification.</li> </ul>
Start Interface Index	<p> This setting only applies to <a href="#">SNMP Traffic sensors</a> and to <a href="#">Cisco IP SLA sensors</a>.</p> <p>Enter the index at which PRTG starts to query the interface range during sensor creation. Enter <b>0</b> for the automatic mode.</p>

Setting	Description
	<p>❗ We recommend that you use the default value.</p>
End Interface Index	<p>❗ This setting only applies to <a href="#">SNMP Traffic sensors</a> and to <a href="#">Cisco IP SLA sensors</a>.</p> <p>Enter the index at which PRTG stops querying the interface range during sensor creation. Enter 0 for the automatic mode.</p> <p>❗ We recommend that you use the default value.</p>

## Proxy Settings for HTTP Sensors

Click  to interrupt the [inheritance](#) <sup>135</sup>.

❗ 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](#) <sup>8325</sup>.

❗ 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



inherit from

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 <b>8080</b> . Enter an integer.
User Name	<p>If the proxy requires authentication, enter the user name for the proxy login.</p> <p>ⓘ Only basic authentication is available. Enter a string or leave the field empty.</p>
Password	If the proxy requires authentication, enter the password for the proxy login.


Setting	Description
	 Only basic authentication is available. Enter a string or leave the field empty.


## Scanning Interval


Click  to interrupt the [inheritance](#) .


### Scanning Interval

 inherit from

**Scanning Interval** 





60 seconds 

**If a Sensor Query Fails** 

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

Scanning Interval

Setting	Description
Scanning Interval	<p>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:</p> <ul style="list-style-type: none"> <li>▪ 30 seconds</li> <li>▪ 60 seconds</li> <li>▪ 5 minutes</li> <li>▪ 10 minutes</li> <li>▪ 15 minutes</li> <li>▪ 30 minutes</li> <li>▪ 1 hour</li> <li>▪ 4 hours</li> <li>▪ 6 hours</li> <li>▪ 12 hours</li> <li>▪ 24 hours</li> </ul>

Setting	Description
	<p> You can change the available intervals in the <a href="#">system administration</a><sup>[3307]</sup> of PRTG Network Monitor.</p>
If a Sensor Query Fails	<p>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 <a href="#">status</a><sup>[179]</sup>. 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:</p> <ul style="list-style-type: none"> <li>▪ Set sensor to down status immediately: Set the sensor to the Down status immediately after the first request fails.</li> <li>▪ 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.</li> <li>▪ 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.</li> <li>▪ 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.</li> <li>▪ 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.</li> <li>▪ 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.</li> </ul> <p> 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.</p> <p> If you define error limits for a sensor's channels, the sensor immediately shows the Down status. None of the interval options apply.</p> <p> If a channel uses <a href="#">lookup</a><sup>[3604]</sup> values, the sensor immediately shows the Down status. None of the interval options apply.</p>

## Cluster Monitoring Exclusion

Click  to interrupt the [inheritance](#)<sup>[135]</sup>.



Setting	Description
Exclude Cluster Nodes	<p>This setting is only visible if you have a <a href="#">failover cluster</a><sup>128</sup>.</p> <p>Sometimes you want to keep a cluster node from monitoring the sensors that run on this probe, group, or device, for example, if a device is not reachable from every cluster node. Select the cluster nodes that you do not want to include in sensor scans. By default, all objects underneath the probe <a href="#">inherit</a><sup>135</sup> this setting.</p>

## Schedules, Dependencies, and Maintenance Window

**i** You cannot interrupt the inheritance for schedules, dependencies, and maintenance windows. The corresponding settings from the parent objects are always active. However, you can define additional schedules, dependencies, and maintenance windows. They are active at the same time as the parent objects' settings.

### Schedules, Dependencies, and Maintenance Window

☐ inherit from

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** <sup>i</sup>

None ▼

**Maintenance Window** <sup>i</sup>





☒ Do not set up a one-time maintenance window  
☐ Set up a one-time maintenance window



**Dependency Type** <sup>i</sup>

☒ Use parent  
☐ Select a sensor

Schedules, Dependencies, and Maintenance Window

Setting	Description
Schedule	<p>Select a schedule from the list. You can use schedules to monitor during a certain time span (days or hours) every week. Choose from:</p> <ul style="list-style-type: none"> <li>None</li> </ul>


Setting	Description
	<ul style="list-style-type: none"> <li>▪ Saturdays</li> <li>▪ Sundays</li> <li>▪ Weekdays</li> <li>▪ Weekdays Eight-To-Eight (08:00 - 20:00)</li> <li>▪ Weekdays Nights (17:00 - 09:00)</li> <li>▪ Weekdays Nights (20:00 - 08:00)</li> <li>▪ Weekdays Nine-To-Five (09:00 - 17:00)</li> <li>▪ Weekends</li> </ul> <p> You can create schedules, edit schedules, or pause monitoring for a specific time span. For more information, see section <a href="#">Schedules</a> .</p>
Maintenance Window	<p>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:</p> <ul style="list-style-type: none"> <li>▪ Do not set up a one-time maintenance window: Do not set up a one-time maintenance window. Monitoring is always active.</li> <li>▪ 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.</li> </ul> <p> To close an active one-time maintenance window before the defined end date, change the time entry in Maintenance Ends to a date in the past.</p>
Maintenance Begins	<p>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.</p>
Maintenance Ends	<p>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.</p>
Dependency Type	<p>Select a dependency type. You can use dependencies to pause monitoring for an object depending on the status of a different object. You can choose from:</p> <ul style="list-style-type: none"> <li>▪ Use parent: Use the dependency type of the parent object.</li> <li>▪ Select a sensor: Use the dependency type of the parent object. Additionally, pause the current object if a specific sensor is in the Down status or in the Paused status because of another dependency.</li> </ul> <p> You do not trigger a status change by dependency if you manually pause a master sensor or if you pause it by schedule.</p>

Setting	Description
	<p> To test your <a href="#">dependencies</a> <sup>[316]</sup>, select Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later, all dependent objects are paused. You can check all dependencies under Devices   Dependencies in the main menu bar.</p>
Dependency	<p>This setting is only visible if you enable Select a sensor above. Click  and use the <a href="#">object selector</a> <sup>[219]</sup> to select a sensor on which the current object will depend.</p>
Dependency Delay (Sec.)	<p>This setting is only visible if you select Select a sensor above. Define a time span in seconds for the dependency delay.</p> <p>After the master sensor for this dependency returns to the Up status, PRTG additionally delays the monitoring of the dependent objects by the time span you define. This can prevent false alarms, for example, after a server restart or to give systems more time for all services to start. Enter an integer.</p>



## Access Rights

Click  to interrupt the [inheritance](#) <sup>[135]</sup>.

### 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	<p>Select the <a href="#">user groups</a> <sup>134</sup> 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:</p> <ul style="list-style-type: none"> <li>▪ Inherited: Inherit the access rights settings of the parent object.</li> <li>▪ 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. <ul style="list-style-type: none"> <li>❗ 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.</li> </ul> </li> <li>▪ Read access: Users in this group can see the object and view its monitoring results. They cannot edit any settings.</li> <li>▪ 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.</li> <li>▪ Full access: Users in this group can see the object, view its monitoring results, edit its settings, and edit its access rights settings.</li> </ul> <p>To automatically set all child objects to inherit this object's access rights, enable the Revert access rights of child objects to "inherited" option.</p> <p>■ For more details on access rights, see section <a href="#">Access Rights Management</a> <sup>144</sup>.</p>









## Channel Unit Configuration

Click  to interrupt the [inheritance](#) <sup>135</sup>.


### Channel Unit Configuration

 inherit from

#### Channel Unit Types

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


Channel Unit Configuration

Setting	Description
Channel Unit Types	<p>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):</p> <ul style="list-style-type: none"><li>▪ Bandwidth</li><li>▪ Memory</li><li>▪ Disk</li><li>▪ File</li><li>▪ Custom</li></ul> <p> Custom channel types are only available on sensor level.</p>

## Advanced Network Analysis

Click  to interrupt the [inheritance](#) <sup>[135]</sup>.

### Advanced Network Analysis

 inherit from

#### Unusual Detection <sup>i</sup>

☒ Enable
 ☐ Disable

#### Similar Sensors Detection <sup>i</sup>

☒ Enable
 ☐ Disable

#### System Information <sup>i</sup>

☒ Enable
 ☐ Disable

Advanced Network Analysis

Setting	Description
Unusual Detection	<p>Select if you want to use the <a href="#">unusual detection</a> <sup>[3309]</sup> for sensors:</p> <ul style="list-style-type: none"> <li>▪ Enabled: Activates the unusual detection for this object and, by default, for all objects underneath in the <a href="#">object hierarchy</a> <sup>[131]</sup>. Sensors that are affected by this setting show the Unusual status if PRTG detects unusual activity.</li> <li>▪ 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.</li> </ul> <p><sup>i</sup> You can configure the behavior of the unusual detection or completely disable it in the <a href="#">system settings</a> <sup>[3309]</sup>.</p>

Setting	Description
Similar Sensors Detection	<p>Select if you want to activate the <a href="#">similar sensors</a><sup>[189]</sup> analysis:</p> <ul style="list-style-type: none"> <li>▪ 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.</li> <li>▪ Disabled: Does not activate the similar sensors detection. PRTG does not consider sensors that are affected by this setting during the similarity analysis.</li> </ul> <p><b>i</b> You can configure the depth of the analysis of the similar sensors detection or completely disable it in the <a href="#">system settings</a><sup>[331]</sup>.</p>
System Information	<p>Select if you want to retrieve and show <a href="#">system information</a><sup>[202]</sup> for your devices:</p> <ul style="list-style-type: none"> <li>▪ Enabled: Activates the system information feature for this object and, by default, for all objects underneath in the hierarchy.</li> <li>▪ Disabled: Does not activate the system information feature.</li> </ul> <p><b>i</b> The System Information feature is enabled by default. To retrieve the data, PRTG automatically uses the <a href="#">credentials for Windows systems</a><sup>[596]</sup> and the <a href="#">credentials for SNMP devices</a><sup>[603]</sup> that you entered in the device settings or that the device <a href="#">inherits</a><sup>[131]</sup> 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 <a href="#">SNMP v1</a> or <a href="#">SNMP v2c</a>, which do not provide encryption.</p> <p><b>☁</b> This setting is not available on the hosted probe of a PRTG Hosted Monitor instance.</p>

## Administrative Probe Settings

Define the IP address to use for outgoing monitoring requests.

- If more than one IP is available on the system, you can specify the IP address that PRTG uses for the outgoing monitoring requests of certain sensors.
  - This setting is for sensors that use the following connection types: HTTP, Domain Name System (DNS), File Transfer Protocol (FTP), Internet Message Access Protocol (IMAP), Post Office Protocol version 3 (POP3), port, remote desktop, Simple Mail Transfer Protocol (SMTP), and Simple Network Management Protocol (SNMP).
  - The setting is valid for all monitoring requests that this probe sends.
  - This setting is useful for devices that expect a certain IP address when they are queried.
  - The default setting is auto. PRTG automatically selects an IP address.
- i** This feature does not support all sensors for technical reasons.
- i** If you change this setting, some sensors might stop working. For example, sensors might show the Down status if the selected IP address is blocked on the way to or directly on the target device.

## Administrative Probe Settings

### Outgoing IPv4 ⓘ

- ☒ auto
- ☐ 192.0.2.0
- ☐ 192.0.2.1
- ☐ 192.0.2.3


### Outgoing IPv6 ⓘ

- ☒ auto
- ☐ 2003:EA:970D:9900:0000:0000:0000:0000
- ☐ 2003:EA:970D:9900:0000:0000:0000:0000
- ☐ FE80:0:0:0:94A7:0000:0000:0000

Administrative Probe Settings

Setting	Description
Outgoing IPv4	Define the IP address for outgoing requests that use the IPv4 protocol. The list shows all available IP addresses on the system. Choose a specific IP address or select auto.
Outgoing IPv6	<p>Define the IP address for outgoing requests that use the IPv6 protocol. The list shows all available IP addresses on the system. Choose a specific IP address or select auto.</p> <p>■ For more information, see section <a href="#">IPv6 Support</a> <sup>149</sup>.</p>
Cluster Connectivity	<p>This setting is only visible if you have a <a href="#">failover cluster</a> <sup>128</sup>.</p> <p>Define if the remote probe connects to all cluster nodes or only to the primary master node:</p> <ul style="list-style-type: none"> <li>Remote probe sends data only to primary master node: The remote probe only connects to the primary master node. You are not able to review monitoring data on failover nodes. Consider this option if you have bandwidth limitations in your network or if the remote probe cannot access your failover nodes.</li> </ul>




Setting	Description
	<ul style="list-style-type: none"> <li>Remote probe sends data to all cluster nodes: The remote probe connects to all cluster nodes and sends monitoring data to the failover nodes in addition to the primary master node. The remote probe is visible on all of your cluster nodes as soon as it automatically connects to the correct IP addresses and ports of the failover nodes. If the primary master node fails, you can still see monitoring data of the remote probe.</li> </ul> <p> PRTG does not notify you if a remote probe is disconnected from a cluster node. Therefore, explicitly check on a cluster node if remote probes are connected (for example, via the device tree in the PRTG web interface on a cluster node).</p>

## Scheduled Restart Settings

 This setting is not available on the hosted probe of a PRTG Hosted Monitor instance.

### Scheduled Restart Settings


**Restart Options** 


☒ No scheduled system or service restart


☐ Scheduled restart of PRTG services

☐ Scheduled system restart (recommended)

Scheduled Restart Settings

Setting	Description
Restart Options	<p>Define if you want to schedule an automatic restart:</p> <ul style="list-style-type: none"> <li>No scheduled system or service restart: Do not automatically perform a scheduled restart of services. We recommend that you manually restart the PRTG core server system every few weeks. You can initiate a restart of the PRTG probe service in the <a href="#">Administrative Tools</a>  in the PRTG web interface.</li> <li>Scheduled restart of PRTG services: Restart the PRTG probe service on the probe system. If you select this option on the local probe, the PRTG core server service restarts as well. Define a schedule under Restart Schedule.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>Scheduled system restart (recommended): Define a schedule under Restart Schedule. We recommend that you restart probe systems once a month for best performance.</li> </ul>
Restart Schedule	<p>This setting is only visible if you select a schedule option above. Choose how often you want to restart the PRTG probe service or the probe system:</p> <ul style="list-style-type: none"> <li>Once per week: Select a day and a time below.</li> <li>Once per month (recommended): Select a day of the month and a time below.</li> </ul>
Day	<p>This setting is only visible if you select a schedule option above. Select a day of the week (Monday to Sunday) or month (1st to 30th or Last). If you select Last, PRTG restarts the PRTG core server system on the last day of the month, regardless of how many days the month has.</p>
Time	<p>This setting is only visible if you select a schedule option above. Select a time for the planned restart.</p> <p> You get a Windows warning message 10 minutes before the restart to inform you about the restart if you are logged in to PRTG. The actual restart time can differ by up to 30 minutes from the time you enter here.</p>

 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>

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>

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>










## 7.6 Group Settings

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

- ❗ This documentation does not refer to the settings of the root group. For more information, see section [Root Group Settings](#)<sup>[419]</sup>.
- ❗ We recommend that you define as many settings as possible in the [root group settings](#)<sup>[419]</sup> so that you can inherit them to all other objects in the [object hierarchy](#)<sup>[131]</sup>.
- ❗ 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](#)<sup>[521]</sup>
- [Device Identification and Auto-Discovery](#)<sup>[523]</sup>
- [Location](#)<sup>[529]</sup>
- [Credentials for Windows Systems](#)<sup>[529]</sup>
- [Credentials for Linux/Solaris/macOS \(SSH/WBEM\) Systems](#)<sup>[532]</sup>
- [Credentials for VMware/XenServer](#)<sup>[536]</sup>
- [Credentials for SNMP Devices](#)<sup>[537]</sup>
- [Credentials for Database Management Systems](#)<sup>[541]</sup>
- [Credentials for AWS](#)<sup>[543]</sup>
- [Credentials for Microsoft 365](#)<sup>[544]</sup>
- [Credentials for Script Sensors](#)<sup>[546]</sup>
- [Credentials for Cisco Meraki](#)<sup>[547]</sup>
- [Credentials for Dell EMC](#)<sup>[548]</sup>
- [Credentials for FortiGate](#)<sup>[549]</sup>
- [Credentials for HPE 3PAR](#)<sup>[550]</sup>
- [Credentials for HTTP](#)<sup>[552]</sup>
- [Credentials for Microsoft Azure](#)<sup>[554]</sup>
- [Credentials for MQTT](#)<sup>[555]</sup>
- [Credentials for NetApp](#)<sup>[557]</sup>
- [Credentials for OPC UA](#)<sup>[559]</sup>
- [Credentials for Soffico Orchestra](#)<sup>[562]</sup>
- [Credentials for Redfish](#)<sup>[564]</sup>
- [Credentials for REST API](#)<sup>[565]</sup>
- [Credentials for Veeam](#)<sup>[567]</sup>

- [Windows Compatibility Options](#) 
- [SNMP Compatibility Options](#) 
- [Proxy Settings for HTTP Sensors](#) 
- [Scanning Interval](#) 
- [Schedules, Dependencies, and Maintenance Window](#) 
- [Access Rights](#) 
- [Channel Unit Configuration](#) 
- [Advanced Network Analysis](#) 
- [Number of Sensors Limitation](#) 

## Basic Group Settings

### Basic Group Settings

Group Name ⓘ

Network Infrastructure

Monitoring Status ⓘ

☒ Started
☐ Paused

Parent Tags ⓘ

Tags ⓘ

+

Priority ⓘ

★ ★ ★ ☆ ☆

Basic Group Settings

Setting	Description
Group Name	<p>Enter a name to identify the group. By default, PRTG shows this name in the <a href="#">device tree</a><sup>[164]</sup>, as well as in <a href="#">alarms</a><sup>[199]</sup>, <a href="#">logs</a><sup>[208]</sup>, <a href="#">notifications</a><sup>[3173]</sup>, <a href="#">reports</a><sup>[3192]</sup>, <a href="#">maps</a><sup>[3214]</sup>, <a href="#">libraries</a><sup>[3176]</sup>, and <a href="#">tickets</a><sup>[211]</sup>.</p> <p><b>i</b> If the name contains angle brackets (&lt;&gt;), PRTG replaces them with braces ({} for security reasons. For more information, see the Knowledge Base: <a href="#">What security features does PRTG include?</a></p>
Monitoring Status	<p>Select the monitoring status of the group:</p> <ul style="list-style-type: none"> <li>Started: Monitor the group.</li> <li>Paused: Pause monitoring for the group. All sensors on all devices in the group are in the Paused <a href="#">status</a><sup>[224]</sup> until you change this setting.</li> </ul>
Parent Tags	<p>Shows the <a href="#">tags</a><sup>[137]</sup> that this group <a href="#">inherits</a><sup>[137]</sup> from its parent <a href="#">probe</a><sup>[132]</sup>.</p> <p><b>i</b> This setting is for your information only. You cannot change it.</p>
Tags	<p>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 <a href="#">inherited</a><sup>[137]</sup>.</p> <p><b>i</b> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with parentheses (()) or angle brackets (&lt;&gt;).</p> <p><b>i</b> For performance reasons, it can take some minutes until you can filter for new tags that you added.</p>
Priority	<p>Select a <a href="#">priority</a><sup>[221]</sup> for the group. This setting determines the position of the group in lists. The highest priority is at the top of a list. You can choose from the lowest priority ( ★☆☆☆☆ ) to the highest priority ( ★★★★★ ).</p>




## Device Identification and Auto-Discovery

### Device Identification and Auto-Discovery

#### Auto-Discovery Level

- ☒ No auto-discovery
- ☐ Standard auto-discovery (recommended)
- ☐ Detailed auto-discovery
- ☐ Auto-discovery with specific device templates

Device Identification and Auto-Discovery

Setting	Description
Auto-Discovery Level	<p>Select the level of detail for the <a href="#">auto-discovery</a> .</p> <ul style="list-style-type: none"> <li>▪ No auto-discovery: Select this option if you only want to manually create devices and sensors.</li> <li>▪ Standard auto-discovery (recommended): Create a set of standard sensors for standard monitoring. This option works fine for most installations.</li> <li>▪ Detailed auto-discovery: Create all standard sensors and additional sensors from detailed variants of device templates. As a result, you might get many sensors. This option is suitable for small network segments and whenever you want to monitor the maximum number of sensors available.</li> <li>▪ Auto-discovery with specific device templates: Customize the auto-discovery and select or combine standard, detailed, and custom device templates. Select one or more templates from the Device Templates list.</li> </ul> <p> Auto-discoveries can be resource intensive. They are primarily intended for devices on the same network as your probes.</p>
Device Templates	<p>This setting is only visible if you select Auto-discovery with specific device templates above. Select one or more device templates by enabling a check box in front of the template name.</p> <p> You can also select all items or cancel the selection by using the check box in the table header.</p> <p>PRTG uses the device templates that you select for the auto-discovery on the device. Choose from:</p>





Setting	Description
	<ul style="list-style-type: none"> <li>▪ ADSL</li> <li>▪ Amazon CloudWatch</li> <li>▪ Buffalo TeraStation NAS</li> <li>▪ Cisco ASA VPN</li> <li>▪ Cisco Device (Generic)</li> <li>▪ Dell EqualLogic</li> <li>▪ Dell MDi Disk</li> <li>▪ DNS Server</li> <li>▪ Environment Jakarta</li> <li>▪ Environment Poseidon</li> <li>▪ FTP Server</li> <li>▪ Generic Device (Ping Only)</li> <li>▪ Generic Device (SNMP Enabled)</li> <li>▪ Generic Device (SNMP Enabled, Detailed)</li> <li>▪ HTTP Web Server</li> <li>▪ Hyper-V Host Server</li> <li>▪ IPMI-enabled Device</li> <li>▪ Juniper NS Device</li> <li>▪ Linux/UNIX Device (SNMP or SSH Enabled)</li> <li>▪ Mail Server (Generic)</li> <li>▪ Mail Server (MS Exchange)</li> <li>▪ Microsoft SharePoint 2010</li> <li>▪ NAS LenovoEMC</li> <li>▪ NAS QNAP</li> <li>▪ NAS Synology</li> <li>▪ NetApp</li> <li>▪ NTP Server</li> <li>▪ Printer (HP)</li> <li>▪ Printer (Generic)</li> <li>▪ RDP Server</li> <li>▪ RMON-compatible Device</li> <li>▪ Server (Cisco UCS)</li> </ul>




Setting	Description
	<ul style="list-style-type: none"> <li>▪ Server (Compaq/HP Agents)</li> <li>▪ Server (Dell)</li> <li>▪ Server (Fujitsu)</li> <li>▪ Server (IBM)</li> <li>▪ SonicWall</li> <li>▪ SSL Security Check</li> <li>▪ Switch (Cisco Catalyst)</li> <li>▪ Switch (Cisco IOS Based)</li> <li>▪ Switch (HP Procurve)</li> <li>▪ UNIX/Linux Device</li> <li>▪ UPS Health (APC)</li> <li>▪ UPS Health (Generic)</li> <li>▪ UPS Health (Liebert)</li> <li>▪ VMware ESXi / vCenter Server</li> <li>▪ Web Server</li> <li>▪ Windows (Detailed via WMI)</li> <li>▪ Windows (via Remote PowerShell)</li> <li>▪ Windows (via WMI)</li> <li>▪ Windows IIS (via SNMP)</li> <li>▪ XenServer Hosts</li> <li>▪ XenServer Virtual Machines</li> </ul> <p>Once the auto-discovery is finished, PRTG creates a new <a href="#">ticket</a><sup>[211]</sup> and lists the device templates that it used to create new sensors.</p>
Schedule	<p>Select when PRTG runs the auto-discovery:</p> <ul style="list-style-type: none"> <li>▪ Once: Run the auto-discovery only once. PRTG adds new devices and sensors once. If you select this option, you must manually <a href="#">start the auto-discovery</a><sup>[265]</sup>.</li> <li>▪ Hourly: Run the auto-discovery for new devices and sensors every 60 minutes. <ul style="list-style-type: none"> <li>❗ Use this option with caution. Frequent auto-discoveries might cause performance issues, in particular when PRTG scans large network segments every hour.</li> </ul> </li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Daily: Run the auto-discovery for new devices and sensors every 24 hours. The first auto-discovery runs immediately. All other discoveries start at the time that you define in the <a href="#">Monitoring</a> settings, section Auto-Discovery.</li> <li>▪ Weekly: Run the auto-discovery for new devices and sensors every 7 days. The first auto-discovery runs immediately. All other discoveries start at the time that you define in the Monitoring settings, section Auto-Discovery.</li> </ul> <p><b>i</b> For performance reasons, PRTG sets Schedule to Once on all devices that the scheduled auto-discovery creates.</p>
IP Address Selection Method	<p>Select how you want to define the IP address range for the auto-discovery:</p> <ul style="list-style-type: none"> <li>▪ Class C base IP address with start/end (IPv4): Enter an IPv4 class C address range.</li> <li>▪ List of individual IP addresses and DNS names (IPv4): Enter a list of individual IPv4 addresses or Domain Name System (DNS) names.</li> <li>▪ IP address and subnet (IPv4): Enter an IPv4 address and subnet mask.</li> <li>▪ IP address with octet range (IPv4): Enter an IPv4 address range for every IP octet individually. With this, you can define very customizable IP address ranges.</li> <li>▪ List of individual IP addresses and DNS names (IPv6): Enter a list of individual IPv6 addresses or DNS names.</li> <li>▪ Use computers from the Active Directory (maximum 1000 computers): Search in the Active Directory for computers to perform the auto-discovery.</li> </ul> <p><b>i</b> Make sure that you specify your Active Directory domain in the <a href="#">Core &amp; Probes</a> settings.</p> <p><b>i</b> PRTG can only discover subnets with up to 65,536 IP addresses. If you define a range with a higher number of addresses, the discovery stops before it is completed.</p>
IPv4 Base	<p>This setting is only visible if you select Class C base IP address with start/end (IPv4) above. Enter a class C network as the IP base for the auto-discovery. Enter the first three octets of an IPv4 address, for example, <a href="#">192.168.0</a>.</p>
IPv4 Range Start	<p>This setting is only visible if you select Class C base IP address with start/end (IPv4) above. Enter the IP octet of the class C network (specified above) from which PRTG starts the auto-discovery. This completes the IP base to an IPv4 address. For example, enter <a href="#">1</a> to discover from <a href="#">192.168.0.1</a> onwards.</p>

Setting	Description
IPv4 Range End	This setting is only visible if you select Class C base IP address with start/end (IPv4) above. Enter the IP octet of the class C network (specified above) at which PRTG stops the auto-discovery. This completes the IP base to an IPv4 address. For example, enter <b>254</b> to discover up to <b>192.168.0.254</b> .
IPv4/DNS Name List IPv6/DNS Name List	This setting is only visible if you select List of individual IP addresses and DNS names (IPv4) or List of individual IP addresses and DNS names (IPv6) above. Enter a list of IP addresses or DNS names that the auto-discovery scans. Enter each address on a separate line.
IPv4 and Subnet (IPv4)	This setting is only visible if you select IP address and subnet (IPv4) above. Enter an expression in the format address/subnet, for example, <b>192.168.3.0/255.255.255.0</b> . You can also use the short form like <b>192.168.3.0/24</b> . PRTG scans the complete host range (without network and broadcast address) that is defined by the IP address and the subnet mask.
IP Address with Octet Range	This setting is only visible if you select IP address with octet range (IPv4) above. Enter an expression in the format a1.a2.a3.a4, where <b>a1</b> , <b>a2</b> , <b>a3</b> , and <b>a4</b> are each a number between 0-255, or a range with two numbers and a hyphen like <b>1-127</b> . PRTG calculates all permutations of all ranges. For example, <b>10.0.1-10.1-100</b> results in 1,000 IP addresses that PRTG scans during the auto-discovery.
Organizational Unit	<p>This setting is only visible if you select Use computers from the Active Directory (maximum 1000 computers) above. Enter an <b>organizational unit (OU)</b> to restrict the Active Directory search to computers that are part of this OU. For top-level OUs, use the distinguished name (DN) format without <b>OU=</b> and without the domain components (DCS). If you leave this field empty, there are not any restrictions.</p> <p>Example:</p> <ul style="list-style-type: none"> <li>For the DN <b>OU=Domain Controllers,DC=example,DC=com</b>, enter only <b>Domain Controllers</b>.</li> </ul> <p>If you have sub-OUs, use the DN format without the leading <b>OU=</b> and without the DCs.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li>For the DN <b>OU=webserver,OU=production,DC=example,DC=com</b>, enter only <b>webserver,OU=production</b>.</li> <li>For the DN <b>OU=intranet,OU=webserver,OU=production,DC=example,DC=com</b>, enter only <b>intranet,OU=webserver,OU=production</b>.</li> </ul> <p><b>i</b> Make sure that the OU contains computer accounts. If the OU is empty, you receive an error message.</p>

Setting	Description
	<p> Do not enter the domain components. PRTG automatically uses the domain components from the domain name you enter in the <a href="#">Core &amp; Probes</a> settings.</p>
Name Resolution	<p>Select how to monitor newly discovered devices. This only affects <a href="#">new</a> devices. This does not change the setting for other devices. Depending on your selection, the IP Address/DNS Name field of an <a href="#">added device</a> shows the DNS name or IP address that PRTG uses to access the target device. Choose between:</p> <ul style="list-style-type: none"> <li>▪ Use DNS names (recommended): Monitor newly discovered devices via their DNS names (if available). We recommend that you use this option.</li> <li>▪ Use IP addresses: Monitor newly discovered devices via their IP addresses.</li> </ul> <p> This setting does not affect how PRTG shows the devices in the device tree.</p>
Device Rescan	<p>Select how to handle known devices:</p> <ul style="list-style-type: none"> <li>▪ Skip auto-discovery for existing devices/IP addresses (recommended): Do not rescan existing devices or IP addresses. PRTG only adds devices with new IP addresses or DNS names. PRTG does not add devices that already exist in your configuration for example, in other groups. We recommend that you use this option.</li> <li>▪ Perform auto-discovery for existing devices/IP addresses: Rescan devices that have existing IP addresses with every auto-discovery. PRTG adds devices that already exist in other groups to this group and runs the auto-discovery on the newly added devices. <ul style="list-style-type: none"> <li> The auto-discovery does not run on devices that already exist in the group. If you want to run the auto-discovery for these devices, you must manually start the auto-discovery on them.</li> </ul> </li> </ul> <p> In certain cases, the IP resolution might not work and might result in PRTG not adding a device if it has the same local IP address as it does in a different LAN.</p>

## 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](#) 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](#).


## Location

Click  to interrupt the [inheritance](#) <sup>[135]</sup>.


### Location

☐ inherit from

Location (for Geo Maps) <sup>[3]</sup>



Location

Setting	Description
Location (for Geo Maps)	<p>If you want to use <a href="#">Geo Maps</a> <sup>[3169]</sup>, 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 <a href="#">sensor status icons</a> <sup>[179]</sup> (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 <a href="#">49.452778 11.077778</a>, or <a href="#">enter 49.452778 any 11.077778 text</a>.</p> <p>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.</p> <p>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.</p> <p> The preview map always has a road map layout regardless of the map layout you set in <a href="#">User Interface</a> <sup>[6297]</sup>.</p>

## Credentials for Windows Systems

Click  to interrupt the [inheritance](#) <sup>[135]</sup>.

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

<ul style="list-style-type: none"> <li>▪ <a href="#">Active Directory Replication Errors</a></li> <li>▪ <a href="#">Event Log (Windows API)</a></li> <li>▪ <a href="#">Exchange Backup (PowerShell)</a></li> <li>▪ <a href="#">Exchange Database (PowerShell)</a></li> <li>▪ <a href="#">Exchange Database DAG (PowerShell)</a></li> <li>▪ <a href="#">Exchange Mail Queue (PowerShell)</a></li> <li>▪ <a href="#">Exchange Mailbox (PowerShell)</a></li> <li>▪ <a href="#">Exchange Public Folder (PowerShell)</a></li> <li>▪ <a href="#">File</a></li> <li>▪ <a href="#">File Content</a></li> <li>▪ <a href="#">Folder</a></li> <li>▪ <a href="#">Hyper-V Cluster Shared Volume Disk Free</a></li> <li>▪ <a href="#">Hyper-V Host Server</a></li> <li>▪ <a href="#">Hyper-V Virtual Machine</a></li> <li>▪ <a href="#">Hyper-V Virtual Network Adapter</a></li> <li>▪ <a href="#">Hyper-V Virtual Storage Device</a></li> <li>▪ <a href="#">PerfCounter Custom</a></li> <li>▪ <a href="#">PerfCounter IIS Application Pool</a></li> <li>▪ <a href="#">Share Disk Free</a></li> <li>▪ <a href="#">Windows CPU Load</a></li> <li>▪ <a href="#">Windows IIS 6.0 SMTP Received</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">Windows IIS 6.0 SMTP Sent</a></li> <li>▪ <a href="#">Windows IIS Application</a></li> <li>▪ <a href="#">Windows MSMQ Queue Length</a></li> <li>▪ <a href="#">Windows Network Card</a></li> <li>▪ <a href="#">Windows Pagefile</a></li> <li>▪ <a href="#">Windows Physical Disk I/O</a></li> <li>▪ <a href="#">Windows Print Queue</a></li> <li>▪ <a href="#">Windows Process</a></li> <li>▪ <a href="#">Windows System Uptime</a></li> <li>▪ <a href="#">Windows Updates Status (PowerShell)</a></li> <li>▪ <a href="#">WMI Battery</a></li> <li>▪ <a href="#">WMI Custom</a></li> <li>▪ <a href="#">WMI Custom String</a></li> <li>▪ <a href="#">WMI Disk Health</a></li> <li>▪ <a href="#">WMI Event Log</a></li> <li>▪ <a href="#">WMI Exchange Server</a></li> <li>▪ <a href="#">WMI Exchange Transport Queue</a></li> <li>▪ <a href="#">WMI File</a></li> <li>▪ <a href="#">WMI Free Disk Space (Multi Disk)</a></li> <li>▪ <a href="#">WMI HDD Health</a></li> <li>▪ <a href="#">WMI Logical Disk I/O</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">WMI Memory</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2005 (Deprecated)</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2008</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2012</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2014</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2016</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2017</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2019</a></li> <li>▪ <a href="#">WMI Remote Ping</a></li> <li>▪ <a href="#">WMI Security Center</a></li> <li>▪ <a href="#">WMI Service</a></li> <li>▪ <a href="#">WMI Share</a></li> <li>▪ <a href="#">WMI SharePoint Process</a></li> <li>▪ <a href="#">WMI Storage Pool</a></li> <li>▪ <a href="#">WMI Terminal Services (Windows 2008+)</a></li> <li>▪ <a href="#">WMI Terminal Services (Windows XP/Vista/2003)</a></li> <li>▪ <a href="#">WMI UTC Time</a></li> <li>▪ <a href="#">WMI Vital System Data v2</a></li> <li>▪ <a href="#">WMI Volume</a></li> <li>▪ <a href="#">WSUS Statistics</a></li> </ul>
--	---	---

## Credentials for Windows Systems



inherit from

Domain or Computer Name <sup>i</sup>

www.example.com

User Name <sup>i</sup>

johnqpublic

Password <sup>i</sup>

.....

Credentials for Windows Systems

Setting	Description
Domain or Computer Name	<p>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.</p> <p>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.</p>
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](#) <sup>135</sup>.

 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	<p>Select the authentication method for the login:</p> <ul style="list-style-type: none"> <li>▪ Password: Provide the password for the login.</li> <li>▪ Private key: Provide an RSA private key for authentication.</li> </ul> <p> PRTG can only handle keys in the OpenSSH format that are not encrypted. You cannot use password-protected keys.</p> <p> PRTG only supports RSA keys. It does not support DSA keys.</p> <p> For details, see section <a href="#">Monitoring via SSH</a> <sup>6437</sup>.</p>
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	<p>This setting is only visible if you select Private key above. Paste the entire RSA private key, including the <b>BEGIN</b> and <b>END</b> lines. Make sure that a corresponding public key exists on the target device.</p> <p> PRTG can only handle keys in the OpenSSH format that are not encrypted. You cannot use password-protected keys.</p> <p> PRTG only supports RSA keys. It does not support DSA keys.</p> <p> For details, see section <a href="#">Monitoring via SSH</a> <sup>6437</sup>.</p> <p> If you do not insert a private key for the first time but if you want to <a href="#">change</a> the private key, you need to <a href="#">restart the PRTG core server service</a> <sup>6352</sup> for the private key change to take effect.</p>
WBEM Protocol	<p>Select the protocol that you want to use for the connection to the system via WBEM:</p> <ul style="list-style-type: none"> <li>▪ HTTP: Use an unsecure connection for WBEM.</li> <li>▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection for WBEM.</li> </ul> <p> This setting is only relevant if you use WBEM sensors.</p>
WBEM Port	<p>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:</p> <ul style="list-style-type: none"> <li>▪ Default: Use one of the default ports. The default port for unsecure connections is <b>5988</b> and the default port for secure connections is <b>5989</b>.</li> <li>▪ Custom: Use a custom port.</li> </ul>

Setting	Description
	<p> This setting is only relevant if you use WBEM sensors.</p>
Custom WBEM Port	This setting is only visible if you select Custom above. Enter a custom WBEM port. Enter an integer.
SSH Port	<p>Enter the port for SSH connections. Enter an integer. The default port is <a href="#">22</a>.</p> <p> By default, PRTG automatically uses this setting for all <a href="#">SSH sensors</a> <sup>[6683]</sup> unless you define a different port number in the sensor settings.</p>
SSH Rights Elevation	<p>Select the rights that you want to use to run the command on the target system:</p> <ul style="list-style-type: none"> <li>▪ Run the command as the connecting user (default): Use the rights of the user who establishes the SSH connection.</li> <li>▪ Run the command as a different user using 'sudo' (with password): Use the rights of a different user with a password required for <a href="#">sudo</a> to run commands on the target system, for example, as a root user.</li> <li>▪ Run the command as a different user using 'sudo' (without password): Use the rights of a different user without a password required for <a href="#">sudo</a> to run commands on the target system, for example, as a root user.</li> <li>▪ Run the command as a different user using 'su': Use the rights of a different user with <a href="#">su</a> to run commands on the target system.</li> </ul>
Target System User Name	<p>This setting is only visible if you select an option that includes <a href="#">sudo</a> or <a href="#">su</a> 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.</p>
Password	<p>This setting is only visible if you select an option that includes <a href="#">sudo</a> or <a href="#">su</a> with password above. Enter the password to run the <a href="#">sudo</a> command or the <a href="#">su</a> command.</p>
SSH Connection Mode	<p>Select the connection mode that you want to use to <a href="#">access data with SSH sensors</a> <sup>[3437]</sup>:</p> <ul style="list-style-type: none"> <li>▪ Default (recommended): This is the default connection mode for SSH sensors. It provides the best performance and security.</li> <li>▪ 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.</li> </ul>

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


## Credentials for VMware/XenServer


Click  to interrupt the [inheritance](#) .


 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** 

**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	<p>Enter the password for access to VMware ESXi, vCenter Server, or Citrix XenServer. Usually, you use credentials with administrator rights.</p> <p> Single sign-on (SSO) passwords for vSphere do not support special characters. For details, see the VMware sensors sections.</p>
VMware Protocol	<p>Select the protocol for the connection to VMware ESXi, vCenter Server, or Citrix XenServer:</p> <ul style="list-style-type: none"> <li>▪ HTTPS (recommended): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection.</li> <li>▪ HTTP: Use an unsecure connection.</li> </ul>
Session Handling	<p>Select if you want to reuse a session for VMware sensors:</p> <ul style="list-style-type: none"> <li>▪ 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.</li> <li>▪ 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.</li> </ul>

## Credentials for SNMP Devices

Click  to interrupt the [inheritance](#) .

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

<ul style="list-style-type: none"> <li>▪ <a href="#">Cisco IP SLA</a></li> <li>▪ <a href="#">SNMP APC Hardware</a></li> <li>▪ <a href="#">SNMP Buffalo TS System Health</a></li> <li>▪ <a href="#">SNMP Cisco ADSL</a></li> <li>▪ <a href="#">SNMP Cisco ASA VPN Connections</a></li> <li>▪ <a href="#">SNMP Cisco ASA VPN Traffic</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">SNMP Fujitsu System Health v2</a></li> <li>▪ <a href="#">SNMP Hardware Status</a></li> <li>▪ <a href="#">SNMP HP LaserJet Hardware</a></li> <li>▪ <a href="#">SNMP HPE BladeSystem Blade</a></li> <li>▪ <a href="#">SNMP HPE BladeSystem Enclosure System Health</a></li> <li>▪ <a href="#">SNMP HPE ProLiant Logical Disk</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">SNMP NetApp Enclosure</a></li> <li>▪ <a href="#">SNMP NetApp I/O</a></li> <li>▪ <a href="#">SNMP NetApp License</a></li> <li>▪ <a href="#">SNMP NetApp Logical Unit</a></li> <li>▪ <a href="#">SNMP NetApp Network Interface</a></li> <li>▪ <a href="#">SNMP NetApp System Health</a></li> <li>▪ <a href="#">SNMP Nutanix Cluster Health</a></li> </ul>
---	--	--

- |   |   |  |
|---|---|--|
| <ul style="list-style-type: none"> <li>▪ <a href="#">SNMP Cisco ASA VPN Users</a></li> <li>▪ <a href="#">SNMP Cisco CBQoS</a></li> <li>▪ <a href="#">SNMP Cisco System Health</a></li> <li>▪ <a href="#">SNMP Cisco UCS Blade</a></li> <li>▪ <a href="#">SNMP Cisco UCS Chassis</a></li> <li>▪ <a href="#">SNMP Cisco UCS Physical Disk</a></li> <li>▪ <a href="#">SNMP Cisco UCS System Health</a></li> <li>▪ <a href="#">SNMP CPU Load</a></li> <li>▪ <a href="#">SNMP Custom</a></li> <li>▪ <a href="#">SNMP Custom Advanced</a></li> <li>▪ <a href="#">SNMP Custom String</a></li> <li>▪ <a href="#">SNMP Custom String Lookup</a></li> <li>▪ <a href="#">SNMP Custom Table</a></li> <li>▪ <a href="#">SNMP Dell EqualLogic Logical Disk</a></li> <li>▪ <a href="#">SNMP Dell EqualLogic Member Health</a></li> <li>▪ <a href="#">SNMP Dell EqualLogic Physical Disk</a></li> <li>▪ <a href="#">SNMP Dell Hardware</a></li> <li>▪ <a href="#">SNMP Dell PowerEdge Physical Disk</a></li> <li>▪ <a href="#">SNMP Dell PowerEdge System Health</a></li> <li>▪ <a href="#">SNMP Disk Free</a></li> </ul> | <ul style="list-style-type: none"> <li>▪ <a href="#">SNMP HPE ProLiant Memory Controller</a></li> <li>▪ <a href="#">SNMP HPE ProLiant Network Interface</a></li> <li>▪ <a href="#">SNMP HPE ProLiant Physical Disk</a></li> <li>▪ <a href="#">SNMP HPE ProLiant System Health</a></li> <li>▪ <a href="#">SNMP IBM System X Logical Disk</a></li> <li>▪ <a href="#">SNMP IBM System X Physical Disk</a></li> <li>▪ <a href="#">SNMP IBM System X Physical Memory</a></li> <li>▪ <a href="#">SNMP IBM System X System Health</a></li> <li>▪ <a href="#">SNMP interSeptor Pro Environment</a></li> <li>▪ <a href="#">SNMP Juniper NS System Health</a></li> <li>▪ <a href="#">SNMP LenovoEMC Physical Disk</a></li> <li>▪ <a href="#">SNMP LenovoEMC System Health</a></li> <li>▪ <a href="#">SNMP Library</a></li> <li>▪ <a href="#">SNMP Linux Disk Free</a></li> <li>▪ <a href="#">SNMP Linux Load Average</a></li> <li>▪ <a href="#">SNMP Linux Meminfo</a></li> <li>▪ <a href="#">SNMP Linux Physical Disk</a></li> <li>▪ <a href="#">SNMP Memory</a></li> <li>▪ <a href="#">SNMP NetApp Disk Free</a></li> </ul> | <ul style="list-style-type: none"> <li>▪ <a href="#">SNMP Nutanix Hypervisor</a></li> <li>▪ <a href="#">SNMP Poseidon Environment</a></li> <li>▪ <a href="#">SNMP Printer</a></li> <li>▪ <a href="#">SNMP QNAP Logical Disk</a></li> <li>▪ <a href="#">SNMP QNAP Physical Disk</a></li> <li>▪ <a href="#">SNMP QNAP System Health</a></li> <li>▪ <a href="#">SNMP Rittal CMC III Hardware Status</a></li> <li>▪ <a href="#">SNMP RMON</a></li> <li>▪ <a href="#">SNMP SonicWall System Health</a></li> <li>▪ <a href="#">SNMP SonicWall VPN Traffic</a></li> <li>▪ <a href="#">SNMP Synology Logical Disk</a></li> <li>▪ <a href="#">SNMP Synology Physical Disk</a></li> <li>▪ <a href="#">SNMP Synology System Health</a></li> <li>▪ <a href="#">SNMP System Uptime</a></li> <li>▪ <a href="#">SNMP Traffic</a></li> <li>▪ <a href="#">SNMP Trap Receiver</a></li> <li>▪ <a href="#">SNMP Windows Service</a></li> </ul> |
|---|---|--|

## 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	<p>Select the Simple Network Management Protocol (SNMP) version for the connection to the target SNMP device:</p> <ul style="list-style-type: none"> <li>▪ <b>SNMP v1:</b> Use SNMP v1 for the connection. SNMP v1 only offers clear-text data transmission.  <input checked="" type="radio"/> <b>SNMP v1</b> does not support 64-bit counters. This might result in invalid data when you monitor traffic via SNMP.</li> <li>▪ <b>SNMP v2c (recommended):</b> Use SNMP v2c for the connection. SNMP v2c also only offers clear-text data transmission but it supports 64-bit counters.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>SNMP v3: Use SNMP v3 for the connection. SNMP v3 provides secure authentication and data encryption.</li> </ul> <p><b>i</b> 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 <a href="#">Interval Delay</a> or <a href="#">Open Requests</a> with the <a href="#">Probe Health</a> sensor, distribute the load over <a href="#">multiple probes</a> <sup>[362]</sup>. SNMP v1 and SNMP v2c do not have this limitation.</p>
Community String	<p>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.</p> <p><b>i</b> We recommend that you use the default value.</p>
Authentication Method	<p>This setting is only visible if you select SNMP v3 above. Select the authentication method:</p> <ul style="list-style-type: none"> <li>MD5: Use message-digest algorithm 5 (MD5) for authentication.</li> <li>SHA: Use Secure Hash Algorithm (SHA) for authentication.</li> <li>SHA-224: Use SHA-224 for authentication.</li> <li>SHA-256: Use SHA-256 for authentication.</li> <li>SHA-384: Use SHA-384 for authentication.</li> <li>SHA-512: Use SHA-512 for authentication.</li> </ul> <p><b>i</b> If you do not want to use authentication but you need SNMP v3, for example, because your device requires <a href="#">context</a>, you can leave the Password field empty. In this case, PRTG uses <a href="#">SNMP_SEC_LEVEL_NOAUTH</a> and it entirely deactivates authentication.</p> <p><b>i</b> The authentication method you select must match the authentication method of your device.</p>
User Name	<p>This setting is only visible if you select SNMP v3 above. Enter the user name for access to the target SNMP device.</p> <p><b>i</b> The user name that you enter must match the user name of your device.</p>
Password	<p>This setting is only visible if you select SNMP v3 above. Enter the password for access to the target SNMP device.</p> <p><b>i</b> The password that you enter must match the password of your device.</p>



Setting	Description
Encryption Type	<p>This setting is only visible if you select SNMP v3 above. Select an encryption type:</p> <ul style="list-style-type: none"> <li>▪ DES: Use Data Encryption Standard (DES) as the encryption algorithm.</li> <li>▪ AES: Use Advanced Encryption Standard (AES) as the encryption algorithm.</li> <li>▪ AES-192: Use AES-192 as the encryption algorithm.</li> <li>▪ AES-256: Use AES-256 as the encryption algorithm.</li> </ul> <p> The encryption type that you select must match the encryption type of your device.</p>
Encryption Key	<p>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.</p> <p> 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.</p>
Context Name	<p>This setting is only visible if you select SNMP v3 above. Enter a context name only if the configuration of the device requires it. <a href="#">Context</a> is a collection of management information that is accessible by an SNMP device. Enter a string.</p>
SNMP Port	<p>Enter the port for the connection to the SNMP target device. Enter an integer. The default port is <a href="#">161</a>.</p> <p> We recommend that you use the default value.</p>
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <a href="#">300</a> seconds (5 minutes).</p>

## Credentials for Database Management Systems

Click  to interrupt the [inheritance](#) <sup>135</sup>.

 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	Enter a custom port for database connections. Enter an integer. ⓘ PRTG uses this custom port for <a href="#">all</a> database sensors and for connections to <a href="#">all</a> your databases.
Custom Port	Enter a custom port for database connections. Enter an integer. ⓘ PRTG uses this custom port for <a href="#">all</a> database sensors and for connections to <a href="#">all</a> your databases.
Authentication Method	This setting is only visible if you select SQL server authentication above. Enter the user name for the database connection.
User Name	This setting is only visible if you select SQL server authentication above. Enter the password for the database connection.

Setting	Description
Password	Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is 300 seconds (5 minutes).
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](#)<sup>135</sup>.

**i** 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** **i**

**Secret Key** **i**

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](#) .

 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: <ul style="list-style-type: none"> <li>Automatic (default): PRTG automatically determines the authorization endpoint URL and the token endpoint URL.</li> <li>Manual: Manually enter the authorization endpoint URL and the token endpoint URL.</li> </ul>
Authorization Endpoint	Enter the authorization endpoint URL including the server. Authorization endpoint URL example:

Setting	Description
	<p><code>https://login.microsoftonline.com/&lt;tenant-ID&gt;/oauth2/v2.0/authorize</code></p> <p>❶ Make sure to replace &lt;tenant-ID&gt; with the <b>directory (tenant) ID</b> from Azure AD.</p>
Token Endpoint	<p>Enter the token endpoint URL including the server.</p> <p>Token endpoint URL example:</p> <p><code>https://login.microsoftonline.com/&lt;tenant-ID&gt;/oauth2/v2.0/token</code></p> <p>❶ Make sure to replace &lt;tenant-ID&gt; with the <b>directory (tenant) ID</b> from Azure AD.</p>


## Credentials for Script Sensors

Click  to interrupt the [inheritance](#) <sup>135</sup>.

❶ 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 <code>%scriptplaceholder1</code> 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 <code>%scriptplaceholder2</code> 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 <code>%scriptplaceholder3</code> 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 <code>%scriptplaceholder4</code> 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 <code>%scriptplaceholder5</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.



## Credentials for Cisco Meraki

Click  to interrupt the [inheritance](#) <sup>135</sup>.

 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](https://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 <a href="https://api.meraki.com">api.meraki.com</a> should be valid for most use cases. ⓘ See the Cisco Meraki Dashboard API documentation for other possible choices.

## Credentials for Dell EMC

Click  to interrupt the [inheritance](#) .

ⓘ 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 <a href="#">443</a> .

## Credentials for FortiGate

Click  to interrupt the [inheritance](#) <sup>135</sup>.

ⓘ 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 <a href="#">443</a> .

## Credentials for HPE 3PAR

Click  to interrupt the [inheritance](#) <sup>135</sup>.

ⓘ 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: <ul style="list-style-type: none"> <li>▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection.</li> <li>▪ HTTP: Use an unsecure connection.</li> </ul>

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 <b>8080</b> and the default port for unsecure connections is <b>8008</b> .  <i>i</i> For more information, see the Knowledge Base: <a href="#">Where can I find the Web Services API (WSAPI) port for the connection to the HPE 3PAR system?</a>
SSH Port	Enter the SSH port for the connection to the HPE 3PAR system. The default port for secure connections is <b>22</b> .

## Credentials for HTTP

Click  to interrupt the [inheritance](#)<sup>135</sup>.

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

- [HTTP v2](#)

### Credentials for HTTP

Authentication Method *i*

☒ None (default)
☐ Basic authentication
☐ Bearer authentication

Placeholder 1 Description *i*

Placeholder 1 *i*

Credentials for HTTP

Setting	Description
Authentication Method	Select the authentication method for access to the server. Choose between: <ul style="list-style-type: none"> <li>▪ None (default): Use no authentication.</li> <li>▪ Basic authentication: Use basic authentication.</li> <li>▪ Bearer authentication: Use an OAuth2 bearer token.</li> </ul>
User Name	This setting is only visible if you select Basic authentication above. Enter the user name for access to the server.

Setting	Description
Password	This setting is only visible if you select Basic authentication above. Enter the password for access to the server.
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 <code>%httpplaceholder1</code> 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 <code>%httpplaceholder2</code> 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 <code>%httpplaceholder3</code> 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 <code>%httpplaceholder4</code> 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 <code>%httpplaceholder5</code> 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

Click  to interrupt the [inheritance](#) <sup>135</sup>.


 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.
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

Click  to interrupt the [inheritance](#)  <sup>135</sup>.

 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 <sup>i</sup>

☒ None (default)

☐ Username/Password

### Port <sup>i</sup>

1883

### Transport-Level Security <sup>i</sup>




☒ Do not use transport-level security (default)

☐ Use transport-level security

Credentials for MQTT

Setting	Description
Authentication Method	<p>Select if you want to connect without credentials or define credentials for access to the MQTT broker.</p> <ul style="list-style-type: none"> <li>None (default): Connect without credentials.</li> <li>User name and password: Define credentials for the connection.</li> </ul>
User Name	<p>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.</p>
Password	<p>This setting is only visible if you select User name and password above. Enter the password for access to the MQTT broker.</p>
Port	<p>Enter the port for the connection to the MQTT broker. The default port for secure connections is <b>8883</b> and the default port for unsecure connections is <b>1883</b>.</p>



Setting	Description
Transport-Level Security	<p>Select if you want to use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection:</p> <ul style="list-style-type: none"> <li>Do not use transport-level security: Establish the connection without connection security.</li> <li>Use transport-level security: Establish the connection with the strongest SSL/TLS method that the target device provides.</li> </ul>
Server Authentication	<p>This setting is only visible if you select Use transport-level security above. Select if you want to use a certificate for server authentication.</p> <ul style="list-style-type: none"> <li>Disable (default): Do not use a certificate for server authentication.</li> <li>Enable: Use a certificate for server authentication.</li> </ul>
CA Certificate	<p>This setting is only visible if you enable Server Authentication above. Paste the certificate authority (CA) certificate for the verification of the MQTT broker.</p> <p> The certificate must be in Privacy-Enhanced Mail (PEM) format.</p>
Client Authentication	<p>This setting is only visible if you select Use transport-level security above. Select if you want to use a certificate for client authentication.</p> <ul style="list-style-type: none"> <li>Disable (default): Do not use a certificate for client authentication.</li> <li>Enable: Use a certificate for client authentication.</li> </ul>
Client Certificate	<p>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.</p> <p> The certificate must be in PEM format.</p>
Client Key	<p>This setting is only visible if you enable Client Authentication above. Enter the client key for access to the MQTT broker.</p> <p> The client key must be in PEM format and it must be encrypted using the Client Key Password.</p>
Client Key Password	<p>This setting is only visible if you enable Client Authentication above. Enter the password for the client key.</p>

## Credentials for NetApp

Click  to interrupt the [inheritance](#) 135.


 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 <a href="#">443</a> .
Protocol	<p>Select the protocol that you want to use for the connection to the ONTAP System Manager. Choose between:</p> <ul style="list-style-type: none"> <li>▪ HTTPS (default)</li> <li>▪ HTTP</li> </ul>

## Credentials for OPC UA

Click  to interrupt the [inheritance](#) <sup>135</sup>.

 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 <a href="#">4840</a> .
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	<p>Select if you want to use encryption:</p> <ul style="list-style-type: none"> <li>None (default): Do not use encryption.</li> <li>Sign: Sign messages between the sensor and the OPC UA server.</li> </ul>

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

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](#)  <sup>135</sup>.

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

- [Soffico Orchestra Channel Health](#)

## Credentials for Soffico Orchestra

☐ inherit from

### Authentication Method <sup>i</sup>

- ☒ None (default)
- ☐ User name and password

### Timeout (Sec.) <sup>i</sup>

60

### Port <sup>i</sup>

8443

### Protocol <sup>i</sup>

- ☒ HTTPS (default)
- ☐ HTTP

Credentials for Soffico Orchestra

Setting	Description
Authentication Method	<p>Select if you want to connect without credentials or define credentials for access to the Orchestra platform:</p> <ul style="list-style-type: none"> <li>▪ None (default): Connect without credentials.</li> <li>▪ User name and password: Define credentials for the connection.</li> </ul>
User Name	<p>This setting is only visible if you select User name and password above. Enter the user name for access to the Orchestra platform.</p>
Password	<p>This setting is only visible if you select User name and password above. Enter the password for access to the Orchestra platform.</p>

Setting	Description
Timeout (Sec.)	Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>300</b> seconds (5 minutes).
Port	Enter the port for the connection to the Orchestra platform. The default port for secure connections is <b>8443</b> and the default port for unsecure connections is <b>8019</b> .
Protocol	<p>Select the protocol that you want to use for the connection to the Orchestra platform:</p> <ul style="list-style-type: none"> <li>▪ <b>HTTPS (default):</b> Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection.</li> <li>▪ <b>HTTP:</b> Use an unsecure connection.</li> </ul>

## Credentials for Redfish

Click  to interrupt the [inheritance](#) .

 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	<p>Select the protocol that you want to use for the connection to the Redfish system. Choose between:</p> <ul style="list-style-type: none"> <li>HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection.</li> <li>HTTP: Use an unsecured connection.</li> </ul>
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](#) <sup>135</sup>.

 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	<p>Select the authentication method for access to the Representational State Transfer (REST) application programming interface (API):</p> <ul style="list-style-type: none"> <li>▪ None (default): Use no authentication.</li> <li>▪ Basic authentication: Use basic authentication.</li> <li>▪ Bearer authentication: Use an OAuth2 bearer token.</li> </ul>
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 <code>%restplaceholder1</code> 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 <code>%restplaceholder2</code> 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 <a href="#">%restplaceholder3</a> 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 <a href="#">%restplaceholder4</a> 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 <a href="#">%restplaceholder5</a> 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](#) <sup>135</sup>.

 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 <a href="#">9398</a> .

## Windows Compatibility Options

Click  to interrupt the [inheritance](#)<sup>135</sup>.

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

Windows Compatibility Options

Setting	Description
Preferred Data Source	<p>ⓘ 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.</p> <p>Define the method that Windows sensors use to query data:</p> <ul style="list-style-type: none"> <li>▪ Performance counters and WMI as fallback: Try to query data via performance counters. If this is not possible, establish a connection via WMI.</li> <li>▪ Performance counters only: Query data via performance counters only. If this is not possible, the sensor returns no data.</li> <li>▪ 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.</li> </ul>
Timeout Method	<p>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:</p> <ul style="list-style-type: none"> <li>▪ Use 1.5× scanning interval (recommended): Multiply the scanning interval of the sensor by 1.5 and use the resulting value.</li> <li>▪ Set manually: Manually enter a timeout value.</li> </ul>

Setting	Description
	<p> We recommend that you use the default value.</p> <p> If you experience ongoing timeout errors, try increasing the timeout value.</p>
Timeout (Sec.)	<p>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).</p>

## SNMP Compatibility Options

Click  to interrupt the [inheritance](#)<sup>135</sup>.

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

## SNMP Compatibility Options

☒ inherit from

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

Setting	Description
SNMP Delay (ms)	<p>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.</p> <p><b>i</b> We recommend that you use the default value.</p> <p><b>i</b> If you experience SNMP connection failures, try increasing the delay.</p>
Failed Requests	<p>Select if an SNMP sensor tries again after a request fails:</p> <ul style="list-style-type: none"> <li>▪ <b>Retry (recommended):</b> Try again if an SNMP request fails. This can prevent false error messages because of temporary timeout failures.</li> <li>▪ <b>Do not retry:</b> Do not retry if an SNMP request fails. If you select this option, an SNMP sensor shows a Down status earlier.</li> </ul>
Overflow Values	<p>Select how PRTG handles overflow values. Some devices do not correctly handle internal buffer overflows. This can cause false peaks.</p> <ul style="list-style-type: none"> <li>▪ <b>Ignore (default):</b> Ignore overflow values and do not include them in the monitoring data. We recommend that you use this option.</li> <li>▪ <b>Handle overflow values as valid results:</b> Regard all overflow values as regular data and include them in the monitoring data.</li> </ul> <p><b>i</b> 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: <a href="#">What is the Overflow Values setting in the SNMP Compatibility Options?</a></p>
Zero Values	<p>Select how PRTG handles zero values. Some devices send incorrect zero values. This can cause false peaks.</p> <ul style="list-style-type: none"> <li>▪ <b>Ignore (recommended):</b> Ignore zero values and do not include them in the monitoring data. We recommend that you use this option.</li> <li>▪ <b>Handle zero values as valid results for delta sensors:</b> Regard all zero values as regular data and include them in the monitoring data.</li> </ul> <p><b>i</b> If you experience problems, try changing this option.</p>
32-bit/64-bit Counters	<p>Select the type of traffic counters that PRTG searches for on a device:</p> <ul style="list-style-type: none"> <li>▪ <b>Use 64-bit counters if available (recommended):</b> The interface scan uses 64-bit traffic counters, if available. This can avoid buffer overflows in the devices</li> </ul> <p><b>i</b> We recommend that you use the default value.</p> <p><b>i</b> If you experience problems, try changing this option.</p>



Setting	Description
	<ul style="list-style-type: none"> <li>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.</li> </ul>
Request Mode	<p>Select the request method that PRTG uses for SNMP sensors:</p> <ul style="list-style-type: none"> <li>Use multi get (recommended): Bundle multiple SNMP requests into one request. We recommend that you use this option. <ul style="list-style-type: none"> <li> If you experience problems, try changing this option.</li> </ul> </li> <li>Use single get: Use one request for each SNMP value. This can increase compatibility with older devices.</li> </ul> <p> PRTG uses <a href="#">paging</a> 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.</p>
Walk Mode	<p>Select the kind of SNMP walk that PRTG uses for SNMP sensors:</p> <ul style="list-style-type: none"> <li>Use GETBULK requests (recommended): Request the next <a href="#">x</a> OIDs in one SNMP request. The default value is <a href="#">10</a>. It is dynamic based on the response size. <ul style="list-style-type: none"> <li> 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 <a href="#">object hierarchy</a><sup>[131]</sup>.</li> </ul> </li> <li>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.</li> </ul>
Port Name Template	<p>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 <a href="#">([port]) [ifalias] [ifsensor]</a>, which creates a name like <a href="#">(001) Ethernet1 Traffic</a>. You can use and combine any field names that are available at an OID of your device, for example:</p> <ul style="list-style-type: none"> <li><a href="#">[port]</a>: The port number of the monitored interface.</li> <li><a href="#">[ifalias]</a>: The 'alias' name for the monitored interface as specified by a network manager, providing a non-volatile handling.</li> <li><a href="#">[ifname]</a>: The textual name of the monitored interface as assigned by the local device.</li> <li><a href="#">[ifdescr]</a>: A textual string containing information about the target device or interface, for example, manufacturer, product name, or version.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ [ifspeed]: An estimate of the monitored interface's current bandwidth (Kbit/s).</li> <li>▪ [ifsensor]: The type of the sensor, this is <a href="#">Traffic</a> or <a href="#">RMON</a>. This helps to differentiate between <a href="#">SNMP Traffic</a> and <a href="#">SNMP RMON</a> sensors.</li> </ul> <p> For more information about SNMP sensor names, see the Knowledge Base: <a href="#">How can I change the defaults for names automatically generated for new SNMP sensors?</a></p>
Port Name Update	<p>Select how PRTG reacts if you change the names of ports in your physical device (for example, a switch or router):</p> <ul style="list-style-type: none"> <li>▪ 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.</li> <li>▪ 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.</li> </ul> <p> For more information about automatic name updates, see the Knowledge Base: <a href="#">Automatically update port name and number for SNMP Traffic sensors when the device changes them.</a></p>
Port Identification	<p>Select the field that PRTG uses for SNMP interface identification:</p> <ul style="list-style-type: none"> <li>▪ Automatic identification (recommended): Try the ifAlias field first to identify an SNMP interface and then try ifDescr.  PRTG does not automatically try ifName.</li> <li>▪ Use ifAlias: For most devices, ifAlias is the best field to use for unique interface names.</li> <li>▪ 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.</li> <li>▪ 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.</li> <li>▪ Do not update ports: Use this option to disable the automatic port identification.</li> </ul>
Start Interface Index	<p> This setting only applies to <a href="#">SNMP Traffic sensors</a> and to <a href="#">Cisco IP SLA sensors</a>.</p> <p>Enter the index at which PRTG starts to query the interface range during sensor creation. Enter <b>0</b> for the automatic mode.</p>

Setting	Description
	<p>❗ We recommend that you use the default value.</p>
End Interface Index	<p>❗ This setting only applies to <a href="#">SNMP Traffic sensors</a> and to <a href="#">Cisco IP SLA sensors</a>.</p> <p>Enter the index at which PRTG stops querying the interface range during sensor creation. Enter 0 for the automatic mode.</p> <p>❗ We recommend that you use the default value.</p>

## Proxy Settings for HTTP Sensors

Click  to interrupt the [inheritance](#) <sup>135</sup>.

❗ 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](#) <sup>8325</sup>.

❗ 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



inherit from

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 <b>8080</b> . Enter an integer.
User Name	<p>If the proxy requires authentication, enter the user name for the proxy login.</p> <p>ⓘ Only basic authentication is available. Enter a string or leave the field empty.</p>
Password	If the proxy requires authentication, enter the password for the proxy login.


Setting	Description
	 Only basic authentication is available. Enter a string or leave the field empty.


## Scanning Interval


Click  to interrupt the [inheritance](#)  <sup>135</sup>.


### Scanning Interval

 inherit from

**Scanning Interval** 





60 seconds 

**If a Sensor Query Fails** 

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

Scanning Interval

Setting	Description
Scanning Interval	<p>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:</p> <ul style="list-style-type: none"> <li>▪ 30 seconds</li> <li>▪ 60 seconds</li> <li>▪ 5 minutes</li> <li>▪ 10 minutes</li> <li>▪ 15 minutes</li> <li>▪ 30 minutes</li> <li>▪ 1 hour</li> <li>▪ 4 hours</li> <li>▪ 6 hours</li> <li>▪ 12 hours</li> <li>▪ 24 hours</li> </ul>

Setting	Description
	<p> You can change the available intervals in the <a href="#">system administration</a><sup>[3307]</sup> of PRTG Network Monitor.</p>
If a Sensor Query Fails	<p>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 <a href="#">status</a><sup>[179]</sup>. 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:</p> <ul style="list-style-type: none"> <li>▪ Set sensor to down status immediately: Set the sensor to the Down status immediately after the first request fails.</li> <li>▪ 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.</li> <li>▪ 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.</li> <li>▪ 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.</li> <li>▪ 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.</li> <li>▪ 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.</li> </ul> <p> 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.</p> <p> If you define error limits for a sensor's channels, the sensor immediately shows the Down status. None of the interval options apply.</p> <p> If a channel uses <a href="#">lookup</a><sup>[3604]</sup> values, the sensor immediately shows the Down status. None of the interval options apply.</p>

## Schedules, Dependencies, and Maintenance Window

Click  to interrupt the [inheritance](#)<sup>[135]</sup>.

## Schedules, Dependencies, and Maintenance Window

☐ inherit from

**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

### Dependency Type ⓘ

- ☒ Use parent
- ☐ Select a sensor

Schedules, Dependencies, and Maintenance Window

Setting	Description
Schedule	<p>Select a schedule from the list. You can use schedules to monitor during a certain time span (days or hours) every week. Choose from:</p> <ul style="list-style-type: none"> <li>▪ None</li> <li>▪ Saturdays</li> <li>▪ Sundays</li> <li>▪ Weekdays</li> <li>▪ Weekdays Eight-To-Eight (08:00 - 20:00)</li> <li>▪ Weekdays Nights (17:00 - 09:00)</li> <li>▪ Weekdays Nights (20:00 - 08:00)</li> <li>▪ Weekdays Nine-To-Five (09:00 - 17:00)</li> <li>▪ Weekends</li> </ul> <p> ⓘ You can create schedules, edit schedules, or pause monitoring for a specific time span. For more information, see section <a href="#">Schedules</a> <sup>3286</sup>.</p>
Maintenance Window	<p>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:</p>

Setting	Description
	<ul style="list-style-type: none"> <li>Do not set up a one-time maintenance window: Do not set up a one-time maintenance window. Monitoring is always active.</li> <li>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.</li> </ul> <p><b>i</b> To terminate an active maintenance window before the defined end date, change the time entry in Maintenance Ends to a date in the past.</p>
Maintenance Begins	<p>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:</p> <ul style="list-style-type: none"> <li>Do not set up a one-time maintenance window: Do not set up a one-time maintenance window. Monitoring is always active.</li> <li>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.</li> </ul>
Maintenance Ends	<p>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.</p>
Dependency Type	<p>Select a dependency type. You can use dependencies to pause monitoring for an object depending on the status of a different object. You can choose from:</p> <ul style="list-style-type: none"> <li>Use parent: Use the dependency type of the parent object.</li> <li>Select a sensor: Use the dependency type of the parent object. Additionally, pause the current object if a specific sensor is in the Down status or in the Paused status because of another dependency.</li> </ul> <p><b>i</b> You do not trigger a status change by dependency if you manually pause a master object or if you pause it by schedule.</p> <p><b>i</b> To test your <a href="#">dependencies</a> <sup>[3166]</sup>, select Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later, all dependent objects are paused. You can check all dependencies under Devices   Dependencies in the main menu bar.</p>
Dependency	<p>This setting is only visible if you enable Select a sensor above. Click  and use the <a href="#">object selector</a> <sup>[219]</sup> to select a sensor on which the current object will depend.</p>
Dependency Delay (Sec.)	<p>This setting is only visible if you select Select a sensor above. Define a time span in seconds for the dependency delay.</p>




Setting	Description
	After the master sensor for this dependency returns to the Up status, PRTG additionally delays the monitoring of the dependent objects by the time span you define. This can prevent false alarms, for example, after a server restart or to give systems more time for all services to start. Enter an integer.



## Access Rights

Click  to interrupt the [inheritance](#) .

### 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	<p>Select the <a href="#">user groups</a> <sup>134</sup> 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:</p> <ul style="list-style-type: none"> <li>▪ Inherited: Inherit the access rights settings of the parent object.</li> <li>▪ 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. <ul style="list-style-type: none"> <li>ⓘ 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.</li> </ul> </li> <li>▪ Read access: Users in this group can see the object and view its monitoring results. They cannot edit any settings.</li> <li>▪ 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.</li> <li>▪ Full access: Users in this group can see the object, view its monitoring results, edit its settings, and edit its access rights settings.</li> </ul> <p>To automatically set all child objects to inherit this object's access rights, enable the Revert access rights of child objects to "inherited" option.</p> <p> For more details on access rights, see section <a href="#">Access Rights Management</a> <sup>144</sup>.</p>









## Channel Unit Configuration

Click  to interrupt the [inheritance](#) <sup>135</sup>.


### Channel Unit Configuration

 inherit from

#### Channel Unit Types

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


Channel Unit Configuration

Setting	Description
Channel Unit Types	<p>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):</p> <ul style="list-style-type: none"><li>▪ Bandwidth</li><li>▪ Memory</li><li>▪ Disk</li><li>▪ File</li><li>▪ Custom</li></ul> <p> Custom channel types are only available on sensor level.</p>

## Advanced Network Analysis

Click  to interrupt the [inheritance](#) <sup>[135]</sup>.

### Advanced Network Analysis

 inherit from

#### Unusual Detection <sup>i</sup>

☒ Enable
 ☐ Disable

#### Similar Sensors Detection <sup>i</sup>

☒ Enable
 ☐ Disable

#### System Information <sup>i</sup>

☒ Enable
 ☐ Disable

Advanced Network Analysis

Setting	Description
Unusual Detection	<p>Select if you want to use the <a href="#">unusual detection</a> <sup>[3309]</sup> for sensors:</p> <ul style="list-style-type: none"> <li>▪ Enabled: Activates the unusual detection for this object and, by default, for all objects underneath in the <a href="#">object hierarchy</a> <sup>[131]</sup>. Sensors that are affected by this setting show the Unusual status if PRTG detects unusual activity.</li> <li>▪ 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.</li> </ul> <p><sup>i</sup> You can configure the behavior of the unusual detection or completely disable it in the <a href="#">system settings</a> <sup>[3309]</sup>.</p>

Setting	Description
Similar Sensors Detection	<p>Select if you want to activate the <a href="#">similar sensors</a><sup>[189]</sup> analysis:</p> <ul style="list-style-type: none"> <li>▪ 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.</li> <li>▪ Disabled: Does not activate the similar sensors detection. PRTG does not consider sensors that are affected by this setting during the similarity analysis.</li> </ul> <p><b>i</b> You can configure the depth of the analysis of the similar sensors detection or completely disable it in the <a href="#">system settings</a><sup>[331]</sup>.</p>
System Information	<p>Select if you want to retrieve and show <a href="#">system information</a><sup>[202]</sup> for your devices:</p> <ul style="list-style-type: none"> <li>▪ Enabled: Activates the system information feature for this object and, by default, for all objects underneath in the hierarchy.</li> <li>▪ Disabled: Does not activate the system information feature.</li> </ul> <p><b>i</b> The System Information feature is enabled by default. To retrieve the data, PRTG automatically uses the <a href="#">credentials for Windows systems</a><sup>[596]</sup> and the <a href="#">credentials for SNMP devices</a><sup>[603]</sup> that you entered in the device settings or that the device <a href="#">inherits</a><sup>[131]</sup> 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 <a href="#">SNMP v1</a> or <a href="#">SNMP v2c</a>, which do not provide encryption.</p> <p><b>☁</b> This setting is not available on the hosted probe of a PRTG Hosted Monitor instance.</p>

## Number of Sensors Limitation

### Number of Sensors Limitation

**Sensor Limit** **i**

☒ Allow unlimited number of sensors  
☐ Limit number of sensors

Number of Sensors Limitation

Setting	Description
Sensor Limit	<p>This setting allows you to set a limit for the maximum number of sensors in this group, including subgroups. If the amount of sensors exceeds the limitation, PRTG sets the surplus sensors to the Paused status. Choose between:</p> <ul style="list-style-type: none"> <li>▪ Allow unlimited number of sensors: Do not limit the number of sensors for this group. Any number of sensors are allowed in this group and its subgroups.</li> <li>▪ Limit number of sensors: Set a limitation for the number of sensors in this group. Only a defined number of sensors are allowed in this group and its subgroups.</li> </ul>
Maximum Number of Sensors	<p>This setting is only visible if you select Limit number of sensors above. Define how many sensors are allowed in this group and its subgroups. Sensors that exceed this group sensor limit are set to the Paused status. Enter an integer.</p> <p>❗ Sensors that are in the Paused status count for this group limit as well (for example, manually paused sensors or sensors that are paused by dependency or schedule), but not for the number of available sensors in your license.</p> <p>❗ Manually paused sensors override the sensor message <b>exceeds group sensor limit</b>.</p>

❗ 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>

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>

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>

## 7.7 Device Settings

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

- ❗ We recommend that you define as many settings as possible in the [root group settings](#)<sup>[419]</sup> so that you can inherit them to all other objects in the [object hierarchy](#)<sup>[131]</sup>.

For device settings, you can also use multi-edit. This enables you to change the settings of many devices at the same time.

■ For more information, see section [Multi-Edit](#)<sup>[3158]</sup>.

- ❗ 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 Device Settings](#)<sup>[589]</sup>
- [Additional Device Information](#)<sup>[591]</sup>
- [Device Identification and Auto-Discovery](#)<sup>[592]</sup>
- [Location](#)<sup>[595]</sup>
- [Credentials for Windows Systems](#)<sup>[596]</sup>
- [Credentials for Linux/Solaris/macOS \(SSH/WBEM\) Systems](#)<sup>[598]</sup>
- [Credentials for VMware/XenServer](#)<sup>[602]</sup>
- [Credentials for SNMP Devices](#)<sup>[603]</sup>
- [Credentials for Database Management Systems](#)<sup>[607]</sup>
- [Credentials for AWS](#)<sup>[609]</sup>
- [Credentials for Microsoft 365](#)<sup>[610]</sup>
- [Credentials for Script Sensors](#)<sup>[612]</sup>
- [Credentials for Cisco Meraki](#)<sup>[613]</sup>
- [Credentials for Dell EMC](#)<sup>[614]</sup>
- [Credentials for FortiGate](#)<sup>[615]</sup>
- [Credentials for HPE 3PAR](#)<sup>[616]</sup>
- [Credentials for HTTP](#)<sup>[618]</sup>
- [Credentials for Microsoft Azure](#)<sup>[620]</sup>
- [Credentials for MQTT](#)<sup>[621]</sup>
- [Credentials for NetApp](#)<sup>[623]</sup>
- [Credentials for OPC UA](#)<sup>[625]</sup>
- [Credentials for Soffico Orchestra](#)<sup>[628]</sup>
- [Credentials for Redfish](#)<sup>[630]</sup>



- [Credentials for REST API](#)<sup>[631]</sup>
- [Credentials for Veeam](#)<sup>[633]</sup>
- [Windows Compatibility Options](#)<sup>[634]</sup>
- [SNMP Compatibility Options](#)<sup>[636]</sup>
- [Proxy Settings for HTTP Sensors](#)<sup>[641]</sup>
- [Scanning Interval](#)<sup>[643]</sup>
- [Schedules, Dependencies, and Maintenance Window](#)<sup>[644]</sup>
- [Access Rights](#)<sup>[647]</sup>
- [Channel Unit Configuration](#)<sup>[648]</sup>
- [Advanced Network Analysis](#)<sup>[649]</sup>

Basic Device Settings

Basic Device Settings

Device Name ⓘ

Device

Monitoring Status ⓘ

☒ Started

☐ Paused

IP Version ⓘ

☒ IPv4

☐ IPv6

IPv4 Address/DNS Name ⓘ

192.0.2.0

Parent Tags ⓘ

Tags ⓘ

+

Priority ⓘ

★ ★ ★ ☆ ☆

Basic Device Settings

Setting	Description
Device Name	<p>Enter a name to identify the device. By default, PRTG shows this name in the <a href="#">device tree</a><sup>[164]</sup>, as well as in <a href="#">alarms</a><sup>[199]</sup>, <a href="#">logs</a><sup>[208]</sup>, <a href="#">notifications</a><sup>[3173]</sup>, <a href="#">reports</a><sup>[3192]</sup>, <a href="#">maps</a><sup>[3214]</sup>, <a href="#">libraries</a><sup>[3176]</sup>, and <a href="#">tickets</a><sup>[211]</sup>.</p> <p> ⓘ If the name contains angle brackets (&lt;&gt;), PRTG replaces them with braces ([]) for security reasons. For more information, see the Knowledge Base: <a href="#">What security features does PRTG include?</a></p>

Setting	Description
Monitoring Status	<p>Select the monitoring status of the device:</p> <ul style="list-style-type: none"> <li>Started: Monitor the device.</li> <li>Paused: Pause monitoring for the device. All sensors on the device are in the Paused <a href="#">status</a><sup>[224]</sup> until you change this setting.</li> </ul>
IP Version	<p>Select the IP protocol that PRTG uses to connect to the device:</p> <ul style="list-style-type: none"> <li>IPv4: Use IP version 4 for all requests to the device.</li> <li>IPv6: Use IP version 6 for all requests to the device.</li> </ul> <p><b>i</b> The setting is valid for all sensors that you create on the device.</p>
IPv4 Address/DNS Name	<p>This setting is only visible if you select IPv4 above. Enter the IP address or Domain Name System (DNS) name for the device. Most sensors that you create on this device inherit this setting and try to connect to this address for monitoring.</p> <p><b>i</b> Some sensors have their own setting for the IP address/DNS name to which they connect.</p>
IPv6 Address/DNS Name	<p>This setting is only visible if you select IPv6 above. Enter the IP address or Domain Name System (DNS) name for the device. Most sensors that you create on this device inherit this setting and try to connect to this address for monitoring.</p> <p><b>i</b> Some sensors have their own setting for the IP address/DNS name to which they connect.</p>
Parent Tags	<p>Shows <a href="#">tags</a><sup>[137]</sup> that this device <a href="#">inherits</a><sup>[137]</sup> from its parent <a href="#">group</a><sup>[132]</sup> and its parent <a href="#">probe</a><sup>[132]</sup>.</p> <p><b>i</b> This setting is for your information only. You cannot change it.</p>
Tags	<p>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 <a href="#">inherited</a><sup>[137]</sup>.</p> <p><b>i</b> We recommend that you use the default value. You can also add additional tags.</p> <p><b>i</b> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with parentheses (()) or angle brackets (&lt;&gt;).</p> <p><b>i</b> For performance reasons, it can take some minutes until you can filter for new tags that you added.</p>

Setting	Description
Priority	Select a <a href="#">priority</a> <sup>[221]</sup> for the device. This setting determines the position of the group in lists. The highest priority is at the top of a list. You can choose from the lowest priority ( ☆☆☆☆☆ ) to the highest priority ( ★★★★★ ).

## Additional Device Information

Additional Device Information

Device Icon ⓘ

Service URL ⓘ

Additional Device Information

Setting	Description
Device Icon	Select a device icon. PRTG shows it in the device tree.
Service URL	Specify a URL to open directly when you select Device Tools   Go to Service URL from the <a href="#">context menu</a> <sup>[234]</sup> of the device. For example, you can configure this option to open the address <a href="http://www.example.com/service.html">http://www.example.com/service.html</a> . Enter a valid URL or leave the field empty.




## Device Identification and Auto-Discovery

### Device Identification and Auto-Discovery

#### Auto-Discovery Level

- ☒ No auto-discovery
- ☐ Standard auto-discovery (recommended)
- ☐ Detailed auto-discovery
- ☐ Auto-discovery with specific device templates

Device Identification and Auto-Discovery


Setting	Description
Auto-Discovery Level	<p>Select the level of detail for the <a href="#">auto-discovery</a> .</p> <ul style="list-style-type: none"> <li>▪ No auto-discovery: Select this option if you only want to manually create devices and sensors.</li> <li>▪ Standard auto-discovery (recommended): Create a set of standard sensors for standard monitoring. This option works fine for most installations.</li> <li>▪ Detailed auto-discovery: Create all standard sensors and additional sensors from detailed variants of device templates. As a result, you might get many sensors. This option is suitable for small network segments and whenever you want to monitor the maximum number of sensors available.</li> <li>▪ Auto-discovery with specific device templates: Customize the auto-discovery and select or combine standard, detailed, and custom device templates. Select one or more templates from the Device Templates list.</li> </ul> <p> Auto-discoveries can be resource intensive. They are primarily intended for devices on the same network as your probes.</p>
Schedule	<p>Select when PRTG runs the auto-discovery:</p> <ul style="list-style-type: none"> <li>▪ Once: Run the auto-discovery only once. PRTG adds new devices and sensors once. If you select this option, you must manually <a href="#">start the auto-discovery</a> .</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Hourly: Run the auto-discovery for new devices and sensors every 60 minutes.  <span style="color: red;">❗</span> Use this option with caution. Frequent auto-discoveries might cause performance issues, in particular when PRTG scans large network segments every hour.</li> <li>▪ Daily: Run the auto-discovery for new devices and sensors every 24 hours. The first auto-discovery runs immediately. All other discoveries start at the time that you define in the <a href="#">Monitoring</a> settings, section Auto-Discovery.</li> <li>▪ Weekly: Run the auto-discovery for new devices and sensors every 7 days. The first auto-discovery runs immediately. All other discoveries start at the time that you define in the Monitoring settings, section Auto-Discovery.</li> </ul> <p><span style="color: blue;">❗</span> For performance reasons, PRTG sets Schedule to Once on all devices that the scheduled auto-discovery creates.</p>
Device Templates	<p>This setting is only visible if you select Auto-discovery with specific device templates above. Select one or more device templates by enabling a check box in front of the template name.</p> <p><span style="color: blue;">❗</span> You can also select all items or cancel the selection by using the check box in the table header.</p> <p>PRTG uses the device templates that you select for the auto-discovery on the device. Choose from:</p> <ul style="list-style-type: none"> <li>▪ ADSL</li> <li>▪ Amazon CloudWatch</li> <li>▪ Buffalo TeraStation NAS</li> <li>▪ Cisco ASA VPN</li> <li>▪ Cisco Device (Generic)</li> <li>▪ Dell EqualLogic</li> <li>▪ Dell MDi Disk</li> <li>▪ DNS Server</li> <li>▪ Environment Jakarta</li> <li>▪ Environment Poseidon</li> <li>▪ FTP Server</li> <li>▪ Generic Device (Ping Only)</li> <li>▪ Generic Device (SNMP Enabled)</li> <li>▪ Generic Device (SNMP Enabled, Detailed)</li> <li>▪ HTTP Web Server</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Hyper-V Host Server</li> <li>▪ IPMI-enabled Device</li> <li>▪ Juniper NS Device</li> <li>▪ Linux/UNIX Device (SNMP or SSH Enabled)</li> <li>▪ Mail Server (Generic)</li> <li>▪ Mail Server (MS Exchange)</li> <li>▪ Microsoft SharePoint 2010</li> <li>▪ NAS LenovoEMC</li> <li>▪ NAS QNAP</li> <li>▪ NAS Synology</li> <li>▪ NetApp</li> <li>▪ NTP Server</li> <li>▪ Printer (HP)</li> <li>▪ Printer (Generic)</li> <li>▪ RDP Server</li> <li>▪ RMON-compatible Device</li> <li>▪ Server (Cisco UCS)</li> <li>▪ Server (Compaq/HP Agents)</li> <li>▪ Server (Dell)</li> <li>▪ Server (Fujitsu)</li> <li>▪ Server (IBM)</li> <li>▪ SonicWall</li> <li>▪ SSL Security Check</li> <li>▪ Switch (Cisco Catalyst)</li> <li>▪ Switch (Cisco IOS Based)</li> <li>▪ Switch (HP Procurve)</li> <li>▪ UNIX/Linux Device</li> <li>▪ UPS Health (APC)</li> <li>▪ UPS Health (Generic)</li> <li>▪ UPS Health (Liebert)</li> <li>▪ VMware ESXi / vCenter Server</li> <li>▪ Web Server</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>Windows (Detailed via WMI)</li> <li>Windows (via Remote PowerShell)</li> <li>Windows (via WMI)</li> <li>Windows IIS (via SNMP)</li> <li>XenServer Hosts</li> <li>XenServer Virtual Machines</li> </ul> <p>Once the auto-discovery is finished, PRTG creates a new <a href="#">ticket</a><sup>[211]</sup> and lists the device templates that it used to create new sensors.</p>

## 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](#)<sup>[419]</sup> 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](#)<sup>[135]</sup>.


## Location

Click  to interrupt the [inheritance](#)<sup>[135]</sup>.

### Location

 inherit from

Location (for Geo Maps) <sup>?</sup>



Location

Setting	Description
Location (for Geo Maps)	<p>If you want to use <a href="#">Geo Maps</a><sup>[3169]</sup>, 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 <a href="#">sensor status icons</a><sup>[179]</sup> (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 <a href="#">49.452778 11.077778</a>, or enter <a href="#">49.452778 any 11.077778 text</a>.</p> <p>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.</p> <p>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.</p> <p><b>i</b> The preview map always has a road map layout regardless of the map layout you set in <a href="#">User Interface</a><sup>[6297]</sup>.</p>

## Credentials for Windows Systems

Click  to interrupt the [inheritance](#)<sup>[135]</sup>.

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

<ul style="list-style-type: none"> <li>▪ <a href="#">Active Directory Replication Errors</a></li> <li>▪ <a href="#">Event Log (Windows API)</a></li> <li>▪ <a href="#">Exchange Backup (PowerShell)</a></li> <li>▪ <a href="#">Exchange Database (PowerShell)</a></li> <li>▪ <a href="#">Exchange Database DAG (PowerShell)</a></li> <li>▪ <a href="#">Exchange Mail Queue (PowerShell)</a></li> <li>▪ <a href="#">Exchange Mailbox (PowerShell)</a></li> <li>▪ <a href="#">Exchange Public Folder (PowerShell)</a></li> <li>▪ <a href="#">File</a></li> <li>▪ <a href="#">File Content</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">Windows IIS 6.0 SMTP Sent</a></li> <li>▪ <a href="#">Windows IIS Application</a></li> <li>▪ <a href="#">Windows MSMQ Queue Length</a></li> <li>▪ <a href="#">Windows Network Card</a></li> <li>▪ <a href="#">Windows Pagefile</a></li> <li>▪ <a href="#">Windows Physical Disk I/O</a></li> <li>▪ <a href="#">Windows Print Queue</a></li> <li>▪ <a href="#">Windows Process</a></li> <li>▪ <a href="#">Windows System Uptime</a></li> <li>▪ <a href="#">Windows Updates Status (PowerShell)</a></li> <li>▪ <a href="#">WMI Battery</a></li> <li>▪ <a href="#">WMI Custom</a></li> <li>▪ <a href="#">WMI Custom String</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">WMI Memory</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2005 (Deprecated)</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2008</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2012</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2014</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2016</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2017</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2019</a></li> <li>▪ <a href="#">WMI Remote Ping</a></li> <li>▪ <a href="#">WMI Security Center</a></li> </ul>
--	--	--



<ul style="list-style-type: none"> <li>▪ <a href="#">Folder</a></li> <li>▪ <a href="#">Hyper-V Cluster Shared Volume Disk Free</a></li> <li>▪ <a href="#">Hyper-V Host Server</a></li> <li>▪ <a href="#">Hyper-V Virtual Machine</a></li> <li>▪ <a href="#">Hyper-V Virtual Network Adapter</a></li> <li>▪ <a href="#">Hyper-V Virtual Storage Device</a></li> <li>▪ <a href="#">PerfCounter Custom</a></li> <li>▪ <a href="#">PerfCounter IIS Application Pool</a></li> <li>▪ <a href="#">Share Disk Free</a></li> <li>▪ <a href="#">Windows CPU Load</a></li> <li>▪ <a href="#">Windows IIS 6.0 SMTP Received</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">WMI Disk Health</a></li> <li>▪ <a href="#">WMI Event Log</a></li> <li>▪ <a href="#">WMI Exchange Server</a></li> <li>▪ <a href="#">WMI Exchange Transport Queue</a></li> <li>▪ <a href="#">WMI File</a></li> <li>▪ <a href="#">WMI Free Disk Space (Multi Disk)</a></li> <li>▪ <a href="#">WMI HDD Health</a></li> <li>▪ <a href="#">WMI Logical Disk I/O</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">WMI Service</a></li> <li>▪ <a href="#">WMI Share</a></li> <li>▪ <a href="#">WMI SharePoint Process</a></li> <li>▪ <a href="#">WMI Storage Pool</a></li> <li>▪ <a href="#">WMI Terminal Services (Windows 2008+)</a></li> <li>▪ <a href="#">WMI Terminal Services (Windows XP/Vista/2003)</a></li> <li>▪ <a href="#">WMI UTC Time</a></li> <li>▪ <a href="#">WMI Vital System Data v2</a></li> <li>▪ <a href="#">WMI Volume</a></li> <li>▪ <a href="#">WSUS Statistics</a></li> </ul>
--	---	---

## Credentials for Windows Systems



inherit from

Domain or Computer Name ⓘ

www.example.com

User Name ⓘ

johnqpublic

Password ⓘ

.....

Credentials for Windows Systems

Setting	Description
Domain or Computer Name	<p>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.</p> <p>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.</p>
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	<p>Select the authentication method for the login:</p> <ul style="list-style-type: none"> <li>▪ Password: Provide the password for the login.</li> <li>▪ Private key: Provide an RSA private key for authentication.</li> </ul> <p> PRTG can only handle keys in the OpenSSH format that are not encrypted. You cannot use password-protected keys.</p> <p> PRTG only supports RSA keys. It does not support DSA keys.</p> <p> For details, see section <a href="#">Monitoring via SSH</a> <sup>B437</sup>.</p>
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	<p>This setting is only visible if you select Private key above. Paste the entire RSA private key, including the <b>BEGIN</b> and <b>END</b> lines. Make sure that a corresponding public key exists on the target device.</p> <p> PRTG can only handle keys in the OpenSSH format that are not encrypted. You cannot use password-protected keys.</p> <p> PRTG only supports RSA keys. It does not support DSA keys.</p> <p> For details, see section <a href="#">Monitoring via SSH</a> <sup>B437</sup>.</p> <p> If you do not insert a private key for the first time but if you want to <a href="#">change</a> the private key, you need to <a href="#">restart the PRTG core server service</a> <sup>B352</sup> for the private key change to take effect.</p>
WBEM Protocol	<p>Select the protocol that you want to use for the connection to the system via WBEM:</p> <ul style="list-style-type: none"> <li>▪ HTTP: Use an unsecure connection for WBEM.</li> <li>▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection for WBEM.</li> </ul> <p> This setting is only relevant if you use WBEM sensors.</p>
WBEM Port	<p>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:</p> <ul style="list-style-type: none"> <li>▪ Default: Use one of the default ports. The default port for unsecure connections is <b>5988</b> and the default port for secure connections is <b>5989</b>.</li> <li>▪ Custom: Use a custom port.</li> </ul>