



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


Credentials for HTTP

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


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


- [HTTP v2](#)

Credentials for HTTP

Authentication Method 

☒ None (default)
☐ Basic authentication
☐ Bearer authentication

Placeholder 1 Description 

Placeholder 1 

Credentials for HTTP

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

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](#) ¹³⁵.


 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](#)  ¹³⁵.

 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 ⁱ

☒ None (default)

☐ Username/Password

Port ⁱ

1883




Transport-Level Security ⁱ

☒ 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"> None (default): Connect without credentials. User name and password: Define credentials for the connection.
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 8883 and the default port for unsecure connections is 1883.</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"> Do not use transport-level security: Establish the connection without connection security. Use transport-level security: Establish the connection with the strongest SSL/TLS method that the target device provides.
Server Authentication	<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"> Disable (default): Do not use a certificate for server authentication. Enable: Use a certificate for server authentication.
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"> Disable (default): Do not use a certificate for client authentication. Enable: Use a certificate for client authentication.
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 443 .
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"> ▪ HTTPS (default) ▪ HTTP

Credentials for OPC UA

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

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

- [Beckhoff IPC System Health](#)
- [OPC UA Certificate](#)
- [OPC UA Custom](#)
- [OPC UA Server Status](#)

Credentials for OPC UA

☐ inherit from

Port ⓘ

4840

Server Path ⓘ

Security Mode ⓘ

☒ None (default)

☐ Sign

☐ Sign & Encrypt




Authentication Method ⓘ


☒ Anonymous (default)

☐ User name and password

Credentials for OPC UA

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

Setting	Description
	<ul style="list-style-type: none"> ▪ Sign & Encrypt: Sign and encrypt messages between the sensor and the OPC UA server.
Security Policy	<p>This setting is only visible if you select Sign or Sign & Encrypt above. Select if you want to use a security policy and define which policy you want to use:</p> <ul style="list-style-type: none"> ▪ None (default): Do not use a security policy. ▪ Basic256Sha256: Use the Basic256Sha256 security policy. ▪ Basic256: Use the Basic256 security policy.
Client Certificate	<p>This setting is only visible if you select Sign or Sign & Encrypt above. Enter the certificate that you created for authenticating the sensor against the OPC UA server.</p> <p> The certificate must meet the following requirements:</p> <ul style="list-style-type: none"> ▪ The key size must be 2048-bit. ▪ The secure hash algorithm must be SHA256. ▪ DataEncipherment must be part of the KeyUsage certificate extension. ▪ A uniform resource indicator (URI) must be set in subjectAltName. ▪ The certificate must be in Privacy-Enhanced Mail (PEM) format.
Client Key	<p>This setting is only visible if you select Sign or Sign & 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 & 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"> ▪ Anonymous (default): Connect without credentials. ▪ User name and password: Define credentials for the connection. <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 & 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](#)  ¹³⁵.

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

- [Soffico Orchestra Channel Health](#)

Credentials for Soffico Orchestra



inherit from

Authentication Method ⁱ



None (default)



User name and password

Timeout (Sec.) ⁱ

60

Port ⁱ

8443

Protocol ⁱ



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"> None (default): Connect without credentials. User name and password: Define credentials for the connection.
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 300 seconds (5 minutes).
Port	Enter the port for the connection to the Orchestra platform. The default port for secure connections is 8443 and the default port for unsecure connections is 8019 .
Protocol	<p>Select the protocol that you want to use for the connection to the Orchestra platform:</p> <ul style="list-style-type: none"> ▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection. ▪ HTTP: Use an unsecure connection.

Credentials for Redfish

Click  to interrupt the [inheritance](#) .

 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"> HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection. HTTP: Use an unsecured connection.
Port	Enter the port for the connection to the Redfish system. The default port for secure connections is 443.

Credentials for REST API

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

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

▪ [REST Custom v2](#)

Credentials for REST API

Authentication Method ⓘ

☒ None (default)

☐ Basic authentication

☐ Bearer authentication

Credentials for REST API

Setting	Description
Authentication Method	<p>Select the authentication method for access to the Representational State Transfer (REST) application programming interface (API):</p> <ul style="list-style-type: none"> ▪ None (default): Use no authentication. ▪ Basic authentication: Use basic authentication. ▪ Bearer authentication: Use an OAuth2 bearer token.
User Name	This setting is only visible if you select Basic authentication above. Enter the user name for access to the REST API.
Password	This setting is only visible if you select Basic authentication above. Enter the password for access to the REST API.
Bearer Token	This setting is only visible if you select Bearer authentication above. Enter a bearer token for access to the REST API.
Placeholder 1 Description	Enter a description for Placeholder 1, for example information about the purpose or content of the placeholder.
Placeholder 1	Enter a value for the placeholder. PRTG inserts the value for the REST API request if you add <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 <code>%restplaceholder3</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 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 <code>%restplaceholder4</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 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 <code>%restplaceholder5</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.

Credentials for Veeam

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

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

- [Veeam Backup Job Status](#)
- [Veeam Backup Job Status Advanced](#)

Credentials for Veeam

User ⓘ

johnqpublic

Password ⓘ

.....

Port ⓘ

9398

Credentials for Veeam

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

Access Rights

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

Account Control

User Type ⓘ

☐ Read/write user
 ☒ Read-only user

Acknowledge Alarms ⓘ

☐ User can acknowledge alarms
 ☒ User cannot acknowledge alarms (default)

Password Change ⓘ

☐ User can change the account password
 ☒ User cannot change the account password (default)

Primary Group ⓘ

PRTG Users Group

Status ⓘ

☒ Active
 ☐ Paused

Last Login ⓘ

(has not logged in yet)

User Access Rights in User Accounts Settings

Setting	Description
User Group Access	<p>Select the user groups^[3346] that have access to the object. You see a table with user groups and group access rights. The table contains all user groups in your setup. For each user group, you can choose from the following group access rights:</p> <ul style="list-style-type: none"> ▪ Inherited: Inherit the access rights settings of the parent object. ▪ No access: Users in this user group cannot see or edit the object. The object neither shows up in lists nor in the device tree. <p> ⓘ 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.</p> ▪ Read access: Users in this group can see the object and view its monitoring results. They cannot edit any settings. ▪ Write access: Users in this group can see the object, view its monitoring results, and edit its settings. They cannot edit its access rights settings. ▪ Full access: Users in this group can see the object, view its monitoring results, edit its settings, and edit its access rights settings. <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 Access Rights Management^[144].</p>

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

More

KNOWLEDGE BASE

What security features does PRTG include?

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

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

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

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


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


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

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

7.2.2 Add a Group


There are several ways to manually add a group:

- Select Devices | Add Group from the [main menu bar](#)^[248]. A dialog appears that guides you through the process of adding a new group.
- Hover over  and select Add Group from the menu.
- Select Add Group from the [context menu](#)^[226] of the probe or group to which you want to add the new group. This skips step 1 and leads you directly to [step 2](#)^[323].

 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:

- [Add a Group](#)^[321]
- [Step 1: Select a Parent](#)^[322]
- [Step 2: Define Group Settings](#)^[323]
- [Basic Group Settings](#)^[324]
- [Inherited Settings](#)^[324]
- [Credentials for Windows Systems](#)^[325]
- [Credentials for Linux/Solaris/macOS \(SSH/WBEM\) Systems](#)^[327]
- [Credentials for VMware/XenServer](#)^[331]
- [Credentials for SNMP Devices](#)^[332]
- [Credentials for Database Management Systems](#)^[336]
- [Credentials for AWS](#)^[338]
- [Credentials for Script Sensors](#)^[339]
- [Credentials for Cisco Meraki](#)^[340]
- [Credentials for Dell EMC](#)^[341]
- [Credentials for FortiGate](#)^[342]
- [Credentials for HPE 3PAR](#)^[343]
- [Credentials for HTTP](#)^[345]
- [Credentials for Microsoft Azure](#)^[347]
- [Credentials for MQTT](#)^[348]
- [Credentials for NetApp](#)^[350]
- [Credentials for OPC UA](#)^[352]
- [Credentials for Soffico Orchestra](#)^[355]
- [Credentials for Redfish](#)^[357]
- [Credentials for REST API](#)^[358]

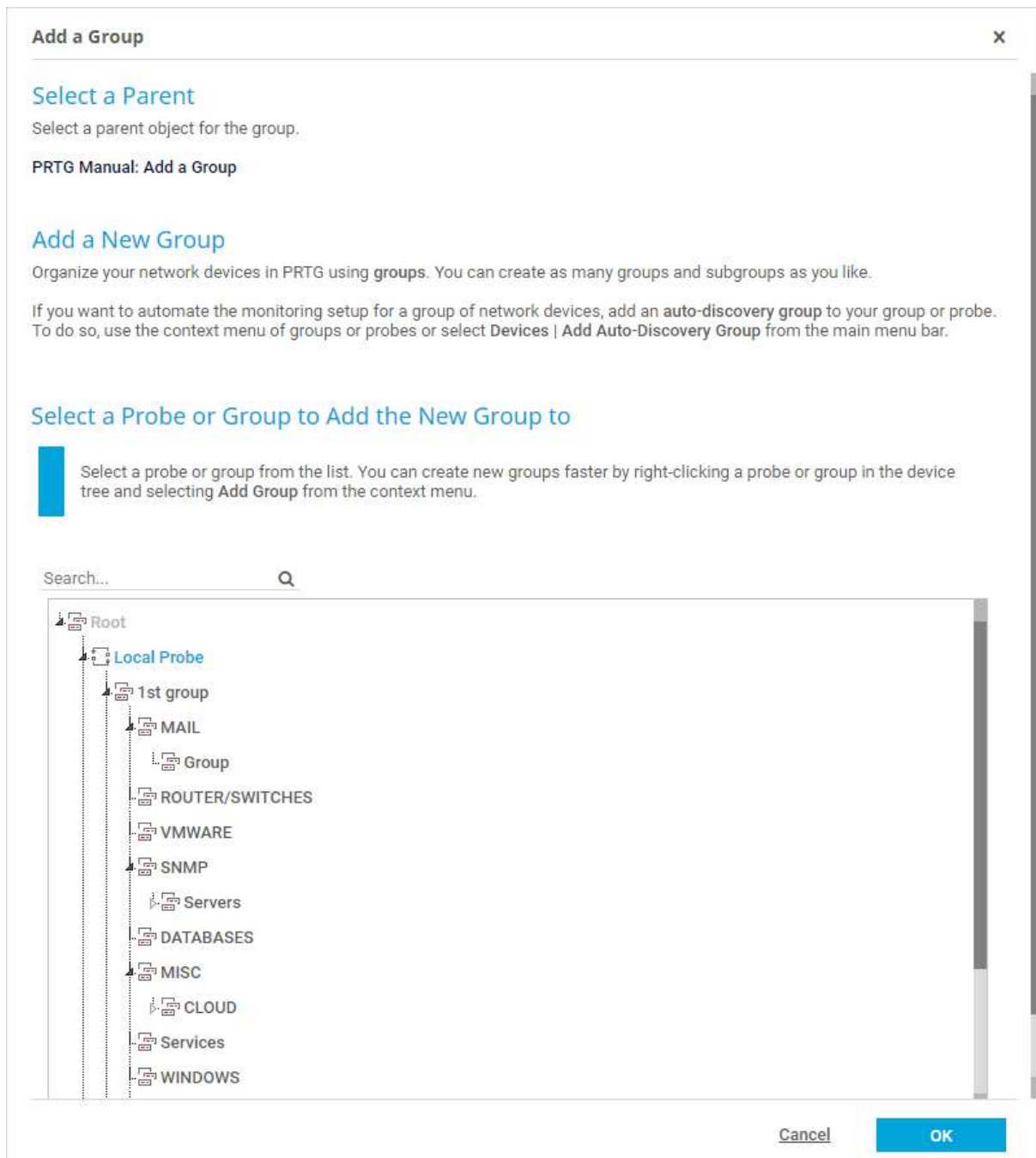
- [Credentials for Veeam](#)  360
- [Access Rights](#)  361

Add a Group

The Add a Group dialog appears when you add a new group to a parent group. It only shows the settings that are required to create the group. Therefore, you do not see all settings in this dialog.

- ① You can change all settings on the Settings tab of the group later. For more information, see section [Group Settings](#)  520.

Step 1: Select a Parent



Add Group Assistant Step 1

Select the probe or group that you want to add the new group to. Click OK.

Step 2: Define Group Settings

Add a Group to Local Probe

Define Group Settings

Specify credentials and access rights for your group, if necessary. All devices in this group will inherit these settings.

[PRTG Manual: Add a Group](#)

Add a New Group

Organize your network devices in PRTG using **groups**. You can create as many groups and subgroups as you like.

If you want to automate the monitoring setup for a group of network devices, add an **auto-discovery group** to your group or probe. To do so, use the context menu of groups or probes or select **Devices | Add Auto-Discovery Group** from the main menu bar.

Basic Group Settings

Group Name [?]

Group

Tags [?]

+

Credentials for Windows Systems

☒ inherit from Local Probe (Domain or Computer Name: paesslergmbh, User: ...)

Credentials for Linux/Solaris/Mac OS (SSH/WBEM) Systems

☒ inherit from Local Probe (User: <empty>, Login: 0, For WBEM Use Port: 0,...)

Credentials for VMware/XenServer

☒ inherit from Local Probe (User: <empty>)

Cancel
OK


Add Group Assistant Step 2

Basic Group Settings

Basic Group Settings

Setting	Description
Group Name	<p>Enter a name to identify the group. By default, PRTG shows this name in the device tree^[164], as well as in alarms^[199], logs^[208], notifications^[3173], reports^[3192], maps^[3214], libraries^[3176], and tickets^[211].</p> <p>i If the name contains angle brackets (<>), PRTG replaces them with braces ([]) for security reasons. For more information, see the Knowledge Base: What security features does PRTG include?</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 inherited^[137].</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with parentheses (()) or angle brackets (<>).</p> <p>i For performance reasons, it can take some minutes until you can filter for new tags that you added.</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](#)^[419] if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#)^[135].

Credentials for Windows Systems

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

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

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

Credentials for Windows Systems



inherit from

Domain or Computer Name ⁱ

www.example.com

User Name ⁱ

johnqpublic

Password ⁱ

.....

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	<p>Enter the user name for access to the Windows system. Usually, you use credentials with administrator rights.</p>
Password	<p>Enter the password for access to the Windows system. Usually, you use credentials with administrator rights.</p>

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"> ▪ Password: Provide the password for the login. ▪ Private key: Provide an RSA private key for authentication. <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 Monitoring via SSH ^[3437].</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 BEGIN and END 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 Monitoring via SSH ^[3437].</p> <p> If you do not insert a private key for the first time but if you want to change the private key, you need to restart the PRTG core server service ^[3352] for the private key change to take effect.</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"> ▪ HTTP: Use an unsecure connection for WBEM. ▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection for WBEM. <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"> ▪ Default: Use one of the default ports. The default port for unsecure connections is 5988 and the default port for secure connections is 5989. ▪ Custom: Use a custom port.

Setting	Description
	<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 22.</p> <p> By default, PRTG automatically uses this setting for all SSH sensors ^[3683] 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"> ▪ Run the command as the connecting user (default): Use the rights of the user who establishes the SSH connection. ▪ Run the command as a different user using 'sudo' (with password): Use the rights of a different user with a password required for sudo to run commands on the target system, for example, as a root user. ▪ Run the command as a different user using 'sudo' (without password): Use the rights of a different user without a password required for sudo to run commands on the target system, for example, as a root user. ▪ Run the command as a different user using 'su': Use the rights of a different user with su to run commands on the target system.
Target System User Name	This setting is only visible if you select an option that includes sudo or su above. Enter a user name to run the specified command on the target system as a different user than the root user. If you leave this field empty, you run the command as a root user. Make sure that you set the Linux password even if you use a public key or a private key for authentication. This is not necessary if the user is allowed to run the command without a password.
Password	This setting is only visible if you select an option that includes sudo or su with password above. Enter the password to run the sudo command or the su command.
SSH Connection Mode	<p>Select the connection mode that you want to use to access data with SSH sensors ^[3437].</p> <ul style="list-style-type: none"> ▪ Default (recommended): This is the default connection mode for SSH sensors. It provides the best performance and security. ▪ Compatibility mode (deprecated): Use this only if the default connection mode does not work on the target system. The compatibility mode is the connection mode that PRTG used in previous versions and it is deprecated.

Setting	Description
	<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"> ▪ HTTPS (recommended): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection. ▪ HTTP: Use an unsecure connection.
Session Handling	<p>Select if you want to reuse a session for VMware sensors:</p> <ul style="list-style-type: none"> ▪ Reuse a session for multiple scans (recommended): Select this option if you want a VMware sensor to reuse a single session for multiple sensor scans to query data. With this option, the sensor does not need to log in and out for each sensor scan. We recommend that you use this option because it reduces network load and log entries on the target device. This can increase performance. ▪ Create a new session for each scan: If you select this option, PRTG does not reuse a session and a VMware sensor has to log in and out for each sensor scan. This can decrease performance.

Credentials for SNMP Devices

Click  to interrupt the [inheritance](#) .

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

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

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

Credentials for SNMP Devices

☐ inherit from

SNMP Version ⓘ

- ☐ SNMP v1
- ☒ SNMP v2c (recommended)
- ☐ SNMP v3

Community String ⓘ

public

SNMP Port ⓘ

161




Timeout (Sec.) ⓘ

5

Credentials for SNMP Devices

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

Setting	Description
	<ul style="list-style-type: none"> SNMP v3: Use SNMP v3 for the connection. SNMP v3 provides secure authentication and data encryption. <p>i SNMP v3 has performance limitations because of the use of encryption. The main limiting factor is CPU power. Also keep in mind that SNMP v3, unlike SNMP v1 and v2c, does not scale with more CPU power. Because of this limitation, PRTG can only handle a limited number of requests per second so that you can use only a limited number of sensors using SNMP v3. If you see an increase in Interval Delay or Open Requests with the Probe Health sensor, distribute the load over multiple probes ^[362]. 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>i 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"> MD5: Use message-digest algorithm 5 (MD5) for authentication. SHA: Use Secure Hash Algorithm (SHA) for authentication. SHA-224: Use SHA-224 for authentication. SHA-256: Use SHA-256 for authentication. SHA-384: Use SHA-384 for authentication. SHA-512: Use SHA-512 for authentication. <p>i If you do not want to use authentication but you need SNMP v3, for example, because your device requires context, you can leave the Password field empty. In this case, PRTG uses SNMP_SEC_LEVEL_NOAUTH and it entirely deactivates authentication.</p> <p>i 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>i 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>i 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"> ▪ DES: Use Data Encryption Standard (DES) as the encryption algorithm. ▪ AES: Use Advanced Encryption Standard (AES) as the encryption algorithm. ▪ AES-192: Use AES-192 as the encryption algorithm. ▪ AES-256: Use AES-256 as the encryption algorithm. <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. Context 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 161.</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 300 seconds (5 minutes).</p>

Credentials for Database Management Systems

Click  to interrupt the [inheritance](#) .

 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 all database sensors and for connections to all your databases.
Custom Port	Enter a custom port for database connections. Enter an integer. ⓘ PRTG uses this custom port for all database sensors and for connections to all your databases.
Authentication Method	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](#) .


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


- [AWS Alarm v2](#)
- [AWS Cost](#)
- [AWS EBS v2](#)
- [AWS EC2 v2](#)
- [AWS ELB v2](#)
- [AWS RDS v2](#)

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

Credentials for AWS

 inherit from

Access Key 

Secret Key 

Credentials for AWS

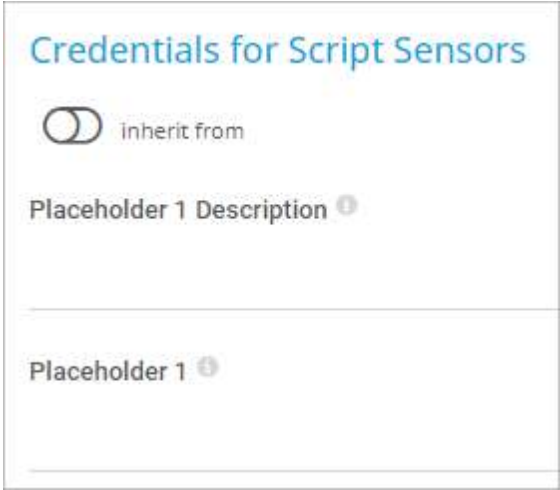
Setting	Description
Access Key	Enter the Amazon Web Services (AWS) access key.
Secret Key	Enter the AWS secret key.

Credentials for Script Sensors

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

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

- [EXE/Script](#)
- [EXE/Script Advanced](#)
- [Python Script Advanced](#)
- [SSH Script](#)
- [SSH Script Advanced](#)



Credentials for Script Sensors

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

Setting	Description
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](#) ¹³⁵.

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

- [Cisco Meraki License](#)
- [Cisco Meraki Network Health](#)

Credentials for Cisco Meraki

 inherit from  Network Infrastructure

API Key ⓘ

Meraki Dashboard API Endpoint ⓘ api.meraki.com

Credentials for Cisco Meraki

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

Credentials for Dell EMC

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 443 .

Credentials for FortiGate

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

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

- [FortiGate System Statistics](#)
- [FortiGate VPN Overview](#)

Credentials for FortiGate

☐ inherit from

API Token ⓘ

Port ⓘ

443

Credentials for FortiGate

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

Credentials for HPE 3PAR

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

ⓘ 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"> ▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection. ▪ HTTP: Use an unsecure connection.

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

Credentials for HTTP

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

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"> ▪ None (default): Use no authentication. ▪ Basic authentication: Use basic authentication. ▪ Bearer authentication: Use an OAuth2 bearer token.
User Name	This setting is only visible if you select Basic authentication above. Enter the user name for access to the server.

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](#) ¹³⁵.


 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](#)  ¹³⁵.

 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 ⁱ

☒ None (default)

☐ Username/Password

Port ⁱ

1883




Transport-Level Security ⁱ

☒ 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"> None (default): Connect without credentials. User name and password: Define credentials for the connection.
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 8883 and the default port for unsecure connections is 1883.</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"> Do not use transport-level security: Establish the connection without connection security. Use transport-level security: Establish the connection with the strongest SSL/TLS method that the target device provides.
Server Authentication	<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"> Disable (default): Do not use a certificate for server authentication. Enable: Use a certificate for server authentication.
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"> Disable (default): Do not use a certificate for client authentication. Enable: Use a certificate for client authentication.
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 443 .
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"> ▪ HTTPS (default) ▪ HTTP

Credentials for OPC UA

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

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

- [Beckhoff IPC System Health](#)
- [OPC UA Certificate](#)
- [OPC UA Custom](#)
- [OPC UA Server Status](#)

Credentials for OPC UA

☐ inherit from

Port ⓘ

4840

Server Path ⓘ

Security Mode ⓘ

☒ None (default)

☐ Sign

☐ Sign & Encrypt




Authentication Method ⓘ


☒ Anonymous (default)

☐ User name and password

Credentials for OPC UA

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

Setting	Description
	<ul style="list-style-type: none"> ▪ Sign & Encrypt: Sign and encrypt messages between the sensor and the OPC UA server.
Security Policy	<p>This setting is only visible if you select Sign or Sign & Encrypt above. Select if you want to use a security policy and define which policy you want to use:</p> <ul style="list-style-type: none"> ▪ None (default): Do not use a security policy. ▪ Basic256Sha256: Use the Basic256Sha256 security policy. ▪ Basic256: Use the Basic256 security policy.
Client Certificate	<p>This setting is only visible if you select Sign or Sign & Encrypt above. Enter the certificate that you created for authenticating the sensor against the OPC UA server.</p> <p> The certificate must meet the following requirements:</p> <ul style="list-style-type: none"> ▪ The key size must be 2048-bit. ▪ The secure hash algorithm must be SHA256. ▪ DataEncipherment must be part of the KeyUsage certificate extension. ▪ A uniform resource indicator (URI) must be set in subjectAltName. ▪ The certificate must be in Privacy-Enhanced Mail (PEM) format.
Client Key	<p>This setting is only visible if you select Sign or Sign & 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 & 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"> ▪ Anonymous (default): Connect without credentials. ▪ User name and password: Define credentials for the connection. <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 & 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](#)  ¹³⁵.

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

- [Soffico Orchestra Channel Health](#)

Credentials for Soffico Orchestra

☐ inherit from

Authentication Method ⁱ

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

Timeout (Sec.) ⁱ

60

Port ⁱ

8443

Protocol ⁱ

- ☒ 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"> None (default): Connect without credentials. User name and password: Define credentials for the connection.
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 300 seconds (5 minutes).
Port	Enter the port for the connection to the Orchestra platform. The default port for secure connections is 8443 and the default port for unsecure connections is 8019 .
Protocol	<p>Select the protocol that you want to use for the connection to the Orchestra platform:</p> <ul style="list-style-type: none"> ▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection. ▪ HTTP: Use an unsecure connection.

Credentials for Redfish

Click  to interrupt the [inheritance](#) .

 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 ⓘ
johnnpublic

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"> HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection. HTTP: Use an unsecure connection.
Port	Enter the port for the connection to the Redfish system. The default port for secure connections is 443 .

Credentials for REST API

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

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

▪ [REST Custom v2](#)

Credentials for REST API

Authentication Method ⓘ

☒ None (default)

☐ Basic authentication

☐ Bearer authentication

Credentials for REST API

Setting	Description
Authentication Method	<p>Select the authentication method for access to the Representational State Transfer (REST) application programming interface (API):</p> <ul style="list-style-type: none"> ▪ None (default): Use no authentication. ▪ Basic authentication: Use basic authentication. ▪ Bearer authentication: Use an OAuth2 bearer token.
User Name	This setting is only visible if you select Basic authentication above. Enter the user name for access to the REST API.
Password	This setting is only visible if you select Basic authentication above. Enter the password for access to the REST API.
Bearer Token	This setting is only visible if you select Bearer authentication above. Enter a bearer token for access to the REST API.
Placeholder 1 Description	Enter a description for Placeholder 1, for example information about the purpose or content of the placeholder.
Placeholder 1	Enter a value for the placeholder. PRTG inserts the value for the REST API request if you add <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 %restplaceholder3 in the Request URL, POST Body, and Custom Headers fields of the REST Custom v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 4 Description	Enter a description for Placeholder 4, for example information about the purpose or content of the placeholder.
Placeholder 4	Enter a value for the placeholder. PRTG inserts the value for the REST API request if you add %restplaceholder4 in the Request URL, POST Body, and Custom Headers fields of the REST Custom v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 5 Description	Enter a description for Placeholder 5, for example information about the purpose or content of the placeholder.
Placeholder 5	Enter a value for the placeholder. PRTG inserts the value for the REST API request if you add %restplaceholder5 in the Request URL, POST Body, and Custom Headers fields of the REST Custom v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.

Credentials for Veeam

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

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

- [Veeam Backup Job Status](#)
- [Veeam Backup Job Status Advanced](#)

Credentials for Veeam

User ⓘ

johnqpublic

Password ⓘ

.....

Port ⓘ

9398

Credentials for Veeam

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

Access Rights

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

Account Control

User Type ⓘ

☐ Read/write user
 ☒ Read-only user

Acknowledge Alarms ⓘ

☐ User can acknowledge alarms
 ☒ User cannot acknowledge alarms (default)

Password Change ⓘ

☐ User can change the account password
 ☒ User cannot change the account password (default)

Primary Group ⓘ

PRTG Users Group

Status ⓘ

☒ Active
 ☐ Paused

Last Login ⓘ

(has not logged in yet)

User Access Rights in User Accounts Settings

Setting	Description
User Group Access	<p>Select the user groups^[3346] that have access to the object. You see a table with user groups and group access rights. The table contains all user groups in your setup. For each user group, you can choose from the following group access rights:</p> <ul style="list-style-type: none"> ▪ Inherited: Inherit the access rights settings of the parent object. ▪ No access: Users in this user group cannot see or edit the object. The object neither shows up in lists nor in the device tree. <p> ⓘ 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.</p> ▪ Read access: Users in this group can see the object and view its monitoring results. They cannot edit any settings. ▪ Write access: Users in this group can see the object, view its monitoring results, and edit its settings. They cannot edit its access rights settings. ▪ Full access: Users in this group can see the object, view its monitoring results, edit its settings, and edit its access rights settings. <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 Access Rights Management^[144].</p>

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

More

KNOWLEDGE BASE

What security features does PRTG include?

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

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

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

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

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

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


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


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

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

7.2.3 Add a Device


There are several ways to manually add a device:

- Select Devices | Add Device from the [main menu bar](#)^[248]. A dialog appears that guides you through the process of adding a new device.
- Hover over  and select Add Device from the menu.
- Select Add Device from the [context menu](#)^[230] of the group to which you want to add the new device. This skips step 1 and leads you directly to [step 2](#)^[367].

 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:

- [Add a Device](#)^[365]
- [Step 1: Select a Parent](#)^[366]
- [Step 2: Define Device Settings](#)^[367]
- [Device Name and Address](#)^[368]
- [Device Identification and Auto-Discovery](#)^[370]
- [Inherited Settings](#)^[373]
- [Credentials for Windows Systems](#)^[373]
- [Credentials for Linux/Solaris/macOS \(SSH/WBEM\) Systems](#)^[376]
- [Credentials for VMware/XenServer](#)^[380]
- [Credentials for SNMP Devices](#)^[381]
- [Credentials for Database Management Systems](#)^[385]
- [Credentials for AWS](#)^[387]
- [Credentials for Script Sensors](#)^[388]
- [Credentials for Cisco Meraki](#)^[390]
- [Credentials for Dell EMC](#)^[390]
- [Credentials for FortiGate](#)^[391]
- [Credentials for HPE 3PAR](#)^[392]
- [Credentials for HTTP](#)^[394]
- [Credentials for Microsoft Azure](#)^[396]
- [Credentials for MQTT](#)^[397]
- [Credentials for NetApp](#)^[399]
- [Credentials for OPC UA](#)^[401]
- [Credentials for Soffico Orchestra](#)^[404]
- [Credentials for Redfish](#)^[406]

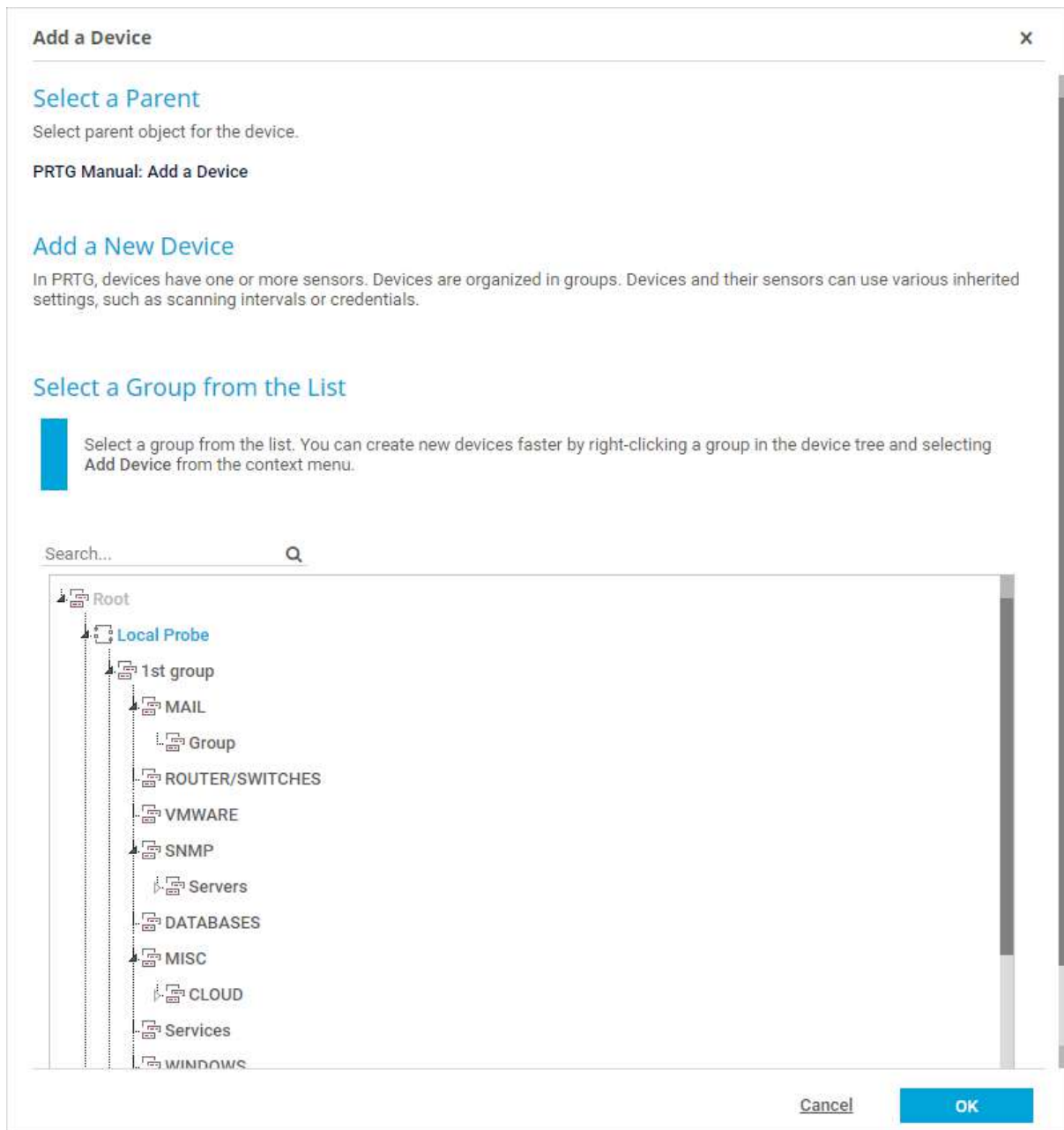
- [Credentials for REST API](#)  407
- [Credentials for Veeam](#)  409
- [Access Rights](#)  410

Add a Device

The Add a Device dialog appears when you add a new device to a group. It only shows the settings that are required to create the device. Therefore, you do not see all settings in this dialog.

- ① You can change all settings on the Settings tab of the device later. For more information, see section [Device Settings](#)  588.

Step 1: Select a Parent



Add Device Assistant Step 1

Select the group that you want to add the new device to. Click OK.

Step 2: Define Device Settings

Add Device to Group Local Probe

Add a New Device

Define a device name and IP address, options for auto-discovery, and credential settings for Windows, Linux, VMware/XenServer, SNMP, and specific vendors, if necessary.

PRTG Manual: Add a Device

Device Name and Address

Device Name ⓘ

Device

IP Version ⓘ

☒ IPv4

☐ IPv6

IPv4 Address/DNS Name ⓘ

This field is required.

Tags ⓘ

+

Device Icon ⓘ

Cancel
OK

Add Device Assistant Step 2

Device Name and Address

Device Name and Address

Device Name ⓘ

Device

IP Version ⓘ

☒ IPv4

☐ IPv6

IPv4 Address/DNS Name ⓘ

192.0.2.0

Tags ⓘ

+

Device Icon ⓘ

Device Name and Address

Setting	Description
Device Name	<p>Enter a name to identify the device. By default, PRTG shows this name in the device tree ^[164], as well as in alarms ^[199], logs ^[208], notifications ^[3173], reports ^[3192], maps ^[3214], libraries ^[3176], and tickets ^[211].</p> <p> ⓘ If the name contains angle brackets (<>), PRTG replaces them with braces ({} for security reasons. For more information, see the Knowledge Base: What security features does PRTG include?</p>
IP Version	<p>Select the IP protocol that PRTG uses to connect to the device:</p> <ul style="list-style-type: none"> ▪ IPv4: Use IP version 4 for all requests to the device.

Setting	Description
	<ul style="list-style-type: none"> IPv6: Use IP version 6 for all requests to the device. <p>i 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>i 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>i Some sensors have their own setting for the IP address/DNS name to which they connect.</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 inherited.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with parentheses (()) or angle brackets (<>).</p> <p>i For performance reasons, it can take some minutes until you can filter for new tags that you added.</p>
Device Icon	Select a device icon. PRTG shows it in the device tree.

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 auto-discovery ^[264]:</p> <ul style="list-style-type: none"> ▪ No auto-discovery: Select this option if you only want to manually create devices and sensors. ▪ Standard auto-discovery (recommended): Create a set of standard sensors for standard monitoring. This option works fine for most installations. ▪ 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. ▪ 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. <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"> ▪ Once: Run the auto-discovery only once. PRTG adds new devices and sensors once. If you select this option, you must manually start the auto-discovery ^[265].

Setting	Description
	<ul style="list-style-type: none"> Hourly: Run the auto-discovery for new devices and sensors every 60 minutes.  Use this option with caution. Frequent auto-discoveries might cause performance issues, in particular when PRTG scans large network segments every hour. 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 Monitoring settings, section Auto-Discovery. 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. <p> 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> 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"> ADSL Amazon CloudWatch Buffalo TeraStation NAS Cisco ASA VPN Cisco Device (Generic) Dell EqualLogic Dell MDi Disk DNS Server Environment Jakarta Environment Poseidon FTP Server Generic Device (Ping Only) Generic Device (SNMP Enabled) Generic Device (SNMP Enabled, Detailed) HTTP Web Server

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

Setting	Description
	<ul style="list-style-type: none"> Windows (Detailed via WMI) Windows (via Remote PowerShell) Windows (via WMI) Windows IIS (via SNMP) XenServer Hosts XenServer Virtual Machines <p>Once the auto-discovery is finished, PRTG creates a new ticket^[211] 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](#)^[419] if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#)^[135].

Credentials for Windows Systems

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

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

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

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

Credentials for Windows Systems



inherit from

Domain or Computer Name ⁱ

www.example.com

User Name ⁱ

johnqpublic

Password ⁱ

.....

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"> ▪ Password: Provide the password for the login. ▪ Private key: Provide an RSA private key for authentication. <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 Monitoring via SSH ^[3437].</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 BEGIN and END 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 Monitoring via SSH ^[3437].</p> <p> If you do not insert a private key for the first time but if you want to change the private key, you need to restart the PRTG core server service ^[3352] for the private key change to take effect.</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"> ▪ HTTP: Use an unsecure connection for WBEM. ▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection for WBEM. <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"> ▪ Default: Use one of the default ports. The default port for unsecure connections is 5988 and the default port for secure connections is 5989. ▪ Custom: Use a custom port.

Setting	Description
	<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 22.</p> <p> By default, PRTG automatically uses this setting for all SSH sensors ^[3683] 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"> ▪ Run the command as the connecting user (default): Use the rights of the user who establishes the SSH connection. ▪ Run the command as a different user using 'sudo' (with password): Use the rights of a different user with a password required for sudo to run commands on the target system, for example, as a root user. ▪ Run the command as a different user using 'sudo' (without password): Use the rights of a different user without a password required for sudo to run commands on the target system, for example, as a root user. ▪ Run the command as a different user using 'su': Use the rights of a different user with su to run commands on the target system.
Target System User Name	This setting is only visible if you select an option that includes sudo or su above. Enter a user name to run the specified command on the target system as a different user than the root user. If you leave this field empty, you run the command as a root user. Make sure that you set the Linux password even if you use a public key or a private key for authentication. This is not necessary if the user is allowed to run the command without a password.
Password	This setting is only visible if you select an option that includes sudo or su with password above. Enter the password to run the sudo command or the su command.
SSH Connection Mode	<p>Select the connection mode that you want to use to access data with SSH sensors ^[3437].</p> <ul style="list-style-type: none"> ▪ Default (recommended): This is the default connection mode for SSH sensors. It provides the best performance and security. ▪ Compatibility mode (deprecated): Use this only if the default connection mode does not work on the target system. The compatibility mode is the connection mode that PRTG used in previous versions and it is deprecated.

Setting	Description
	<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"> ▪ HTTPS (recommended): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection. ▪ HTTP: Use an unsecure connection.
Session Handling	<p>Select if you want to reuse a session for VMware sensors:</p> <ul style="list-style-type: none"> ▪ Reuse a session for multiple scans (recommended): Select this option if you want a VMware sensor to reuse a single session for multiple sensor scans to query data. With this option, the sensor does not need to log in and out for each sensor scan. We recommend that you use this option because it reduces network load and log entries on the target device. This can increase performance. ▪ Create a new session for each scan: If you select this option, PRTG does not reuse a session and a VMware sensor has to log in and out for each sensor scan. This can decrease performance.

Credentials for SNMP Devices

Click  to interrupt the [inheritance](#) .

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

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

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

Credentials for SNMP Devices

☐ inherit from

SNMP Version ⓘ

- ☐ SNMP v1
- ☒ SNMP v2c (recommended)
- ☐ SNMP v3

Community String ⓘ

public

SNMP Port ⓘ

161




Timeout (Sec.) ⓘ

5

Credentials for SNMP Devices

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

Setting	Description
	<ul style="list-style-type: none"> ▪ SNMP v3: Use SNMP v3 for the connection. SNMP v3 provides secure authentication and data encryption. <p>i SNMP v3 has performance limitations because of the use of encryption. The main limiting factor is CPU power. Also keep in mind that SNMP v3, unlike SNMP v1 and v2c, does not scale with more CPU power. Because of this limitation, PRTG can only handle a limited number of requests per second so that you can use only a limited number of sensors using SNMP v3. If you see an increase in Interval Delay or Open Requests with the Probe Health sensor, distribute the load over multiple probes ^[362]. 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>i 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"> ▪ MD5: Use message-digest algorithm 5 (MD5) for authentication. ▪ SHA: Use Secure Hash Algorithm (SHA) for authentication. ▪ SHA-224: Use SHA-224 for authentication. ▪ SHA-256: Use SHA-256 for authentication. ▪ SHA-384: Use SHA-384 for authentication. ▪ SHA-512: Use SHA-512 for authentication. <p>i If you do not want to use authentication but you need SNMP v3, for example, because your device requires context, you can leave the Password field empty. In this case, PRTG uses SNMP_SEC_LEVEL_NOAUTH and it entirely deactivates authentication.</p> <p>i 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>i 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>i 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"> ▪ DES: Use Data Encryption Standard (DES) as the encryption algorithm. ▪ AES: Use Advanced Encryption Standard (AES) as the encryption algorithm. ▪ AES-192: Use AES-192 as the encryption algorithm. ▪ AES-256: Use AES-256 as the encryption algorithm. <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. Context 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 161.</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 300 seconds (5 minutes).</p>

Credentials for Database Management Systems

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

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

- [ADO SQL v2](#)
- [Microsoft SQL v2](#)
- [MySQL v2](#)
- [Oracle SQL v2](#)

▪ [PostgreSQL](#)

Credentials for Database Management Systems

☐ inherit from

Port ⓘ

☒ Default (recommended)
 ☐ Custom port for all database sensors

Authentication Method ⓘ



☒ Windows authentication with impersonation
 ☐ SQL server authentication

Timeout (Sec.) ⓘ

60

Credentials for Database Management Systems

Setting	Description
Port	<p>Select the port that PRTG uses for connections to the monitored databases:</p> <ul style="list-style-type: none"> ▪ Default (recommended): PRTG automatically determines the type of the database and uses the corresponding default port to connect. PRTG uses the following default ports: <ul style="list-style-type: none"> ▪ Microsoft SQL: 1433 ▪ MySQL: 3306 ▪ Oracle SQL: 1521 ▪ PostgreSQL: 5432 ▪ Custom port for all database sensors: Select this option if your database management systems do not use the default ports. Enter a custom port for database connections below. <p>ⓘ PRTG uses this custom port for all database sensors and for connections to all your databases.</p>


Setting	Description
Custom Port	<p>Enter a custom port for database connections. Enter an integer.</p> <p> PRTG uses this custom port for all database sensors and for connections to all your databases.</p>
Authentication Method	<p>Select the authentication method for the connection to the Structured Query Language (SQL) database:</p> <ul style="list-style-type: none"> Windows authentication with impersonation: PRTG uses the Windows credentials that you define in settings that are higher in the object hierarchy^[131], for example, in the settings of the parent device; for the database connection.  The user whose credentials PRTG uses needs to have permission to log in to the probe system with a database sensor. This is necessary for the impersonation. SQL server authentication: Use explicit credentials for database connections. Enter a user name and password below.
User Name	<p>This setting is only visible if you select SQL server authentication above. Enter the user name for the database connection.</p>
Password	<p>This setting is only visible if you select SQL server authentication above. Enter the password for the database connection.</p>
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is 300 seconds (5 minutes).</p>

Credentials for AWS

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

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

- [AWS Alarm v2](#)
- [AWS Cost](#)
- [AWS EBS v2](#)
- [AWS EC2 v2](#)
- [AWS ELB v2](#)
- [AWS RDS v2](#)

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

Credentials for AWS

☐ inherit from

Access Key ⓘ

Secret Key ⓘ

Credentials for AWS

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

Credentials for Script Sensors

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

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

- [EXE/Script](#)
- [EXE/Script Advanced](#)
- [Python Script Advanced](#)
- [SSH Script](#)
- [SSH Script Advanced](#)

Credentials for Script Sensors

☐ inherit from

Placeholder 1 Description ⓘ

Placeholder 1 ⓘ

Credentials for Script Sensors

Setting	Description
Placeholder 1 Description	Enter a description for Placeholder 1, for example information about the purpose or content of the placeholder.
Placeholder 1	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <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.

Setting	Description
Placeholder 5	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add %scriptplaceholder5 in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.


Credentials for Cisco Meraki


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

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


- [Cisco Meraki License](#)
- [Cisco Meraki Network Health](#)

Credentials for Cisco Meraki

 inherit from  Network Infrastructure


API Key 

.....

Meraki Dashboard API Endpoint 

api.meraki.com

Credentials for Cisco Meraki

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

Credentials for Dell EMC

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

 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 ⓘ

johnnpublic

Password ⓘ

.....

Port ⓘ

443

Credentials for Dell EMC

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

Credentials for FortiGate

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

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

- [FortiGate System Statistics](#)
- [FortiGate VPN Overview](#)

Credentials for FortiGate

☐ inherit from

API Token ⓘ

Port ⓘ

443

Credentials for FortiGate

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

Credentials for HPE 3PAR

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

ⓘ 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"> ▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection. ▪ HTTP: Use an unsecure connection.

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

Credentials for HTTP

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

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"> ▪ None (default): Use no authentication. ▪ Basic authentication: Use basic authentication. ▪ Bearer authentication: Use an OAuth2 bearer token.
User Name	This setting is only visible if you select Basic authentication above. Enter the user name for access to the server.


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


 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](#)  ¹³⁵.

 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 ⁱ

☒ None (default)

☐ Username/Password

Port ⁱ

1883




Transport-Level Security ⁱ

☒ 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"> None (default): Connect without credentials. User name and password: Define credentials for the connection.
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 8883 and the default port for unsecure connections is 1883.</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"> Do not use transport-level security: Establish the connection without connection security. Use transport-level security: Establish the connection with the strongest SSL/TLS method that the target device provides.
Server Authentication	<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"> Disable (default): Do not use a certificate for server authentication. Enable: Use a certificate for server authentication.
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"> Disable (default): Do not use a certificate for client authentication. Enable: Use a certificate for client authentication.
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