Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for Qualys QualysGuard File

Configuration Guide

October 17, 2017

Configuration Guide

SmartConnector for Qualys QualysGuard File

October 17, 2017

Warranty

Restricted Rights Legend

Revision History

Date	Description
10/17/2017	Added encryption parameters to Global Parameters.
08/15/2017	Replaced "arcsight connectorsetup" command with "runagentsetup".
04/15/2017	Updated troubleshooting information for out of memory error.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
02/16/2015	Added additional proxy configuration information to the Troubleshooting section.
02/14/2014	Added support for versions 7.11 and 7.12.
08/15/2013	Added support for version 7.9. Added and updated mappings.
02/15/2013	Added support for version 7.7. Added and updated mappings.
11/15/2012	Added support for version 7.4. Added and updated mappings.
08/15/2012	Added support for version 7.1. Added and updated mappings.

Contents

SmartConnector for Qualys QualysGuard File

This guide provides information for installing the SmartConnector for Qualys QualysGuard File for report event collection. This SmartConnector is supported on platforms that support Java 1.3 or later. QualysGuard versions 4.0, 4.7, 5.0, 6.0, 6.5, 6.19, 7.0, 7.1, 7.4, 7.7, 7.9, 7.11, and 7.12 are supported.

Product Overview

Qualys QualysGuard is an on demand solution that enables organizations to discover and prioritize all network assets; proactively identify and fix security vulnerabilities; prevent worms, viruses and trojan horses; manage and reduce business risk; and ensure compliance with laws, regulations and corporate security policies.

The SmartConnector for QualysGuard is an XML connector. It connects to the Qualys web interface (over HTTPS) to retrieve reports and sends the information to the ArcSight ESM Manager.

Configuration

During the installation process, you will be asked to fill in a number of parameters. To be prepared:

- If Qualys requires a Client Certificate, you will need access to the client certificate `.pfx` or `.jkcs` file. The installation wizard asks you for the certificate type, path, and password, and will ask you to download and save the client certificate to a particular location.
- The name of a user with authority to gain access to the report repository and the password for this user will be required.
- The URL used to retrieve stored reports as well as the URL used to retrieve the list of stored reports will be required.
- If you will be going through a proxy, you will select `true` for "Proxy Server Used" and you also will be asked to provide the IP address or host name and port number for the proxy server, as well as the user name and password for proxy authentication.

You also will be asked to select one of two operational modes:

- **Interactive** – This mode is designed to be used by an operator who requires only certain reports to be sent to ArcSight ESM. In this mode, the connector first retrieves a list of reports stored in the user's Qualys account (unsent), and presents it in a UI window where the user can select the scan reports to be sent to the ArcSight ESM Manager. After making a selection, clicking on the **Send** button sends all the selected scanner reports to ArcSight ESM. Closing the window when all the desired scans have been sent terminates the connector. In this mode, the connector should not be run as a daemon/service, only as a standalone application.
- **Automatic** – This mode is designed to automatically import the reports from Qualys to the ArcSight ESM Manager whenever a new report is generated. In this mode, the connector periodically checks for any new scan reports. When the connector detects that a new scan has been successfully completed, it sends the report to the ArcSight ESM Manager. The connector can run as a service in this mode since it is designed to run in unattended mode.

Install the SmartConnector

The following sections provide instructions for installing and configuring your selected SmartConnector.

Connector Appliance/ArcSight Management Center supports mounting for Network File System (NFS) and CIFS (Windows) shares. When you install this connector on one of these devices, establish a CIFS mount on the device before adding the connector. Provide this share name during connector configuration. For more information, see **Remote File Systems** in the Connector Appliance or ArcSight Management Center Administrator's Guide.

Prepare to Install Connector

Before you install any SmartConnectors, make sure that the ArcSight products with which the connectors will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger).

For complete product information, read the *Administrator's Guide* as well as the *Installation and Configuration* guide for your ArcSight product before installing a new SmartConnector. If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* for instructions, and start the installation procedure at "Set Global Parameters (optional)" or "Select Connector and Add Parameter Information."

Before installing the SmartConnector, be sure the following are available:

- Local access to the machine where the SmartConnector is to be installed
- Administrator passwords

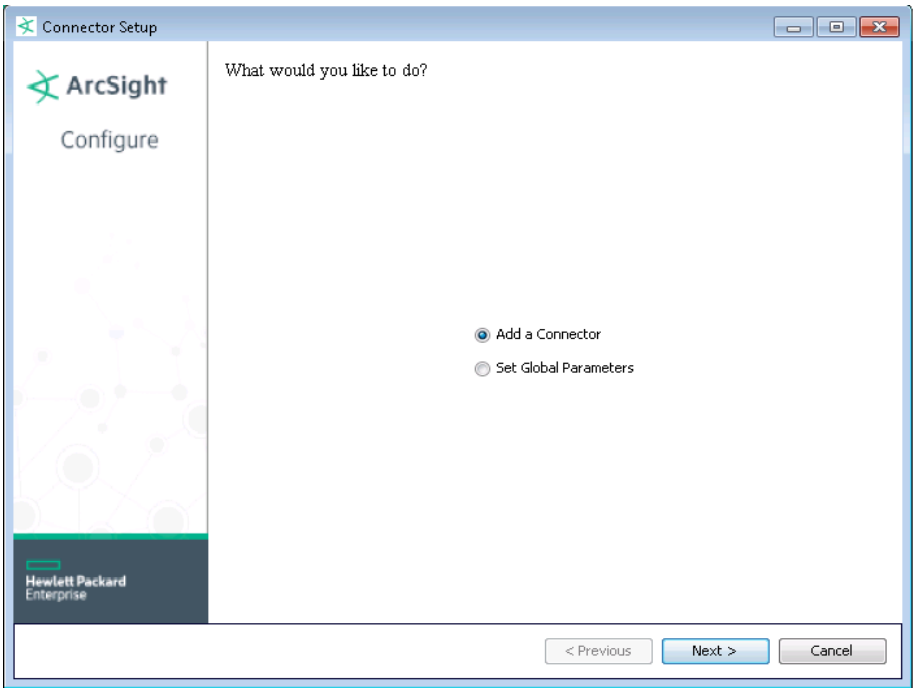
Install Core Software

Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms; for the complete list, see the *SmartConnector Product and Platform Support* document, available from the HPE SSO and Protect 724 sites.

1. Download the SmartConnector executable for your operating system from the HPE SSO site.
2. Start the SmartConnector installation and configuration wizard by running the executable.

   Follow the wizard through the following folder selection tasks and installation of the core connector software:

   Introduction
   Choose Install Folder
   Choose Shortcut Folder
   Pre-Installation Summary
   Installing...
3. When the installation of SmartConnector core component software is finished, the following window is displayed:



Next, you will need to download and save the license file for this SmartConnector.

A Click **Cancel** to exit the wizard at this point. Next, create a `Qualys` folder at the following location:

```
$ARCSIGHT_HOME/current/user/agent/Qualys
```

B Download and save the client certificate .pfx or .jkcs file to the `Qualys` directory you just created. Contact Qualys support for this certificate file. The name of and path to the client certificate file is needed during SmartConnector setup.

C From `$ARCSIGHT_HOME/bin`, enter `runagentsetup` to return to the SmartConnector Configuration Wizard.

Set Global Parameters (optional)

If you choose to perform any of the operations shown in the following table, do so before adding your connector. You can set the following parameters:

Parameter	Setting
FIPS mode	Select 'Enabled' to enable FIPS compliant mode. To enable FIPS Suite B Mode, see the SmartConnector User Guide under "Modifying Connector Parameters" for instructions. Initially, this value is set to 'Disabled'.
Remote Management	Select 'Enabled' to enable remote management from ArcSight Management Center. When queried by the remote management device, the values you specify here for enabling remote management and the port number will be used. Initially, this value is set to 'Disabled'.
Remote Management Listener Port	The remote management device will listen to the port specified in this field. The default port number is 9001.
Preferred IP Version	When both IPv4 and IPv6 IP addresses are available for the local host (the machine on which the connector is installed), you can choose which version is preferred. Otherwise, you will see only one selection. The initial setting is IPv4.

The following parameters should be configured only if you are using HPE SecureData solutions to provide encryption. See the *HPE SecureData Architecture Guide* for more information.

Parameter	Setting
Format Preserving Encryption	Data leaving the connector machine to a specified destination can be encrypted by selecting 'Enabled' to encrypt the fields identified in 'Event Fields to Encrypt' before forwarding events. If encryption is enabled, it cannot be disabled. Changing any of the encryption parameters again will require a fresh installation of the connector.
Format Preserving Policy URL	Enter the URL where the HPE SecureData Server is installed.
Proxy Server (https)	Enter the proxy host for https connection if any proxy is enabled for this machine.
Proxy Port	Enter the proxy port for https connection if any proxy is enabled for this machine.
Format Preserving Identity	The HPE SecureData client software allows client applications to protect and access data based on key names. This key name is referred to as the identity. Enter the user identity configured for HPE SecureData.
Format Preserving Secret	Enter the secret configured for HPE SecureData to use for encryption.
Event Fields to Encrypt	Recommended fields for encryption are listed; delete any fields you do not want encrypted and add any string or numeric fields you want encrypted. Encrypting more fields can affect performance, with 20 fields being the maximum recommended. Also, because encryption changes the value, rules or categorization could also be affected. Once encryption is enabled, the list of event fields cannot be edited.

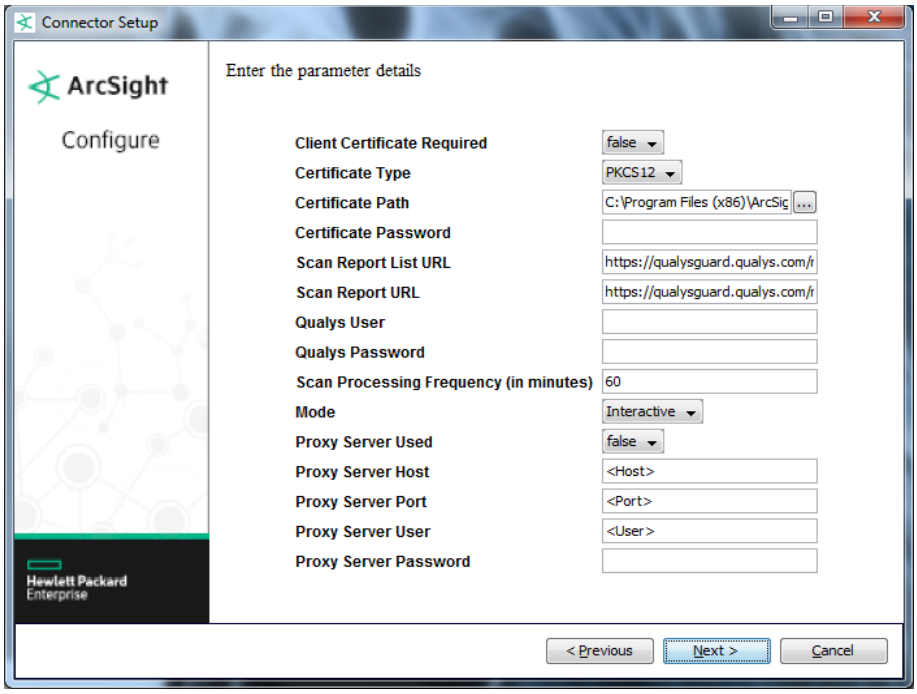
After making your selections, click **Next**. A summary screen is displayed. Review the summary of your selections and click **Next**. Click **Continue** to return to proceed with "Add a Connector" window. Continue the installation procedure with "Select Connector and Add Parameter Information."

Select Connector and Add Parameter Information

1. Select **Add a Connector** and click **Next**. If applicable, you can enable FIPS mode and enable remote management later in the wizard after SmartConnector configuration.

2. Select **Qualys QualysGuard File** and click **Next**.

3. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



Parameter	Description
Client Certificate Required	Select 'True' if Qualys requires the connector to present an SSL client certificate; otherwise, select 'False'.
Certificate Type	Select the SSL Keystore type, PKCS12 or JKCS. (Ignore this parameter if Qualys does not require SSL client certificate.)
Certificate Path	Enter the SSL Keystore file path and name. This can be the path to the certificate or a keystore containing the certificate. In either case, this file must be present in the folder or subfolders of the folder in which the ArcSight SmartConnector is installed. Otherwise, the connector is unable to pick up the certificate. (Ignore this parameter if Qualys does not require SSL client certificate.)
Certificate Password	Enter the SSL Keystore password. (Ignore this parameter if Qualys does not require SSL client certificate.)
Scan Report List URL	Enter the URL used to retrieve the list of stored reports. By default, this is set to 'https://qualysguard.qualys.com/msp/scan_report_list.php'. When Qualys requires a client certificate, this should be set to 'https://certs.qualysguard.qualys.com/msp/scan_report_list.php'.
Scan Report URL	Enter the URL used to retrieve stored reports, given the report ID. By default, this is set to 'https://qualysguard.qualys.com/msp/scan_report.php'. When Qualys requires a client certificate, this should be set to 'https://certs.qualysguard.qualys.com/msp/scan_report.php'.
Qualys User	Enter the name of a user with authority to gain access to the report repository.
Qualys Password	Enter the password for the above user.
Scan Processing Frequency (in minutes)	Enter the desired scan processing frequency for Automatic mode in minutes.
Mode	Select Interactive or Automatic. In Interactive mode, a graphical UI is displayed showing the reports available for sending to the ArcSight ESM Manager. In Automatic mode, the new reports are sent automatically to the ArcSight ESM Manager.
Proxy Server Used	Select true if a proxy is used; otherwise, leave the default value of false.

Parameter	Description
Proxy Server Host	Enter the IP Address or Host Name for the Internet Proxy Server (required only when you will go through a proxy).
Proxy Server Port	Enter the number of the port on which Internet Proxy Server is running the proxy service (required only when you will go through a proxy).
Proxy Server User	Enter the User Name used by Internet Proxy Server for proxy authentication (needed only if your proxy uses basic authentication.)
Proxy Server Password	Enter the password for the Proxy Server User (needed only if your proxy uses basic authentication).

Note: For more information about proxy configuration, see the Troubleshooting section under the topic: "Communication with the Qualys URL cannot be established. What can I do?"

Select a Destination

1. The next window asks for the destination type; select a destination and click **Next**. For information about the destinations listed, see the *ArcSight SmartConnector User Guide*.

2. Enter values for the destination. For the ArcSight Manager destination, the values you enter for **User** and **Password** should be the same ArcSight user name and password you created during the ArcSight Manager installation. Click **Next**.

3. Enter a name for the SmartConnector and provide other information identifying the connector's use in your environment. Click **Next**. The connector starts the registration process.

4. If you have selected ArcSight Manager as the destination, the certificate import window for the ArcSight Manager is displayed. Select **Import the certificate to the connector from destination** and click **Next**. (If you select **Do not import the certificate to connector from destination**, the connector installation will end.) The certificate is imported and the **Add connector Summary** window is displayed.

Complete Installation and Configuration

1. Review the **Add Connector Summary** and click **Next**. If the summary is incorrect, click **Previous** to make changes.

2. The wizard now prompts you to choose whether you want to run the SmartConnector as a stand-alone process or as a service. If you choose to run the connector as a stand-alone process, select **Leave as a standalone application**, click **Next**, and continue with step 5.

3. If you chose to run the connector as a service, with **Install as a service** selected, click **Next**. The wizard prompts you to define service parameters. Enter values for **Service Internal Name** and **Service Display Name** and select **Yes** or **No** for **Start the service automatically**. The **Install Service Summary** window is displayed when you click **Next**.

4. Click **Next** on the summary window.

5. To complete the installation, choose **Exit** and Click **Next**.

For instructions about upgrading the connector or modifying parameters, see the *SmartConnector User Guide*.

Run the SmartConnector

SmartConnectors can be installed and run in stand-alone mode, on Windows platforms as a Windows service, or on UNIX platforms as a UNIX daemon, depending upon the platform supported. On Windows platforms, SmartConnectors also can be run using shortcuts and optional Start menu entries.

If the connector is installed in stand-alone mode, it must be started manually and is not automatically active when a host is restarted. If installed as a service or daemon, the connector runs automatically when the host is restarted. For information about connectors running as services or daemons, see the *ArcSight SmartConnector User Guide*.

To run all SmartConnectors installed in stand-alone mode on a particular host, open a command window, go to `$ARCSIGHT_HOME\current\bin` and run: `arcsight connectors`

To view the SmartConnector log, read the file `$ARCSIGHT_HOME\current\logs\agent.log`; to stop all SmartConnectors, enter `Ctrl+C` in the command window.

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See the *ArcSight Console User's Guide* for more information about the ArcSight data fields.

Qualys Infos Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Very High = Urgent; High = Critical, Serious; Medium = Medium; Low = Minimal
Destination Address	IPvalue
Destination Host Name	One of (NetbiosHostName, IPname)
Destination Port	Port
Device Custom String 1	Result
Device Custom String 2	CVEID
Device Custom String 3	Diagnosis
Device Custom String 4	Consequence
Device Custom String 5	Solution
Device Event Category	EventCategory
Device Event Class ID	concatenate("Qualys|","INFOS|",Number)
Device Product	'Qualys'
Device Receipt Time	Date
Device Severity	Severity, (1 = Minimal, 2 = Medium, 3 = Serious, 4 = Critical, 5 = Urgent)
Device Vendor	'Qualys'
Name	TITLE
Old File Path	_FILE_PATH
Transport Protocol	Protocol

Qualys Practices Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Additional Data	ExpltDescription
Agent (Connector) Severity	Very High = Urgent; High = Critical, Serious; Medium = Medium; Low = Minimal
Destination Address	IPvalue
Destination Host Name	One of (IPname, NetbiosHostName)
Destination Port	Port
Device Custom String 1	Result
Device Custom String 2	CVEID
Device Custom String 3	Diagnosis
Device Custom String 4	Consequence
Device Custom String 5	Solution
Device Custom String 6	CVSSBaseScore
Device Event Category	EventCategory
Device Event Class ID	concatenate("Qualys|","PRACTICES|",Number)
Device Product	'Qualys'
Device Receipt Time	Date
Device Severity	Severity (1 = Minimal, 2 = Medium, 3 = Serious, 4 = Critical, 5 = Urgent)
Device Vendor	'Qualys'
Name	TITLE
Old File Path	_FILE_PATH
Transport Protocol	Protocol

Qualys Open Ports Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Very High = 5; High = 3,4; Medium = 2; Low = 1
Category Technique	Vulnerability Category
Destination Address	IPvalue
Destination Host Name	One of (IPname, NetbiosHostname)
Device Custom String 1	Result
Device Domain	'Network'
Device Event Class ID	concatenate("Qualys|","Open Port|",Number)
Device Product	'Qualys'
Device Receipt Time	Date
Device Severity	Severity
Device Vendor	'Qualys'
Device Version	Version
Name	'Open Port'
Old File Path	_FILE_PATH
Transport Protocol	Protocol

Qualys Scanner Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Destination Address	value
Target Host Name	One of (NetbiosHostName, name)

Qualys Services Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Very High= 5; High = 3,4,; Medium = 2; Low = 1
Destination Address	IPvalue
Destination Host Name	One of (IPname, NetbiosHostName)
Destination Port	Port
Device Custom String 1	Result
Device Custom String 3	Diagnosis
Device Custom String 4	Consequence
Device Custom String 5	Solution
Device Domain	'Network'
Device Event Category	EventCategory
Device Event Class ID	concatenate("Qualys|","Services|",Number)
Device Product	'Qualys'
Device Receipt Time	Date
Device Severity	Severity
Device Vendor	'Qualys'
Device Version	Version
Name	Service
Old File Path	_FILE_PATH
Transport Protocol	Protocol

Qualys URIs Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Very High= 5; High = 3,4; Medium = 2; Low = 1
Category Technique	Vulnerability Category
Destination Address	IPvalue
Destination Host Name	One of (IPname, NetbiosHostName)
Device Domain	'Network'
Device Event Class ID	concatenate("Qualys|","URI|",One of(OSName,OSDetected))
Device Product	'Qualys'
Device Receipt Time	Date
Device Severity	Severity
Device Vendor	'Qualys'
Device Version	Version
File Path	One of (OSName, OSDetected)
Name	Operating System; one of (OSName, OSDetected)

ArcSight ESM Field	Device-Specific Field
Old File Path	_FILE_PATH

Qualys Vulnerability Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Additional data	ExpltDescription
Agent (Connector) Severity	Very High= 5; High = 3,4,; Medium = 2; Low = 1
Category Technique	Vulnerability Category
Destination Address	IPvalue
Destination Host Name	One of (IPname, NetbiosHostName)
Destination Port	Port
Device Custom String 1	Result
Device Custom String 2	CVEID
Device Custom String 3	Diagnosis
Device Custom String 4	Consequence
Device Custom String 5	Solution
Device Custom String 6	CVSSBaseScore
Device Domain	'Network'
Device Event Category	EventCategory
Device Event Class ID	Concatenate("Qualys", Number, TITLE, Severity, Diagnosis, Consequence, Solution, CVEID")
Device Product	'Qualys'
Device Receipt Time	Date
Device Severity	Severity
Device Vendor	'Qualys'
Device Version	Version
Name	Both ("Vulnerability:", Number)
Old File Path	_FILE_PATH
Transport Protocol	Protocol

Troubleshooting

Why do I get an 'Invalid credentials' error?

The username and password entered do not match the information in the database. Check to make sure the information you entered is correct. Usernames and passwords are case sensitive, so make sure Caps Lock is turned off. If Certificate Authentication is enabled for your account, then several additional validation checks occur. You will get an "Invalid credentials" error if you do not meet these conditions:

- A certificate is present in your browser.
- The certificate in your browser is not expired.

- The email address in the certificate in your browser matches the email address in your QualysGuard user account.
- The issuer ID in the certificate in your browser matches the issuer ID in the certificate provided to Qualys for the subscription.

The exact method of implementing authentication will vary according to which programming language is used; see the "Sample API Code" section of the *QualysGuard API User Guide* for details.

My SmartConnector throws an out-of-memory error. What should I do in this case?

The SmartConnector can throw an out-of-memory error when the xml data file is too large. This error is due to the amount of temporary memory required while attempting to build the document.

If the SmartConnector is running as an application, you can resolve this problem by increasing the java heap size in `$ARCSIGHT_HOME\current\bin\scripts\Connectors.bat` or `Connectors.sh`.

The name of the argument for Windows is:

```
ARCSIGHT_MEM_OPTIONS= -Xms256m -Xmx256m
```

The name of the argument for other platforms is:

```
ARCSIGHT_MEMORY_OPTIONS= -Xms256m -Xmx256m
```

The max value should be changed.

Or

If the SmartConnector is running as a service, you can resolve this problem by increasing the java heap size in `$ARCSIGHT_HOME\current\user\agent\agent.wrapper.conf`. The name of the property is:

```
wrapper.java.maxmemory=256
```

Following are some performance measurements from a development environment indicating conditions that may throw an out-of-memory error:

- Data files larger than 50MB for 256MB java heap size
- Data files larger than 125MB for 512MB java heap size
- Data files larger than 300MB for 1024MB java heap size

Split the scanning of any large number of assets into multiple smaller chunks so that a set of small XML reports are created rather than one large XML file.

Communication with the Qualys URL cannot be established. What can I do?

There is a known issue with the connector framework attempting to access the Internet directly, even when you specify proxy settings during connector setup. This causes communication to the Qualys URL to fail. To work around this problem, modify the following settings in the `$ARCSIGHT_HOME/current/jre/lib/net.properties` file:

```
http.proxyHost=<proxyHost>
http.proxyPort=<proxyPort>

https.proxyHost=<proxyHost>
https.proxyPort=<proxyPort>
```

The following property is applied to both HTTP and HTTPS connections automatically. There is no need to repeat it for each:

```
http.nonProxyHosts=localhost|127.0.0.1|<managerHost_or_IP>|<loggerHost_or
_IP>
```

If your Proxy server requires authentication, then also add the following properties:

This is NOT the same as Qualys authentication. This authentication is just for the proxy itself.

```
http.proxyUser=<ProxyUserNameInClearText>
http.proxyPassword=<ProxyPasswordInClearText>

https.proxyUser=<ProxyUserNameInClearText>
https.proxyPassword=<ProxyPasswordInClearText>
```

The connector will require a restart before any changes to the net.properties file will take affect.