Micro Focus Security ArcSight SmartConnectors

Software Version: 8.3.0

SmartConnector for HPE Operations Manager Incident Web Service

Document Release Date: February 2022
Software Release Date: February 2022

Legal Notices

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

https://www.microfocus.com

Copyright Notice

Trademark Notices

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

https://www.microfocus.com/support-and-services/documentation

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

Contents

SmartConnector for HPE Operations Manager Incident Web Service

SmartConnector for HPE Operations Manager Incident Web Service

This guide provides information for installing the SmartConnector for HPE Operations Manager Incident Web Service and configuring the device for event collection. This connector is included in the SmartConnectors installation executable. There is no separate install executable for this SmartConnector. For supported devices and versions, see Technical Requirements.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight SmartConnectors.

Additional Documentation

The ArcSight SmartConnectors documentation library includes the following resources:

- *Installation Guide for ArcSight SmartConnectors*, which provides detailed information about installing SmartConnectors.
- *Configuration Guides for ArcSight SmartConnectors*, which provides information about configuring SmartConnectors to collect events from different sources.
- *Release Notes for ArcSight SmartConnectors*, which provides information about the latest release

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the documentation site for ArcSight SmartConnectors.

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to Documentation-Feedback@microfocus.com.

For specific product issues, contact Micro Focus Customer Care.

Product Overview

HPE Operations Manager (HPE OM) provides comprehensive event management, proactive performance monitoring, and automated alerting, reporting, and graphing for operating systems, middleware, and applications. HPE Operations Manager software acts as the consolidated enterprise operations console for your IT infrastructure. It monitors both physical and virtual servers to identify the cause of event storms, allowing faster time to resolution.

The messages generated by HPE OM are retrieved through HPE OM's Incident Web Service and forwarded into the ArcSight System.

Configure Operations Manager for Event Collection

The SmartConnector can validate Operation Manager's authentication certificate. To operate in this configuration, first get the certificate from Operations Manager, then import it into the SmartConnector Java Runtime Environment (JRE) during the connector installation process, prior to running the SmartConnector.

The following steps presume you have configured Operations Manager to let the SmartConnector communicate with it. If you have not done so, see your HPE documentation for information about the configuration of access lists or allowed hosts.

Obtain the Authentication Certificate

HPE recommends that you connect to the HPE OM Web Services using HTTPS connections, which require a suitable certificate on the server. Although the Incident Web Service can listen to both HTTP and HTTPS at the same time, the SmartConnector always attempts to connect through HTTPS. Both the Incident Web Service and its certificate are components generally installed on the HPE OM server by default. The port that the service uses for HTTPS communication depends upon the configuration of the HPE OM server. The default HTTPS port number on HPE OM on UNIX or Linux is 8444. For Windows, the default port is 443.

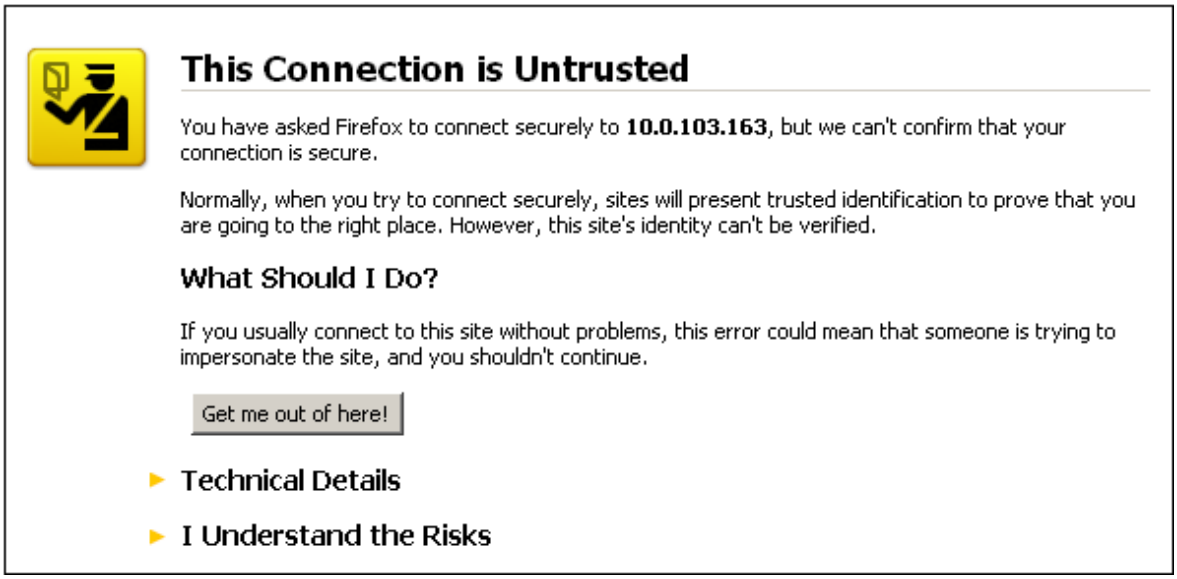
For further security, HPE recommends you verify the hostname and certificate for each HTTPS connection. To verify the certificate for an HTTPS connection, the client system must trust the server's certificate. You will export the server's certificate and import it to the SmartConnector system.

On Windows

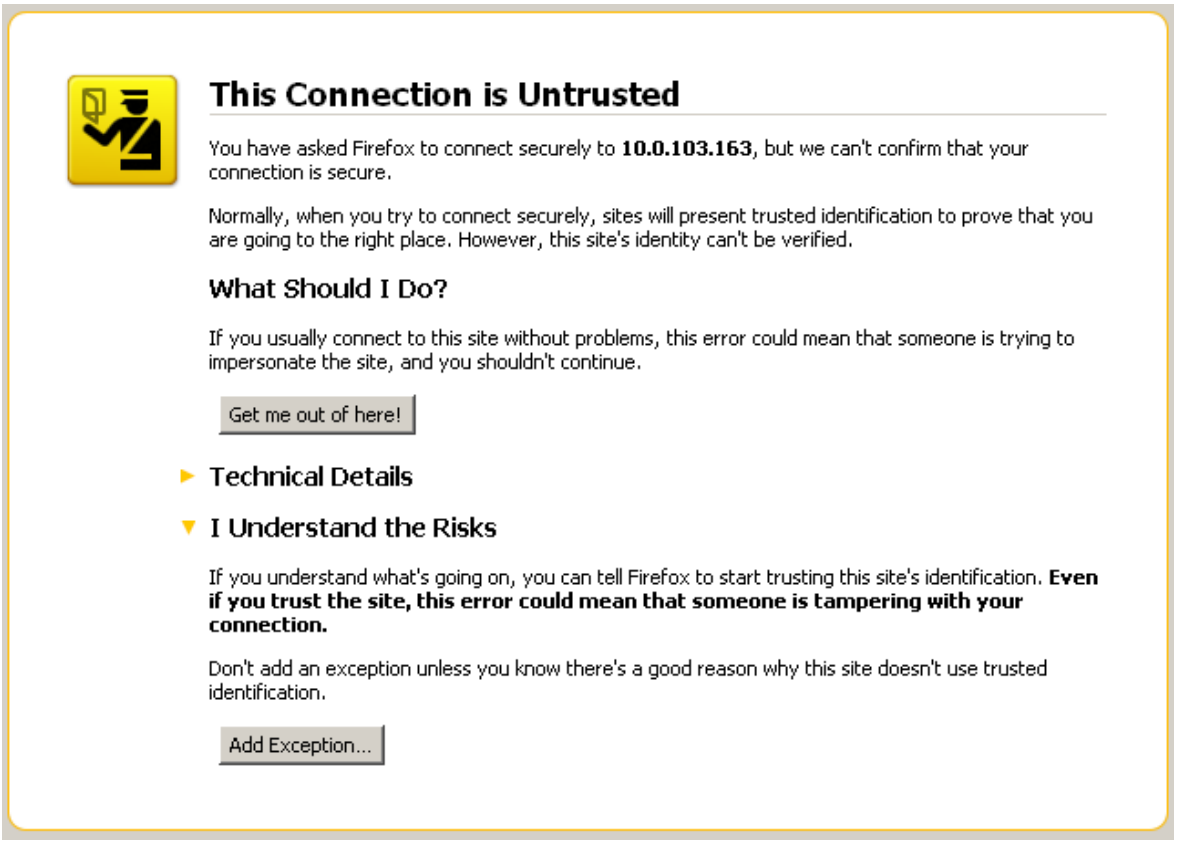
The examples in the following procedure use Mozilla Firefox.

To export the Incident Web Service certificate using Windows:

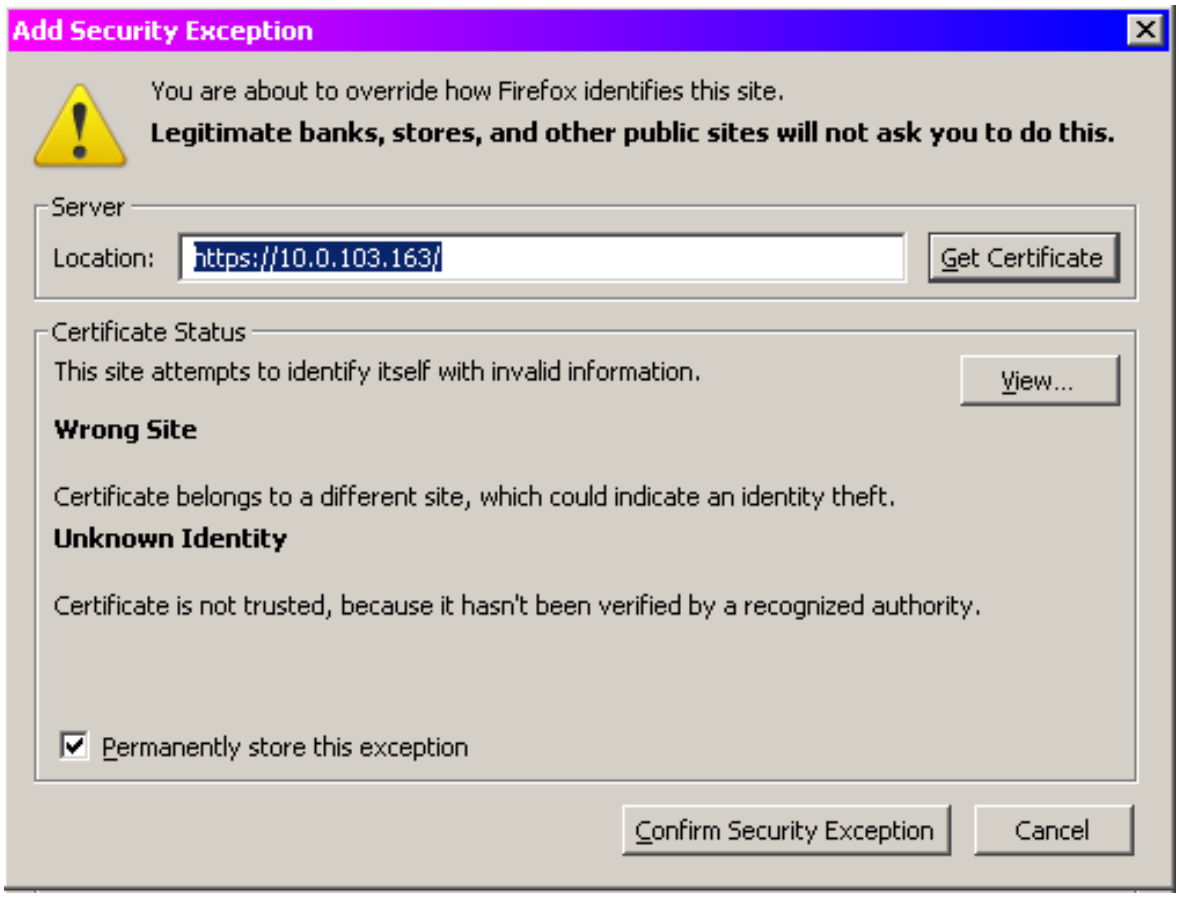
1 Enter the HPE OM server IP address in your browser.



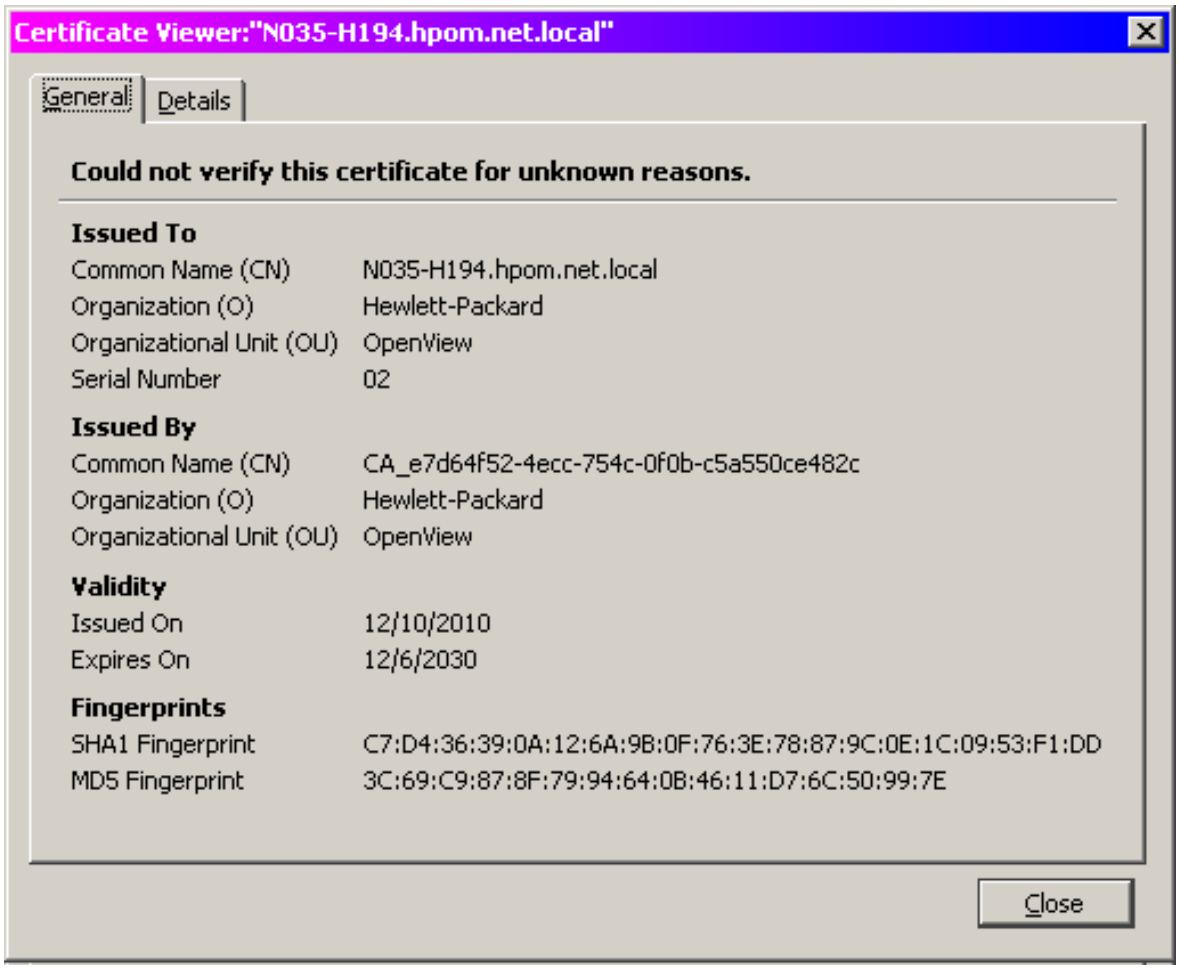
2 Click **I Understand the Risks**.



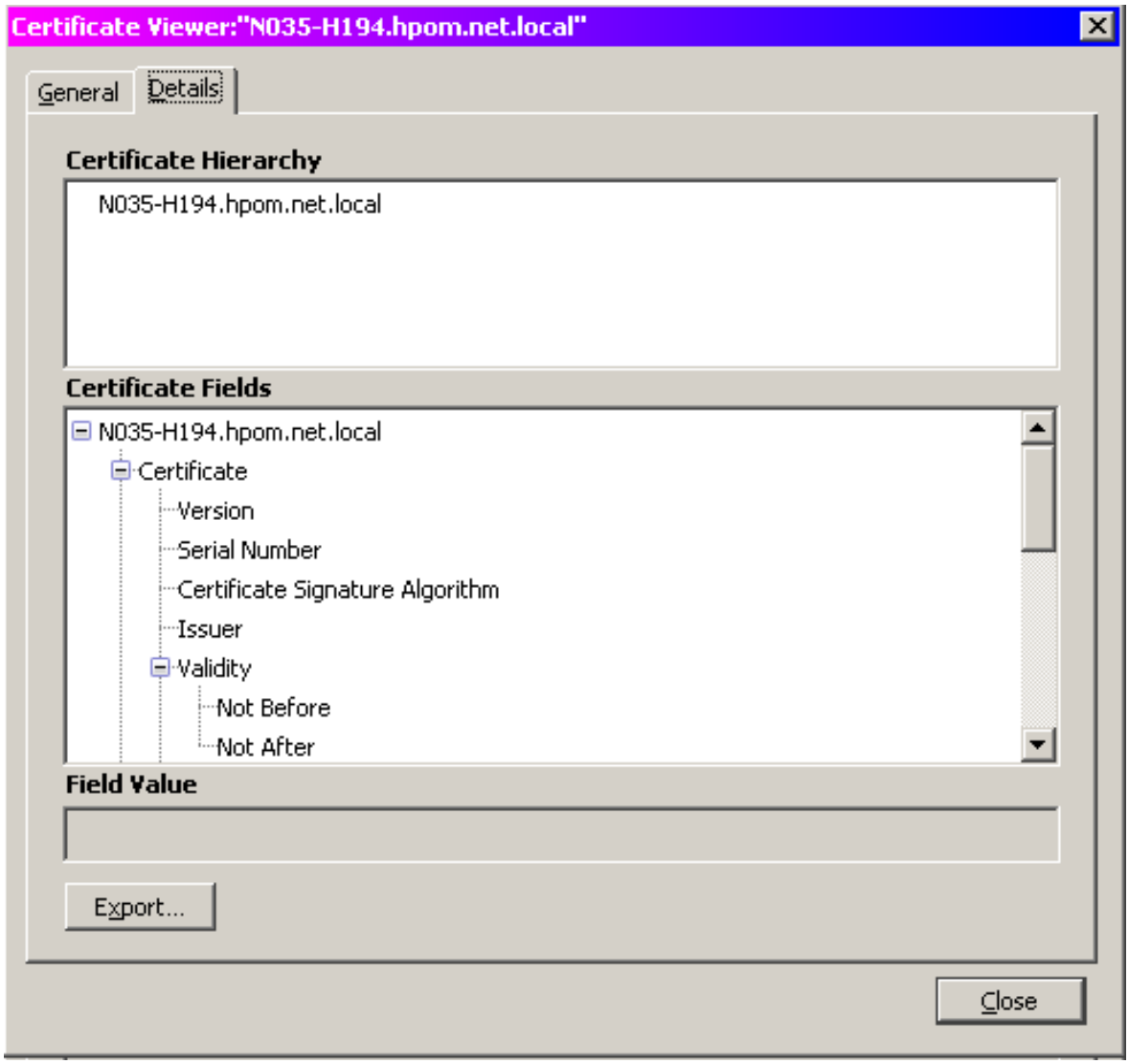
3 Click **Add Exception...**.


Add Security Exception
You are about to override how Firefox identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.
Server
Location:
https://10.0.103.163/
Get Certificate
Certificate Status
This site attempts to identify itself with invalid information.
View...
Wrong Site
Certificate belongs to a different site, which could indicate an identity theft.
Unknown Identity
Certificate is not trusted, because it hasn't been verified by a recognized authority.
Permanently store this exception
Confirm Security Exception
Cancel

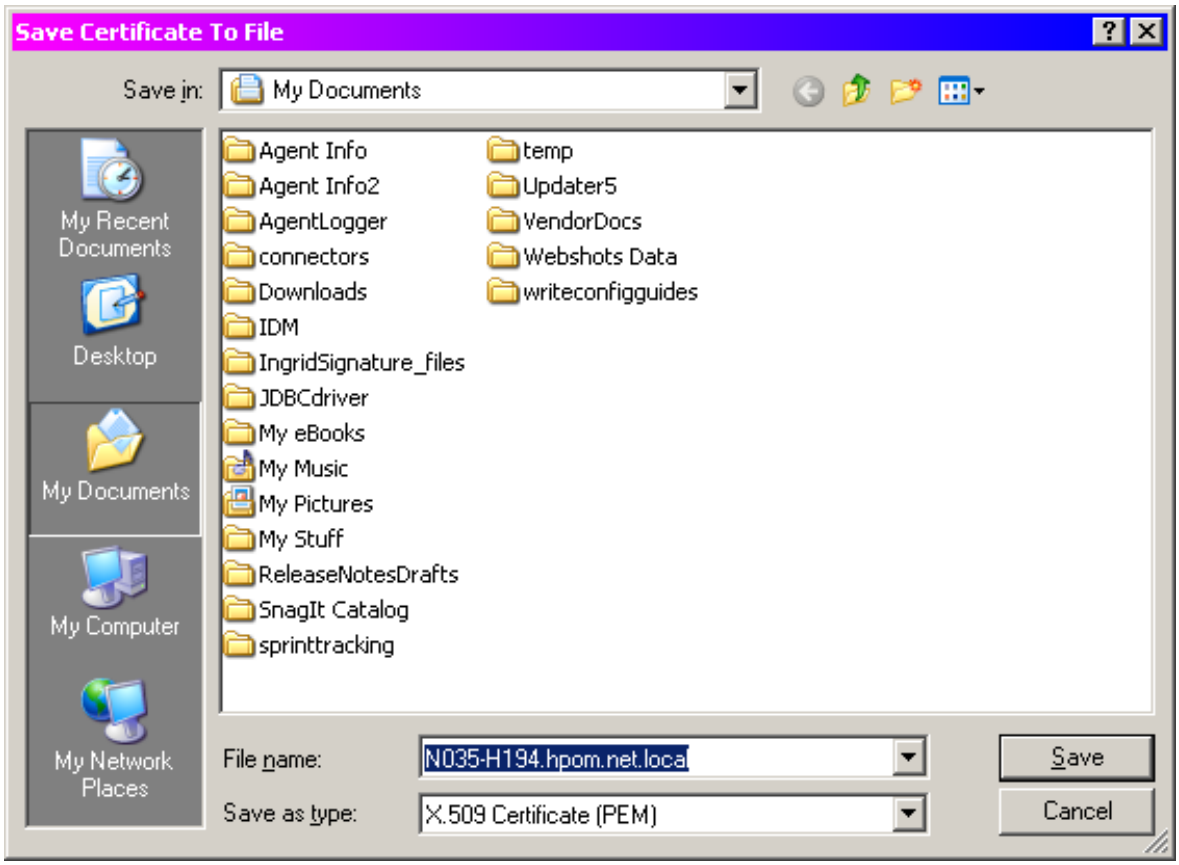
4 Click **View...**.



5 Click the **Details** tab.



6 Click **Export...**.



7 Navigate to the folder into which you want to save the certificate; click Save.

On Linux

To export the server's certificate from your management server:

1 Open a shell and navigate to the directory containing the keystore file:

```
/var/opt/OV/certificates/tomcat/b
```

2 Issue the following command to determine the keystore list containing the certificate:

```
/opt/OV/nonOV/jre/b/bin/keytool -keystore tomcat.keystore -list
```

3 When prompted, enter the default password `changeit`. Keystore information such as shown in the following example is displayed.

```
Keystore type: JKS
 Keystore provider: SUN
 Your keystore contains 1 entry
 ovtomcatb, Dec 15, 2010, PrivateKeyEntry,
 Certificate fingerprint (MD5):
36:FC:82:FB:46:E0:54:3B:FB:D8:18:F6:53:C8:9F:4A
```

4 Export the certificate using the following command:

```
/opt/OV/nonOV/jre/b/bin/keytool -keystore tomcat.keystore -export -
alias <keystorename> -file /tmp/<server.cer>
```

where <keystorename> is the keystore name and <server.cer> is the name of the certificate file. For example:

```
/opt/OV/nonOV/jre/b/bin/keytool -keystore tomcat.keystore -export -
alias ovtomcatb -file /tmp/hpeoml910.cer
```

5 Enter the default password changeit and the certificate will be saved into the certificate file you specified under /tmp. You will receive a message such as the following:

```
Certificate stored in file </tmp/hpeoml910.cer>
```

You will import the certificate during the SmartConnector installation process.

Install the SmartConnector

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

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 Micro Focus SSO and Protect 724 sites.

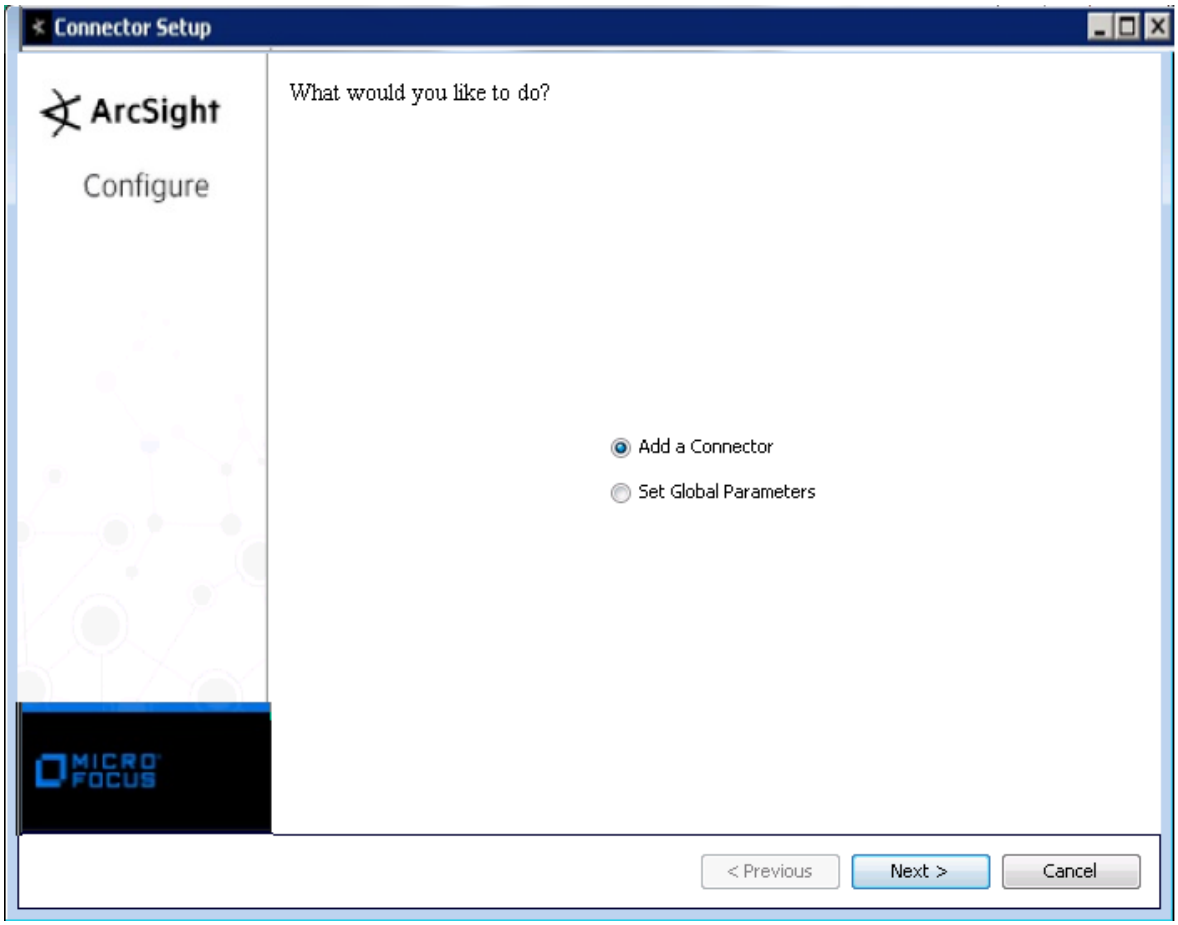
1 Download the SmartConnector executable for your operating system from the Micro Focus SSO site.

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:



The following steps are for importing the server certificate to the connector's Local Java Run Environment; this example is for Windows systems. If you are making use of Linux or Unix, change the command to reflect your $ARCSIGHT_HOME and change \ to /.

A Click **Cancel** to exit the configuration wizard.

B From `$ARCSIGHT_HOME\current\user\agent`, create an `hpeom` subdirectory; copy the certificate file you obtained during HPE OM configuration (for example, `server.cer`) and save it into this subdirectory.

C From `$ARCSIGHT_HOME\current\bin`, execute the **keytool** application to import the `server.cer` certificate. Enter this **keytool** command on a single line.

```
arcsight agent keytool -import -alias server_1_1_1_1 -file
  <\user\agent\hpeom\server.cer> -store clientcerts
```

where `<\user\agent\hpeom\server.cer>` is the path and name of the HPE OM Incident Web Service's certificate file.

D Following the prompts, answer **yes** for the prompt **Trust this certificate?**.

```
Trust this certificate? [no]: yes
```

The certificate is added to keystore.

E Verify the imported certificate by entering the following command from `$ARCSIGHT_HOME\current\bin`:

```
arcsight agent keytool -list -store clientcerts
```

The new certificate (for example, alias=server_1_1_1_1) is displayed in the list.

F From `$ARCSIGHT_HOME/current/bin`, double-click `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 Micro Focus SecureData solutions to provide encryption. See the *Micro Focus 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 Micro Focus 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 Micro Focus 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 Micro Focus SecureData.
Format Preserving Secret	Enter the secret configured for Micro Focus 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.

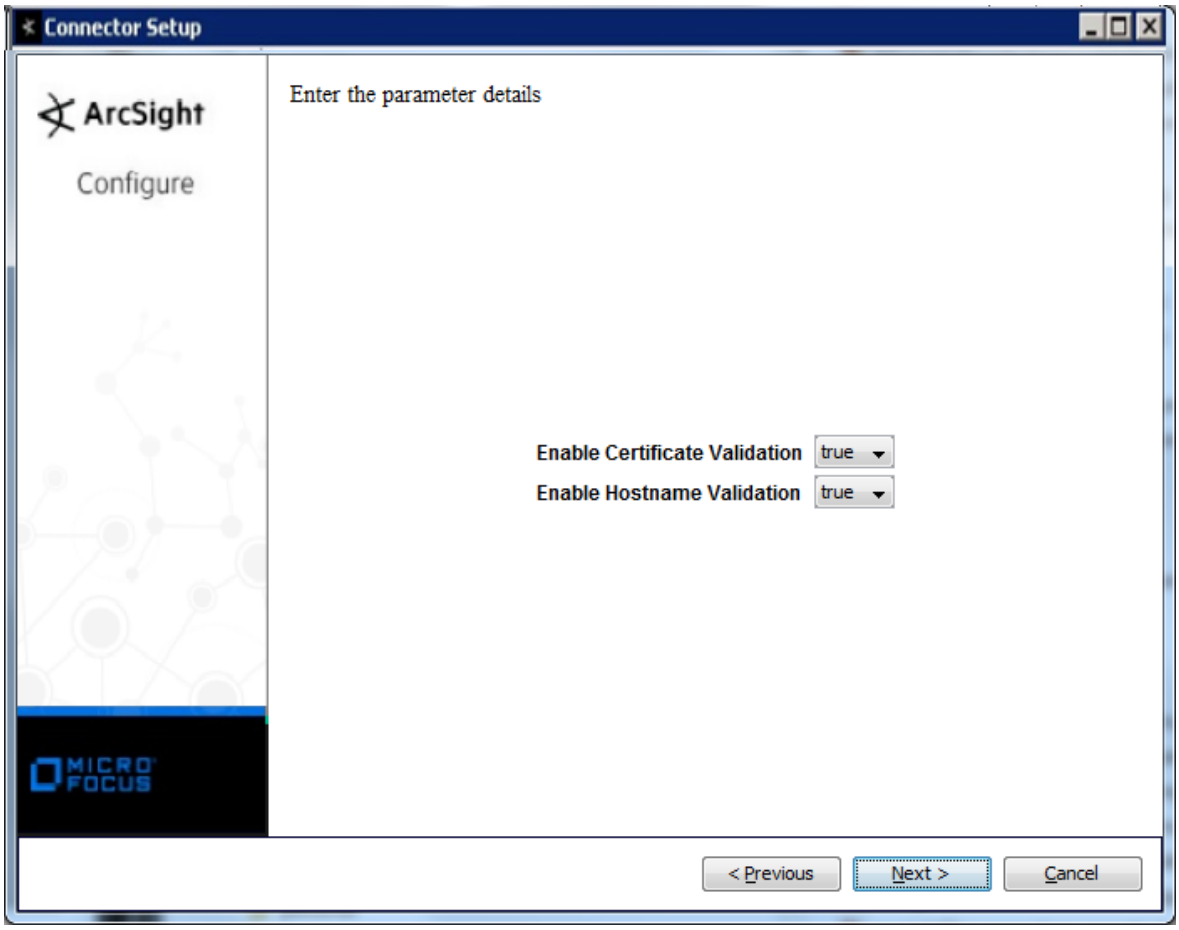
After making your selections, click **Next**. A summary screen is displayed. Review the summary of your selections and click **Next**. Click **Continue** to return to proceed with "Add a Connector" window. Continue the installation procedure with "Select Connector and Add Parameter Information."

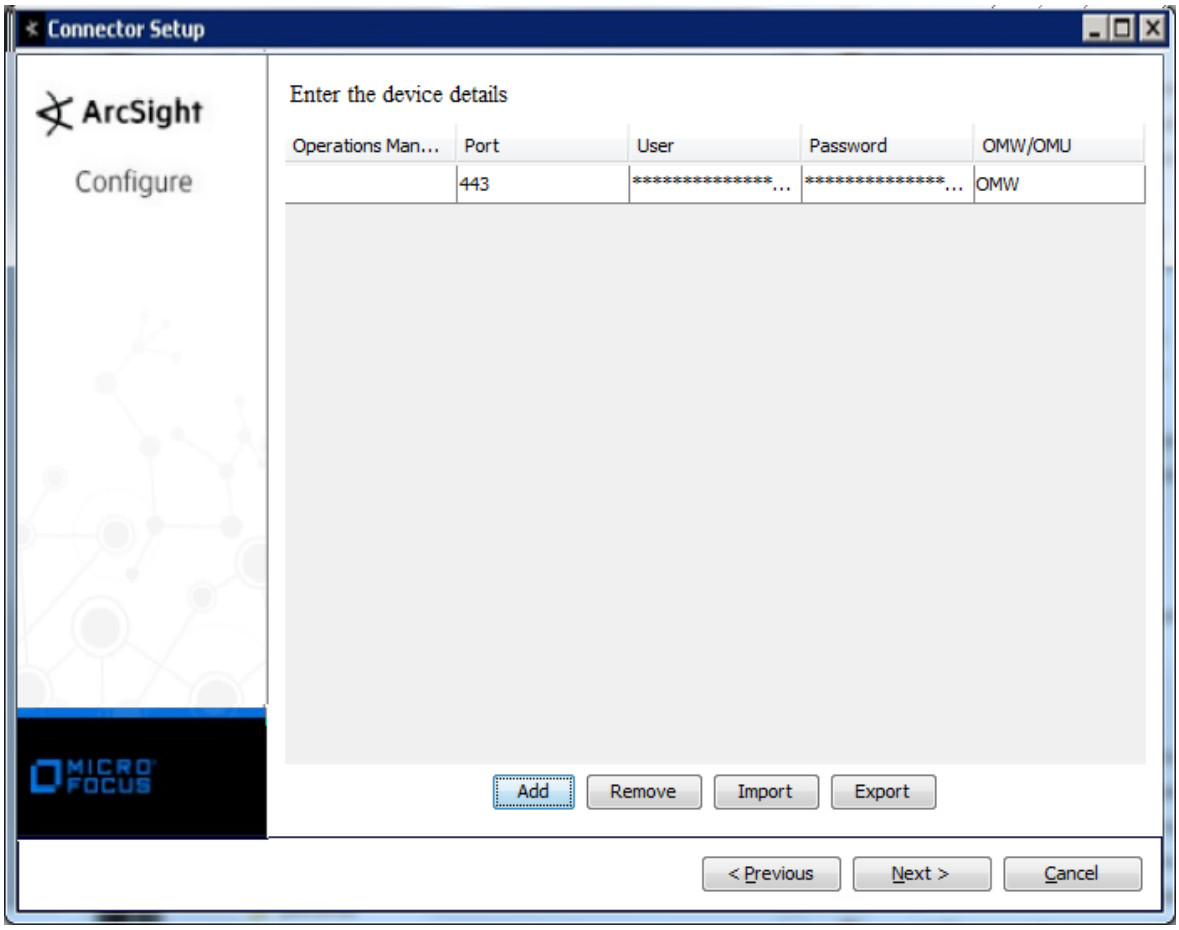
Select Connector and Add Parameter Information

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 **HPE Operations Manager Incident Web Service** and click **Next**.

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


Connector Setup
ArcSight
Configure
Enter the parameter details
Enable Certificate Validation
true
Enable Hostname Validation
true
MICRO FOCUS
< Previous
Next >
Cancel



Parameter	Description
Enable Certificate Validation	Specify whether the SmartConnector is to enable the validation of HPE Operations Manager certificate for the client. Certificate validation is enabled (true) by default.
Enable Hostname Validation	Specify whether the SmartConnector is to enable the validation of HPE Operations Manager hostname. Hostname validation is enabled (true) by default.
Operations Manager Host IP	Enter the host name or IP address of the HPE OM server.
Port	Specify the port to which the Incident Web Service is listening.
	To detect whether the Incident Web Service is listening, enter the following URL in your browser. You should receive a response from the service.
	https://<HPEOM server IP>:<HPE OM Incident Web Service Listening Port, by default 443>/opr-webservice/incident.svc. The default HTTPS port number on HPE OM on UNIX or Linux is 8444. For Windows, the default port is 443.

Parameter	Description
User	Enter the user name for the Incident Web Service user. The user name must contain the Windows domain name for certificate validation.
Password	Enter the password for the Incident Web Service user.
OMW/OMU	Select OMW for Operations Manager for Windows; select OMU for Operations Manager for Unix. Operations Manager for Linux is the currently supported Unix platform.

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.

Operations Manager Event Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Base Event Count	NumberOfDuplicates
Device Action	Solution
Device Custom Date 1	StateChangeTime (Time Owned or Time Acknowledged)
Device Custom Date 2	ReceivedTime (Time Received)
Device Custom String 1	LifeCycleState
Device Custom String 2	Source
Device Custom String 3	ConditionMatched (Unmatched)
Device Custom String 4	AutomaticActionStatus (Automatic Action Status)
Device Custom String 5	OperatorActionStatus (Operator Action Status)
Device Custom String 6	Object
Device Event Category	Category (Message Group)
Device Event Class ID	Severity
Device Product	'Operations Manager'
Device Receipt Time	CreationTime (Time Created)
Device Severity	Severity
Device Vendor	'HPE'
External ID	IncidentID (Message No.)
Message	OriginalEvent (Original Message)
Name	One of (Description, Title, 'HPE OM message')

ArcSight ESM Field	Device-Specific Field
Request Client Application	Application
Source Host Name	EmittingNode.DnsName (Node)
Type	Type (Message Type)

Limit Message Type (optional)

By default, the connector deals with all open, closed, and work in progress message types. To limit the message types collected, you can change the `uniquemessagetype` parameter setting to **open**, **closed**, or **work in progress** to limit the connector to deal with only one type of message.

To make changes to this parameter, edit it in the `agent.properties` file located after connector installation at `$ARCSIGHT_HOME\current\user\agent`, save the file, and restart the connector for the change to take effect.

Troubleshooting

I have an issue upgrading HPE OM from 9.10 to 9.10.230

A possible issue can result when you upgrade HPE OM from 9.10 to 9.10.230. In this case, the SmartConnector does not receive events from HPE OM Incident Web Service after the upgrade.

To resolve this issue:

1 Download the HPE OM 09.10.230 Accessories Patch, (OML_00064, PHSS_43292, ITOSOL_00786).

2 Backup the original file under:

```
/opt/OV/www/webapps/opc/opr-webservice/WEB-INF/lib/om-ws-server.jar
```

as

```
/opt/OV/www/webapps/opc/opr-webservice/WEB-INF/lib/om-ws-server.jar_
OML_00064>
```

3 Install the new jar file into this location:

```
>cp /tmp/om-ws-server.jar /opt/OV/www/webapps/opc/opr-webservice/WEB-
INF/lib/om-ws-server.jar
```

```
>chmod 644 /opt/OV/www/webapps/opc/opr-webservice/WEB-INF/lib/om-ws-
server.jar
```

4 Restart ovtomcatB:

```
> ovc -restart ovtomcatB
```

I have an issue when I attempt to run HPE Operations Manager Incident Web Service SmartConnector in a cluster environment.

An issue can result if you attempt to run the HPE Operations Manager Incident Web Service SmartConnector in a cluster environment. By default, the connector is not designed to work with an HPE OM cluster. If installed in a cluster, and if during a failover the active node changes to a standby node within the cluster, the connector cannot accommodate this change to the standby node and does not automatically resubscribe.

To resolve this issue, do not attempt to run HPE Operations Manager Incident Web Service SmartConnector in a cluster environment.
please confirm that when customer used MySQL JDBC driver 5.1.38, they had issue to receivee events. And the workaround is to apply older driver 5.0.8, after that connector is

able to received events.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on SmartConnector for HPE Operations Manager Incident Web Service (SmartConnectors 8.3.0)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to Documentation-Feedback@microfocus.com.

We appreciate your feedback!