
Micro Focus Security ArcSight SmartConnectors

Software Version: 8.3.0

SmartConnector for HPE Operations Manager i Web Services

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

© Copyright 2022 Micro Focus or one of its affiliates

Confidential computer software. Valid license from Micro Focus required for possession, use or copying. The information contained herein is subject to change without notice.

The only warranties for Micro Focus products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein.

No portion of this product's documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's internal use, without the express written permission of Micro Focus.

Notwithstanding anything to the contrary in your license agreement for Micro Focus ArcSight software, you may reverse engineer and modify certain open source components of the software in accordance with the license terms for those particular components. See below for the applicable terms.

U.S. Governmental Rights. For purposes of your license to Micro Focus ArcSight software, "commercial computer software" is defined at FAR 2.101. If acquired by or on behalf of a civilian agency, the U.S. Government acquires this commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of the Agreement as specified in 48 C.F.R. 12.212 (Computer Software) and 12.211 (Technical Data) of the Federal Acquisition Regulation ("FAR") and its successors. If acquired by or on behalf of any agency within the Department of Defense ("DOD"), the U.S. Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of the Agreement as specified in 48 C.F.R. 227.7202-3 of the DOD FAR Supplement ("DFARS") and its successors. This U.S. Government Rights Section 18.11 is in lieu of, and supersedes, any other FAR, DFARS, or other clause or provision that addresses government rights in computer software or technical data.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

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 i Web Services	5
Product Overview	6
Configure BSM OMi for SmartConnector Event Collection	7
Obtain the Authentication Certificate	7
Install the SmartConnector	13
Prepare to Install Connector	13
Install Core Software	14
Set Global Parameters (optional)	16
Select Connector and Add Parameter Information	17
Select a Destination	19
Complete Installation and Configuration	19
Additional Configuration	20
Read Older Events from HPE OMi	20
Filter the Event Types to Import from OMi	20
Access Advanced Parameters	20
Run the SmartConnector	21
Device Event Mapping to ArcSight Fields	22
Operations Manager i Web Services Mappings	22
Send Documentation Feedback	24

SmartConnector for HPE Operations Manager i Web Services

This guide provides information for installing the SmartConnector for HPE Operations Manager i Web Services and configuring the device for event collection. 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

BSM Operations Management is the event management foundation for a complete BSM monitoring solution. As the operations bridge, it consolidates all IT infrastructure monitoring in a central event console, and relates the events to the IT services that depend on that infrastructure.

BSM Operations Management links infrastructure management with application and business service management. It combines events from HPE Business Service Management components, such as Business Process Monitor (BPM), Real User Monitor (RUM), and Service Level Management (SLM), with events from the operations management components of the BSM solution, such as HPE Operations Manager (HPEOM) and HPE Network Node Manager *ii* (NNMi), letting you keep track of all the events that occur in your monitored environment.

The messages generated by BSM OMi are retrieved through HPE's OMi Web Services and forwarded into the ArcSight System.

Configure BSM OMi for SmartConnector Event Collection

The SmartConnector can validate OMi's authentication certificate. To operate in this configuration, first get the certificate from Operations Manager i, 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 i 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 BSM OMi Web Services using HTTPS connections, which require a suitable certificate on the server. Although the Web Services can listen to both HTTP and HTTPS at the same time, the SmartConnector always attempts to connect through HTTPS. Both BSM OMi Web Services and its certificate are components generally installed on the BSM OMi server by default. The port that the service uses by default for HTTPS communication is 443. The default port for HTTP communication is 80.

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.

The examples in the following procedure use Mozilla Firefox.

To export the OMi Web Services certificate:

- 1 Enter the BSM server IP address in your browser.



This Connection is Untrusted

You have asked Firefox to connect securely to **10.0.103.163**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Get me out of here!

- ▶ Technical Details
- ▶ I Understand the Risks

2 Click I Understand the Risks.



This Connection is Untrusted

You have asked Firefox to connect securely to **10.0.103.163**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Get me out of here!

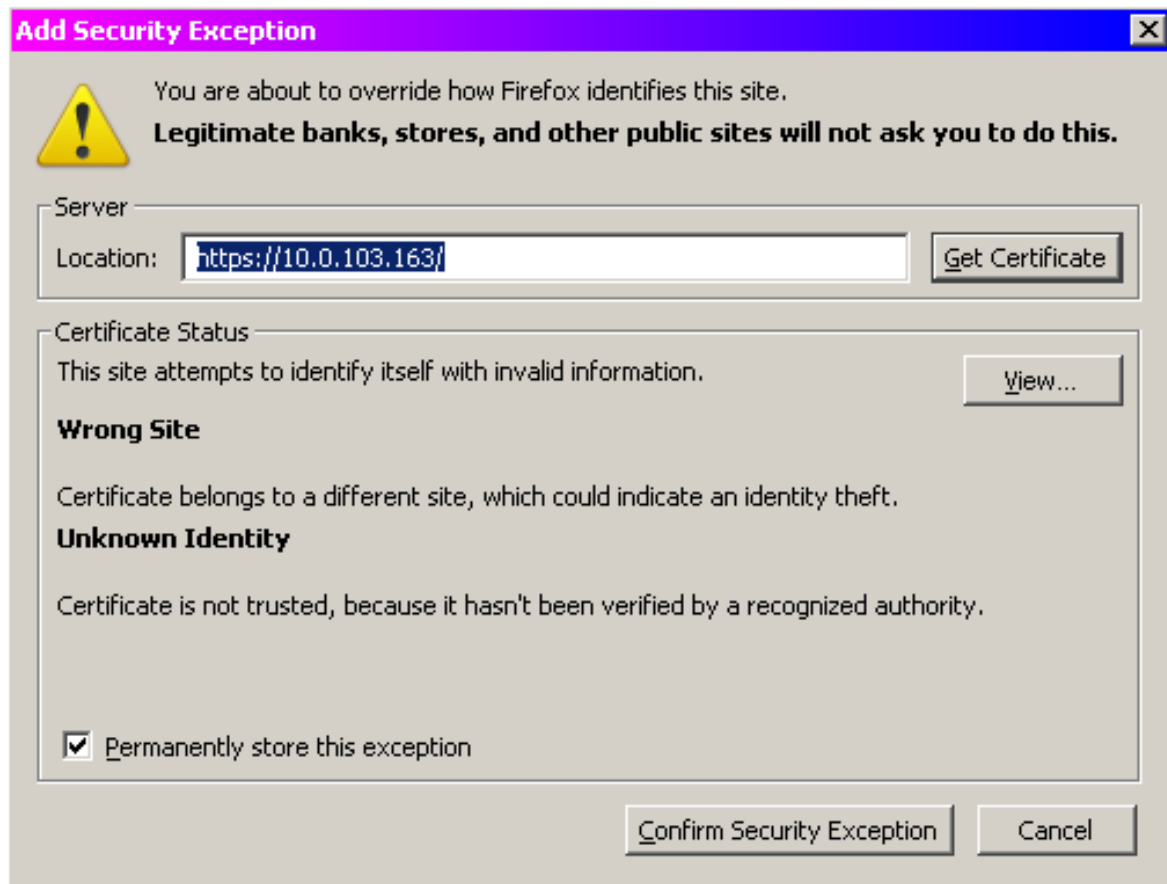
- ▶ Technical Details
- ▼ I Understand the Risks

If you understand what's going on, you can tell Firefox to start trusting this site's identification. **Even if you trust the site, this error could mean that someone is tampering with your connection.**

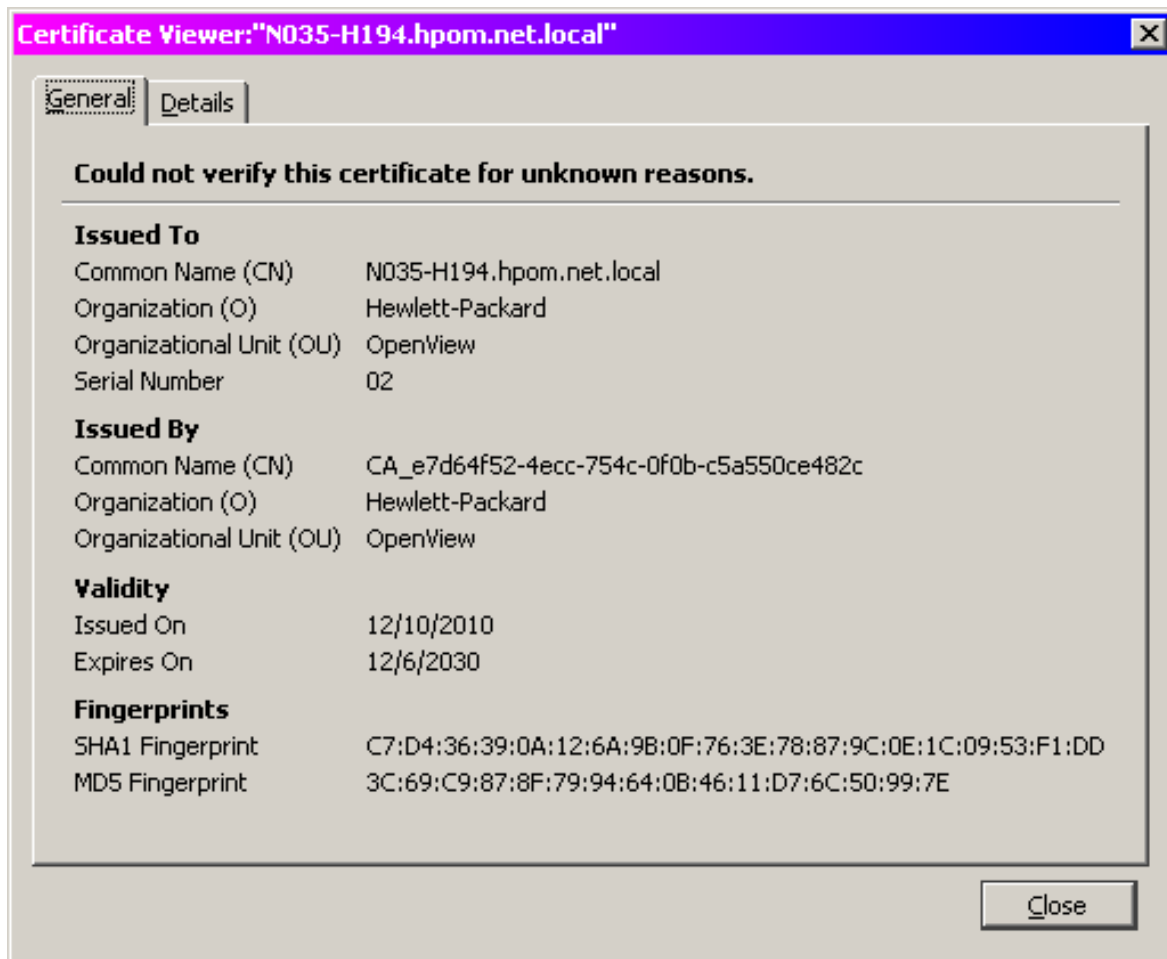
Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.

Add Exception...

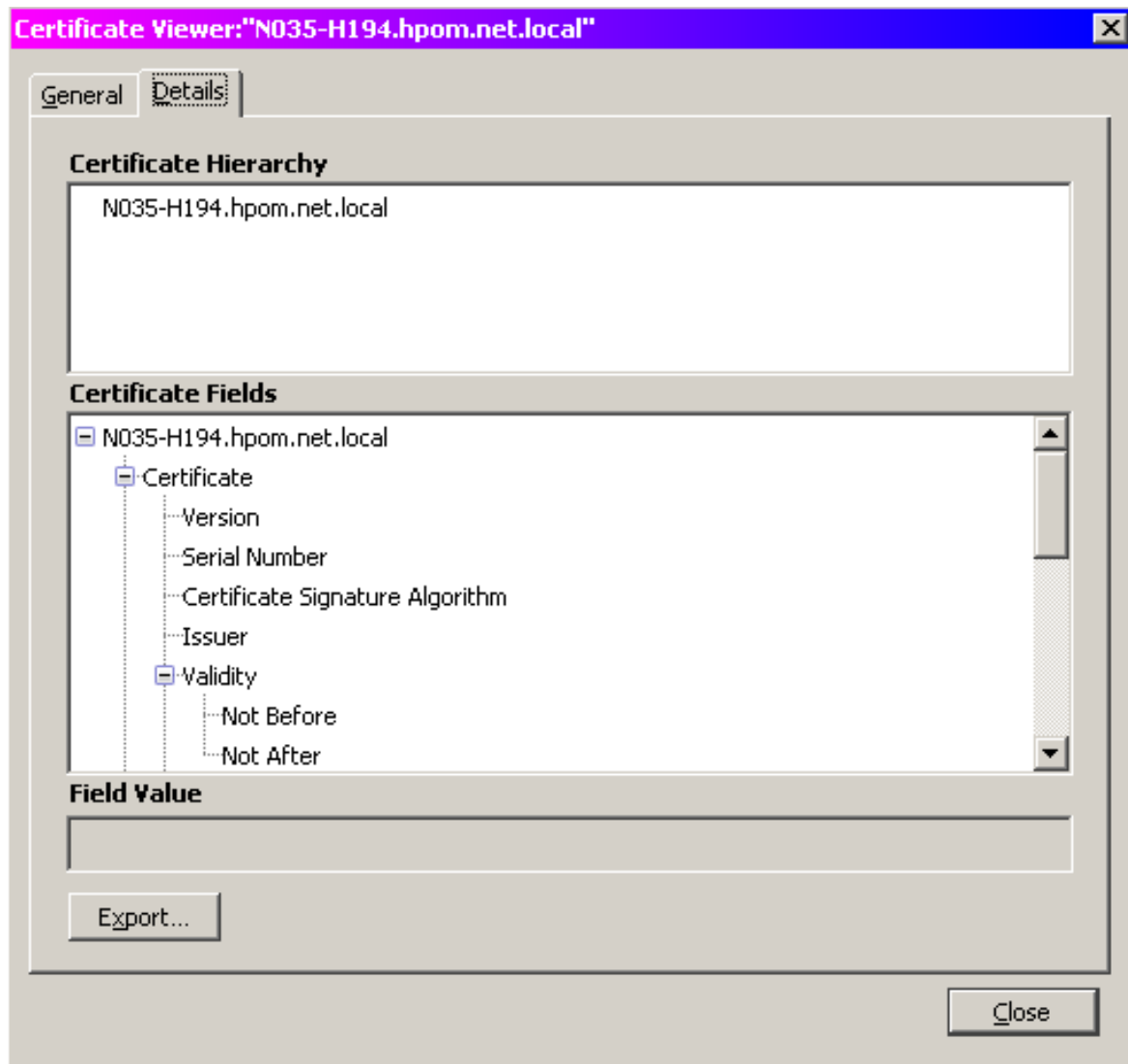
3 Click Add Exception....



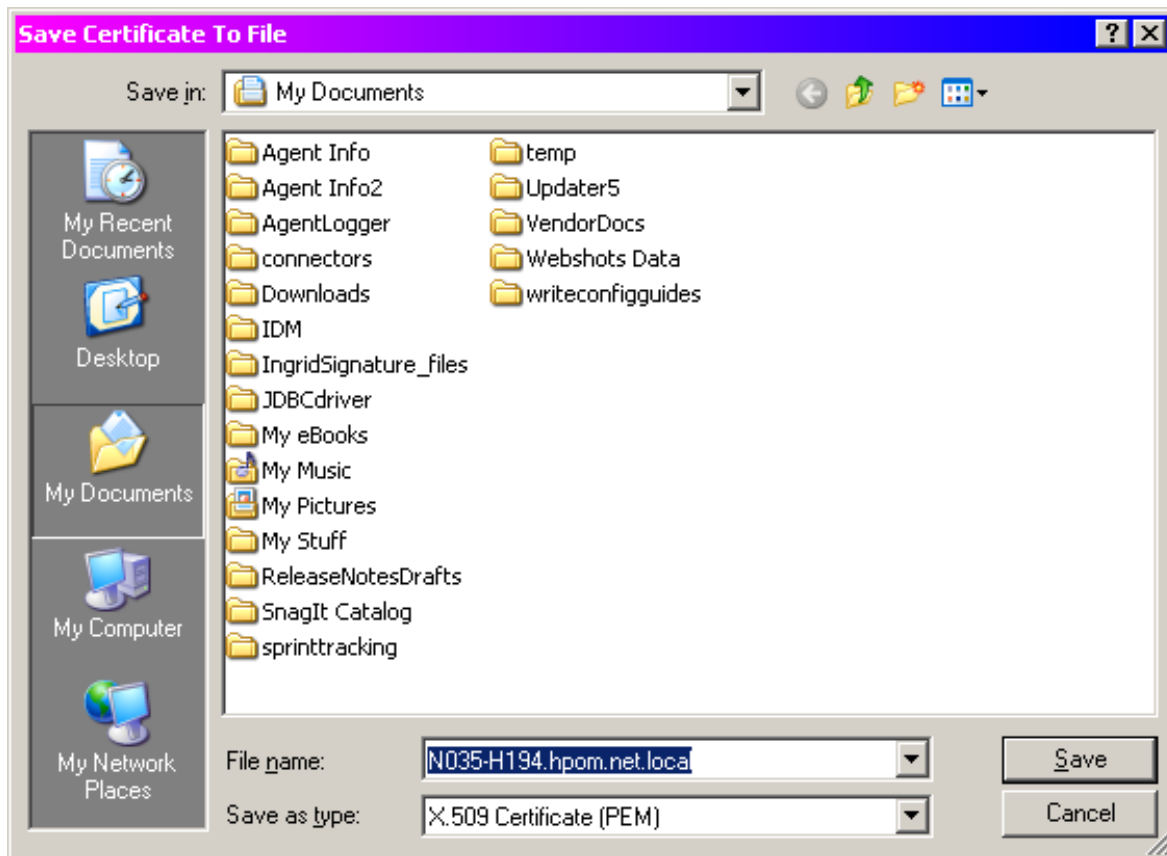
4 Click **View...**



5 Click the **Details** tab.



6 Click **Export....**



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

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

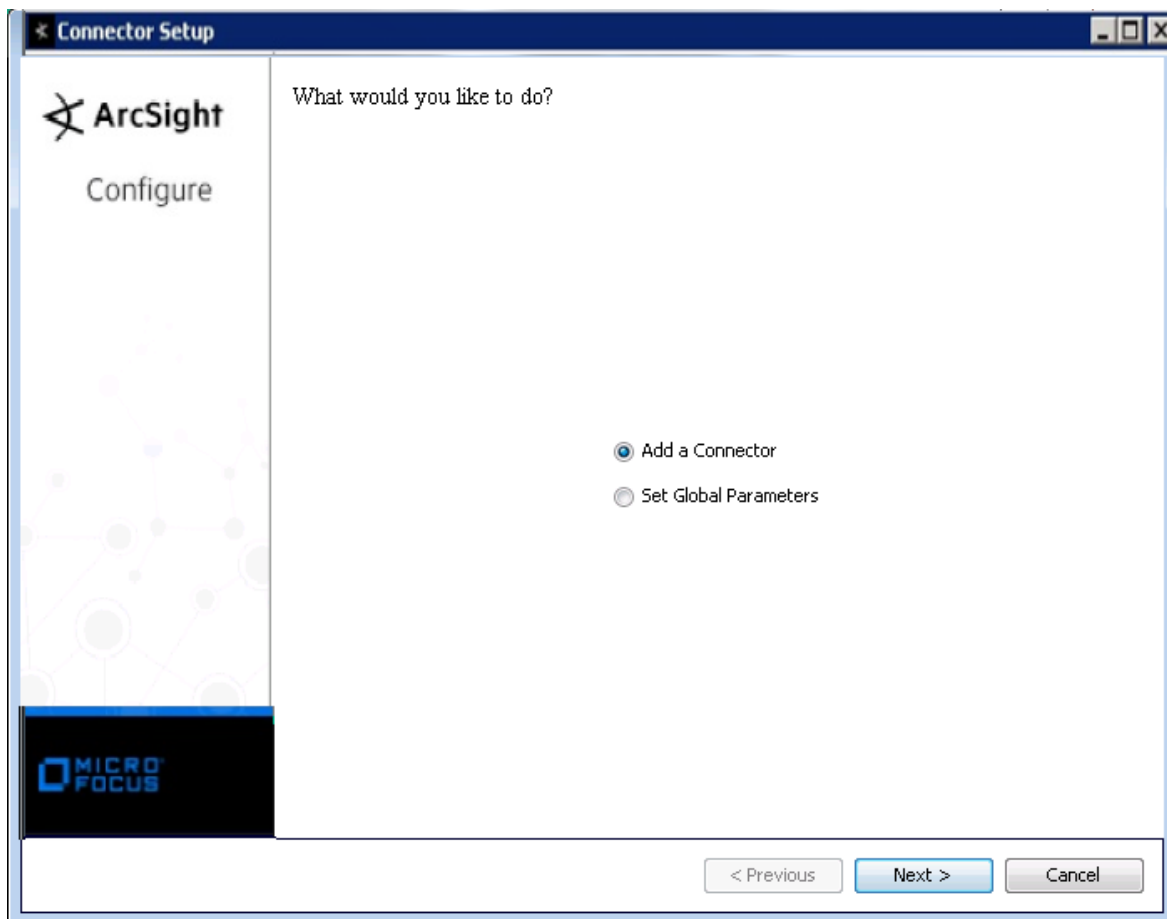
Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms; for the complete list, see the *SmartConnector Product and Platform Support* document, available from the Micro Focus SSO and Protect 724 sites.

- 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 hpeomi subdirectory; copy the certificate file you obtained during HPE OMi 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\hpeomi\server.cer> -store clientcerts
```

where <\user\agent\hpeom\server.cer> is the path and name of the HPE OMi Web Services' 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.

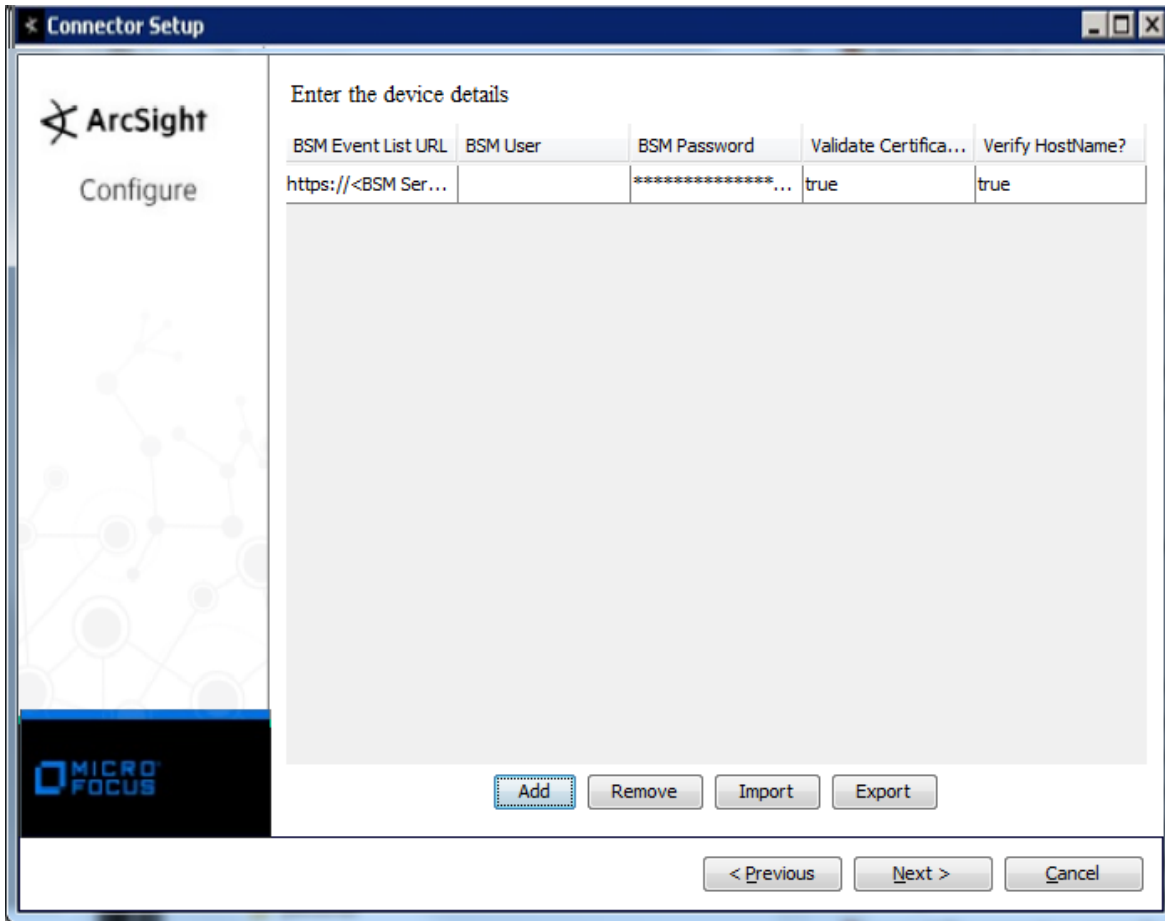
The following parameters should be configured only if you are using Micro Focus SecureData solutions to provide encryption. See the *Micro Focus SecureData Architecture Guide* for more information.

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 i Web Services** and click **Next**.
- 3 Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



Parameter	Description
BSM Event List URL	Specify the port to which OMi Web Services is listening. To detect whether Web Services is listening, enter the following URL in your browser. You should receive a response from the service. https://<BSM Server>/opr-console/rest/event_list
BSM User	Enter the user name for the BSM user.
BSM Password	Enter the password for the BSM user.
Validate Certificate	Specify whether the SmartConnector is to enable the validation of the BSM OMi SSL certificate for the client. Certificate validation is enabled (true) by default.
Verify HostName	Specify whether the SmartConnector is to enable the validation of the BSM OMi hostname. Hostname validation is enabled (true) by default.

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*.

Additional Configuration

Read Older Events from HPE OMi

By default, the connector reads only live events starting from the time the connector is up. You can set the advanced parameter `watermark` to an older date and time in the format `<yyyy-MM-ddTHH:mm:ssZ>` (for example, `2010-12-23T00:00:00-08:00`) before starting the connector. This tells the connector to read events from a specific time in history. *Make sure to unset this parameter after reading the older events.* Otherwise, the connector will read older events every time it is intentionally or unintentionally restarted. See "Access Advanced Parameters" for how to change these parameters.

Filter the Event Types to Import from OMi

By default, the connector reads all types of events from OMi, including those that have been closed by the operator, and does not perform any filtering. You can, however, choose not to import closed events by setting the advanced parameter `include_closed` to `false`. You can also limit the types of events imported by configuring a value for the advanced parameter `query`. The value for the query should follow the Event Web Service Query Language described in the *BSM OMi Extensibility Guide*. See "Access Advanced Parameters" for how to change these parameters.

Access Advanced Parameters

After SmartConnector installation, you can change parameter values by editing the `agent.properties` file located at `$ARCSIGHT_HOME\current\user\agent`. Change values, save the file, and restart the connector for your changes to take effect.

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 i Web Services Mappings

ArcSight ESM Field	Device-Specific Field
Additional data	community
Additional data	component
Additional data	enterprise
Additional data	exit_code
Additional data	original_event
Additional data	policy_id
Additional data	specific_trap_type
Additional data	trap_type
Additional data	variables
Additional data	eventNumber
Additional data	parameterId
Additional data	Self-Monitoring
Agent (Connector) Severity	Very High = critical; High = major; Medium = warning, minor; Low = normal
Aggregated Event Count	duplicate_count
Destination Address	node_hints_node_ip_address
Destination Host Name	node_hints_node_dns_name
Device Custom Date 1	time_state_changed
Device Custom Date 2	Date Expired
Device Custom Number 1	sequence_number
Device Custom String 1	match_info_policy_name

ArcSight ESM Field	Device-Specific Field
Device Custom String 2	state
Device Custom String 3	application
Device Custom String 4	source_ci_hints_node_dns_name
Device Custom String 5	originating_server_dns_name
Device Custom String 6	sending_server_dns_name
Device Event Category	match_info_policy_type
Device Event Class ID	eti_hint
Device Host Name	drilldown_url
Device Product	'Operations Manager i'
Device Receipt Time	time_received
Device Severity	severity (critical, major, warning, minor, normal)
Device Vendor	'HPE'
End Time	time_changed
External ID	id
Message	title
Request URL	drilldown_url
Source User ID	assigned_user_login_name
Source User Name	assigned_user_user_name
Source User Privileges	assigned_group_name
Start Time	time_created

please confirm that when customer used MySQL JDBC driver 5.1.38, they had issue to receive events. And the workaround is to apply older driver 5.0.8, after that connector is able to receive 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 i Web Services
(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!