

Configuration Guide

ArcSight Forwarding Connector
5.2.7.6582.0

March 5, 2013



Copyright © 2013 Hewlett-Packard Development Company, L.P.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP 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. HP shall not be liable for technical or editorial errors or omissions contained herein.

Follow this link to see a complete statement of copyrights and acknowledgements:

<http://www.hpenterprisesecurity.com/copyright>

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

This document is confidential.

Contact Information

Phone	A list of phone numbers is available on the HP ArcSight Technical Support page: http://www8.hp.com/us/en/software-solutions/software.html?compURI=1345981#.URitMaVwpWl .
Support Web Site	http://support.openview.hp.com
Protect 724 Community	https://protect724.arcsight.com

Revision History

Date	Product Version	Description
03/05/2013	5.2.7.6582.0	Added full 64-bit JVM package support including wrapper libraries and fixed Known Issue CON-12005.
09/25/2012	5.2.5.6403.0	Added new installation wizard.
02/15/2012	5.1.7.6154.0 (32-bit)	Added support for 64-bit JVM.
	5.1.7.6151.0 (64-bit)	
11/15/2011	5.1.7.6085.0	SNMP Interceptor policies for HP OM and HP OMi are decoupled from the connector.
09/27/2011	5.1.5.5973.0	Added support for McAfee ePO 4.6.
08/15/2011	5.1.5.5973.0	Added support for JRE 1.6.0_26.
06/20/2011	5.1.4.5941.0	Added support for HP OMi.
05/19/2011		Restructured guide to include multiple chapters, added instructions for using multiple destinations and added a chapter on HP OM configuration.

Contents

Chapter 1: Overview and Installation	5
Product Overview	5
The ArcSight ESM Source Manager	5
Sending Events to an ArcSight ESM Destination Manager	6
Sending Events to ArcSight Logger	6
Sending Events to a Non-ESM Location	6
Standard Installation Procedures	7
Verifying that ESM is Correctly Installed	7
Assigning Privileges on the ESM Source Manager	7
Forwarding Correlation Events	9
Increasing the FileStore size (Enhanced version only)	10
Installing the Forwarding Connector	11
Uninstalling a Forwarding Connector	12
Upgrading a Forwarding Connector	12
Chapter 2: Configuration for Forwarding Events	13
Forwarding Events to an ArcSight Manager	13
Forwarding Events to ArcSight Logger	18
Forwarding Events to NSP Device Poll Listener	20
Forwarding CEF Syslog Events	21
Forwarding Events to a CSV File	23
Forwarding Events to McAfee ePolicy Orchestrator	24
Installing the Microsoft JDBC Driver for SQL Server	26
ArcSight Event to McAfee CEF Mappings	27
Configuring Multiple Destinations	28
Chapter 3: Configuration for HP OM and HP OMi	31
The ArcSight ESM Source Manager	32
Supported Versions of HP OM and HP OMi	32
HP OM and HP OMi and Correlation Events	32
Installing the Connector	32
Creating an SNMP Interceptor Policy for HP Operations Manager (HP OM)	35
Uploading Interceptor Template	35

Deploying the Policy	35
Creating an SNMP Interceptor Policy for HP Operations Manager i (HP OMi)	35
Uploading Interceptor Template	36
Troubleshooting Tips	36
Duplicate Events (for HP OMi)	36
Dropped Events	36
Adjusting the Event Processing Rate for HP OM and HP OMi	36
Appendix A: Using the Forwarding Connector with FIPS	39
What is FIPS?	39
ArcSight ESM Installation	39
FIPS-Enabled Forwarding Connector Installation	40
Manually Importing the Certificate	40
Enabling FIPS Suite B Mode	41
Using Logger in FIPS Mode	45

Chapter 1

Overview and Installation

This chapter provides information for installing an ArcSight Forwarding Connector for event collection from an ArcSight Manager installation. The following topics are discussed.

[“Product Overview” on page 5](#)

[“The ArcSight ESM Source Manager” on page 5](#)

[“Standard Installation Procedures” on page 7](#)

[“Uninstalling a Forwarding Connector” on page 12](#)

[“Upgrading a Forwarding Connector” on page 12](#)

The ArcSight Forwarding Connector is supported on Red Hat Enterprise 6.2 platform.

ArcSight recommends using the Forwarding Connector installer included with the corresponding ESM or HP integration release. The Forwarding Connector is released as part of the ESM release, however its build version might not match that of other ESM components within the release.



Note

The ESM or ArcSight Express version with which this Forwarding Connector is released may not support all Forwarding Connector features. Refer to the ESM or ArcSight Express release notes for details about what Forwarding Connector features the accompanying version of ESM or ArcSight Express supports.

Product Overview

The ArcSight Forwarding Connector lets you receive events from a source Manager installation and send them to a secondary destination Manager, a non-ESM location or to an ArcSight Logger.

The ArcSight ESM Source Manager

The ESM Source Manager is the installation from which events originate on a network using the ArcSight Forwarding Connector. The Forwarding Connector sends on (or “forwards”) events to a destination Manager, a non-ESM location or a Logger appliance.

With data originating from an ArcSight ESM Source Manager, the ArcSight Forwarding Connector provides these destination options for forwarding events:

- An ArcSight ESM destination Manager

- ArcSight Logger
- NSP Device Poll Listener
- CEF Syslog
- A CSV file
- McAfee ePolicy Orchestrator v4.0, v4.5, or v4.6
- HP Operations Manager
- HP Operations Manager i

Sending Events to an ArcSight ESM Destination Manager

The ArcSight Forwarding Connector logs into the source Manager and then forwards events to a destination Manager. For configuration instructions, see [“Forwarding Events to an ArcSight Manager” on page 13](#).

Sending Events to ArcSight Logger

ArcSight Logger is a hardware storage solution optimized for high event throughput. A typical use for Logger is to collect firewall data and then forward a subset of that data to an ArcSight Manager for realtime monitoring and correlation. Logger now supports the Federal Information Processing Standard 140-2 (FIPS 140-2). See [“Using Logger in FIPS Mode” on page 45](#) for details.

SmartMessage is an ArcSight technology that provides a secure channel between ArcSight SmartConnectors and Logger. SmartMessage provides an end-to-end encrypted secure channel. One end is an ArcSight SmartConnector that receives events from the many devices supported by ArcSight SmartConnectors, and the other is a SmartMessage Receiver housed on the Logger appliance.

Before configuring the Forwarding Connector that sends events to the Receiver, you must create a Receiver of type **SmartMessage**. After you create this Receiver, you can configure the SmartConnector to send events to Logger.

For information on configuring a Forwarding Connector to forward events to Logger, see [“Forwarding Events to ArcSight Logger” on page 18](#).

Refer to the ArcSight Logger Administrator's Guide for complete instructions about:

- Receivers
- Configuring a SmartConnector to Send Events to Logger
- Configuring SmartConnectors to Send Events to Both Logger and a Manager
- Sending Events from ArcSight ESM to Logger
- Using Logger in FIPS mode

Sending Events to a Non-ESM Location

The ArcSight Forwarding Connector logs into the source Manager and then forwards events to a non-ESM location.

For configuration instructions on forwarding events to NSP, see [“Forwarding Events to NSP Device Poll Listener” on page 20](#).

For configuration instructions on forwarding CEF Syslog events, see [“Forwarding CEF Syslog Events” on page 21](#).

For configuration instructions on forwarding events to a .csv file, see [“Forwarding Events to a CSV File” on page 23](#).

For configuration instructions on forwarding events to McAfee ePolicy Orchestrator (ePO), see [“Forwarding Events to McAfee ePolicy Orchestrator” on page 24](#).



Use of ePO requires installation of **MS SQL Server 2005 for JDBC driver**. For downloading instructions, see [“Installing the Microsoft JDBC Driver for SQL Server” on page 26](#).

For detailed configuration instructions on forwarding events to HP Operations Manager (HP OM) and HP Operations Manager i (HP OMi), see [Chapter 3, Configuration for HP OM and HP OMi, on page 31](#).

Standard Installation Procedures

This section describes the standard installation procedures for the ArcSight Forwarding Connector.

Verifying that ESM is Correctly Installed

Before you install the ArcSight Forwarding Connector, make sure that ArcSight Manager and Console has already been installed correctly. Review the ArcSight Installation and Configuration Guide before attempting a new ArcSight Forwarding Connector installation.

To ensure a successful ESM installation:

- 1 Make sure that the Manager, Database, and Console are installed and functioning.
- 2 Run the ArcSight Manager; the Manager command prompt window or terminal box displays a **Ready** message when the Manager has started successfully. You can also monitor the `server.std.log` file located in `ARCSIGHT_HOME\logs\default`.
- 3 Run the ArcSight Console. Although not necessary, it is helpful to have the ArcSight Console running when installing the SmartConnector to verify successful installation.

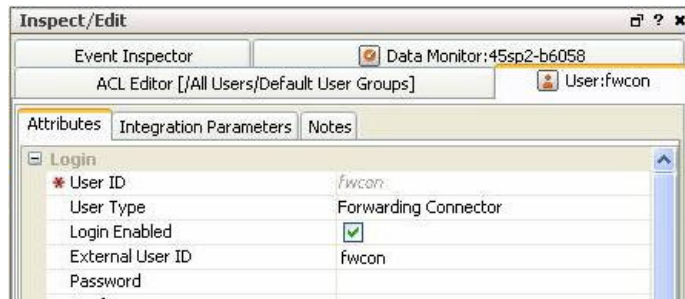
Assigning Privileges on the ESM Source Manager

Before installing the ArcSight Forwarding Connector, you need to create a **Forwarding Connector** account on the source Manager. You can then assign filters for incoming events.

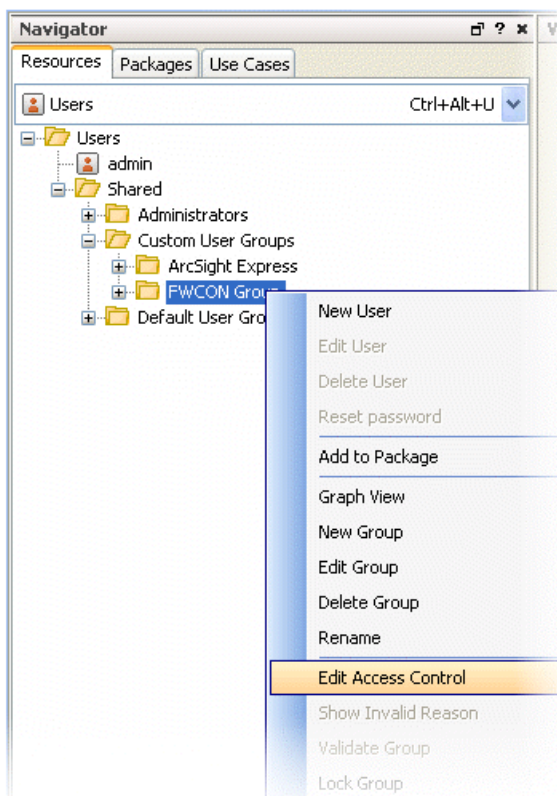
To assign privileges in the Manager:

- 1 Run the ArcSight Console and log in to the ArcSight Manager.
- 2 From the Navigator **Resources** tab, choose **Users**.
- 3 Create a user group under the **Custom User Group**.

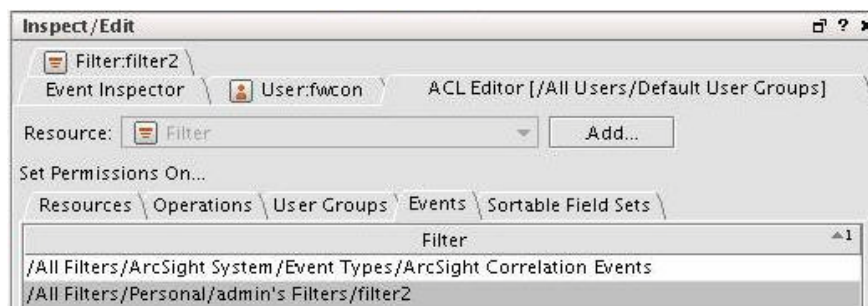
- 4 Under the group created in **step 3**, create a user account of user type **Forwarding Connector**, as shown below.



- 5 Return to the Navigator **Resources** tab and right-click your chosen user group.
- 6 From the menu, choose **Edit Access Control**.



- 7 From the **Inspect/Edit** window, click the **Events** tab under the new user type and assign the filters.



For detailed instructions on creating filters and users using ArcSight Console, refer to the ArcSight Console User's Guide.

Forwarding Correlation Events

The ArcSight Forwarding Connector can forward events based upon the ACL assigned to the User Group on the source Manager. The connector can be configured to allow forwarding of ArcSight correlation events from the source Manager to the target (or destination) Manager. The ACL can also be configured to allow for viewing of the detailed chain of the forwarded correlation event, including the original correlated event.



HP OM users commonly require only correlated events to be retrieved from ESM. In such cases, HP OM users can specify the selection of correlated events. To allow for only correlated events and restrict the retrieval of base events, configure ESM to **retrieve correlated events**, then **allow the forwarding of correlation events**, as described below. These steps should be performed in sequence, then restart the source Manager.

Perform the following steps to retrieve correlated events.

Configuring to Retrieve Correlated Events

To configure the source Manager to send both correlation events and on-demand correlated events to the destination Manager, the ACL must contain two separate filters:

- 1 Note Filter 1, which is provided with the latest version of ArcSight ESM:
`/All Filters/ArcSight System/Event Types/ArcSight Correlation Events`
- 2 Create Filter 2, using the condition, `Event Annotation Flags ContainsBits correlated`.
- 3 Both filters need to be applied to the Event Permissions of the User Group ACL to be able to extract correlated events from the correlation events that are forwarded to the target Manager.



Correlated events retrieved on-demand are for viewing only. They do not persist in the destination Manager.

- 4 Restart the manager.

Configuring to Allow Forwarding of Correlated Events

The Forwarding Connector can also be configured to automatically forward correlated events irrespective of the User Group ACL. Only one Forwarding Connector per Manager can be configured to work in this mode. This configuration can aid in hierarchical deployment scenarios in which you need to automatically forward correlated events for further correlation and reporting on the destination Manager.

The source Manager keeps track of the events that have been previously forwarded by using the "Forwarded" annotation, disallowing duplicates.

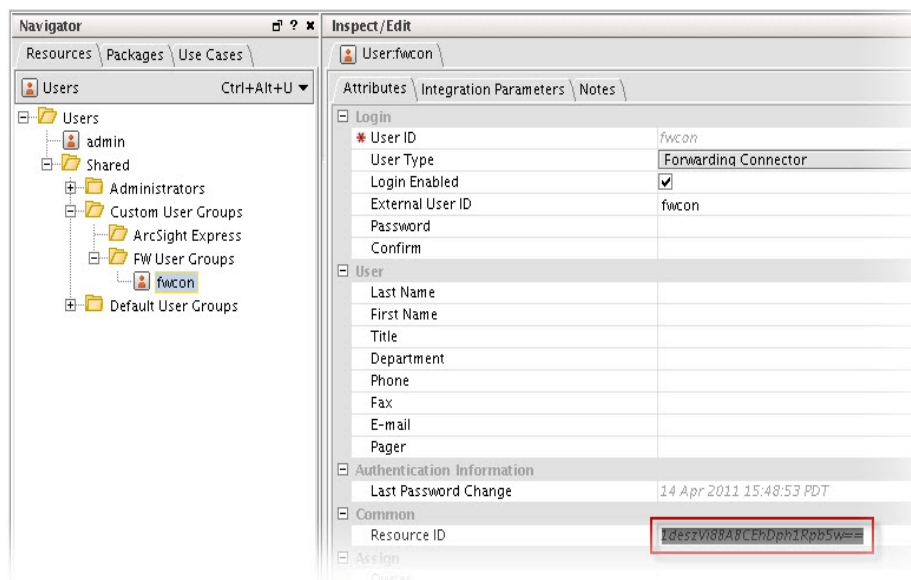
To configure the source Manager to send both correlation events and correlated events automatically, you must specify the **container ID**. The container ID consists of two elements, the **entityid** and the **userid**. To begin the configuration, you must locate these two elements and combine them in the `server.properties` file.

- 1 To find the **entityID**, go to `$AGENT_HOME/user/agent/agent.properties` and search for `agents[0].entityid`. Copy the text string starting in `3w` to a text editing program, such as Notepad.

```
agents[0].entityid=3w+05uiYBABCCLKvzx0stdQ\==
```

- 2 To find the **userid**, go to the Console of the **source Manager**.

- a From the **Navigator** panel, choose the **Resources** tab.
- b Choose **Users** to find your Forwarding Connector user.
- c Locate the **Resource ID** and copy the text string from the second column, as shown below.



In the `$Arcsight_HOME/config/server.properties` file on the source Manager, add the **entityid** and **userid** to the `eventstream.cfc` property, as shown below.

```
eventstream.cfc=EntityID.UserID
```

- 3 Restart the source Manager and, if still running, the Forwarding Connector.

Increasing the FileStore size (Enhanced version only)

Installation of the ArcSight Forwarding Connector (Enhanced) option provides fault-tolerance, enabling events to be saved in the event of a failure.

The capacity of events that can be stored during a system failure is dependent on the amount of disk space the FileStore can use on the source Manager. Although the default size of 1024 MB (1 GB) is suitable for most installations, you can increase the size of your FileStore.

To increase the size of the FileStore:

- 1 Open the `server.defaults.properties` file, located under `$ARCSIGHT_HOME\config`.

The file displays the default file size:

```
filestore.disksize.max.megabytes.int=1024
```

- 2 Use this formula to determine appropriate rates for minutes of storage on your system:

$$\text{MinutesOfStorage} = ((\#MB / 1024) * 21,474,833) / \text{EPS} / 60$$

- ◆ Given the most typical event sizes, a FileStore of 1 GB can store approximately 21,474,833 events, and at a rate of 5000 events per second, the default size provides approximately 71 minutes of storage.
- ◆ When the FileStore fills up, the oldest events are purged to make room for recent ones.

Installing the Forwarding Connector

Before installing the Forwarding Connector, you need to assign privileges on your Manager. For instructions on how to do this, see ["Assigning Privileges on the ESM Source Manager" on page 7](#).



Note

For information regarding operating systems and platforms supported, refer to SmartConnector Product and Platform Support, available from ArcSight Technical Support with each SmartConnector release.

To install the Forwarding Connector:

- 1 Download the install executable for your operating system. See the release notes for download information.
- 2 Start the installer by running the executable for your operating system, then follow the folder selection tasks and installation of the core SmartConnector software:

- ◆ Introduction
- ◆ Choose Install Folder
- ◆ Choose Install Set
- ◆ Choose Shortcut Folder
- ◆ Pre-Installation Summary
- ◆ Installing...

When installation of the connector core component is complete, navigate through the installer and choose from the following ArcSight Forwarding Connector destinations.

- ◆ To forward events to an ArcSight ESM Manager, proceed with ["Forwarding Events to an ArcSight Manager" on page 13](#).
- ◆ To forward events to an ArcSight Logger, proceed with ["Forwarding Events to ArcSight Logger" on page 18](#).
- ◆ To forward events to an NSP appliance, proceed with ["Forwarding Events to NSP Device Poll Listener" on page 20](#).
- ◆ To forward events to a CEF Syslog, proceed with ["Forwarding CEF Syslog Events" on page 21](#).

- ◆ To forward events to McAfee ePolicy Orchestrator (ePO), proceed with [“Forwarding Events to McAfee ePolicy Orchestrator”](#) on page 24.

**Caution**

Use of ePO requires installation of **MS SQL Server 2005 for JDBC driver**. For instructions on downloading, see [“Installing the Microsoft JDBC Driver for SQL Server”](#) on page 26.

- ◆ To forward events to a .csv file, proceed with [“Forwarding Events to a CSV File”](#) on page 23.
- ◆ For configuration instructions about forwarding events to HP Operations Manager or HP Operations Manager i, see [Chapter 3, Configuration for HP OM and HP OMi](#), on page 31.
- ◆ To install the Forwarding Connector in FIPS-compliant mode, proceed with [“FIPS-Enabled Forwarding Connector Installation”](#) on page 40.

Uninstalling a Forwarding Connector

Before uninstalling a Forwarding Connector that is running as a service or daemon, first stop the service or daemon.

To uninstall on UNIX hosts, open a command window on the \$ARCSIGHT_HOME/UninstallerData directory and run the command:

```
./Uninstall_ArcSightAgents
```

**Note**

The UninstallerData directory contains the file .com.zerog.registry.xml with Read, Write, and Execute permissions for all users. On Windows platforms, these permissions are required for the uninstaller to work. However, on UNIX platforms, you can change the permissions to Read and Write for everyone (that is, 666).

The Uninstaller does not remove all the files and directories under the ArcSight SmartConnector home folder. After completing the uninstall procedure, delete these folders manually.

Upgrading a Forwarding Connector

**Note**

Be sure to check the ESM release notes for supported Forwarding Connector upgrade paths.

To locally upgrade the Forwarding Connector:

- 1 Stop the running connector.
- 2 Run the installer for the ArcSight Forwarding Connector, which prompts you for an installation location.
- 3 Select the location of the Forwarding Connector you want to upgrade; you will receive the message “Previous Version Found - Upgrade Possible”. Select the option to continue and upgrade the connector.

The original installation is renamed by prefacing characters to the original folder name; the upgraded connector is installed in the location \$ARCSIGHT_HOME\current

Configuration for Forwarding Events

This chapter provides step-by-step instructions for configuring various Forwarding Connector destinations and contains these topics:

- ["Forwarding Events to an ArcSight Manager" on page 13](#)
- ["Forwarding Events to ArcSight Logger" on page 18](#)
- ["Forwarding Events to NSP Device Poll Listener" on page 20](#)
- ["Forwarding CEF Syslog Events" on page 21](#)
- ["Forwarding Events to a CSV File" on page 23](#)
- ["Forwarding Events to McAfee ePolicy Orchestrator" on page 24](#)
- ["Configuring Multiple Destinations" on page 28](#)

**Note**

Event fields that refer to local resources in the manager are not forwarded to the next manager. Instead those fields are repopulated based upon the local resources present on the next manager. For example, the **Target Asset** field is recalculated and can have a different value based upon what resources exist on each manager.

Forwarding Events to an ArcSight Manager

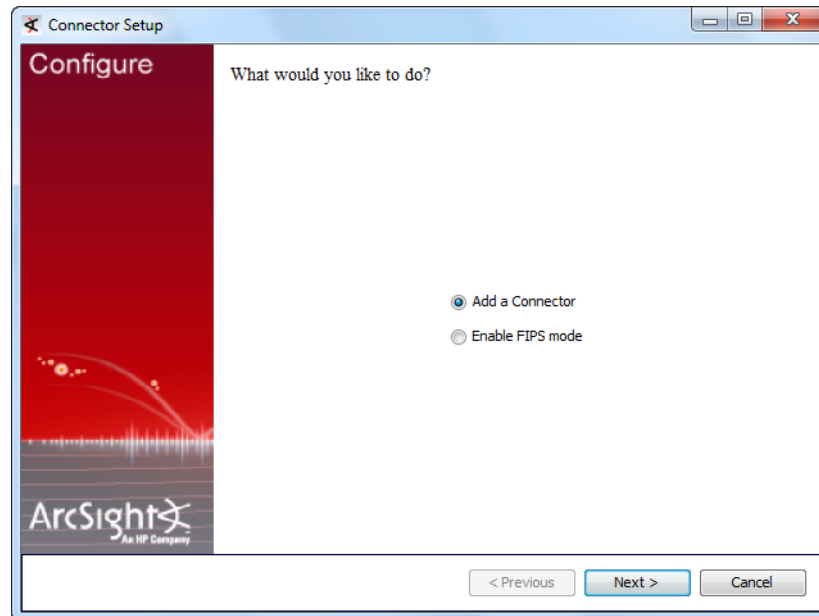
To continue connector configuration for forwarding events to a Manager, follow the procedure below.

**Note**

If the Manager will be using a non-demo certificate, this certificate must be imported before connector configuration can occur. Refer to the ArcSight ESM Administrator's Guide for instructions about configuring your SmartConnector when the Manager is using a self-signed or CA-signed certificate, and for instructions about enabling SSL client authentication on SmartConnectors so that the connectors and the Manager authenticate each other before sending data.

To continue connector configuration:

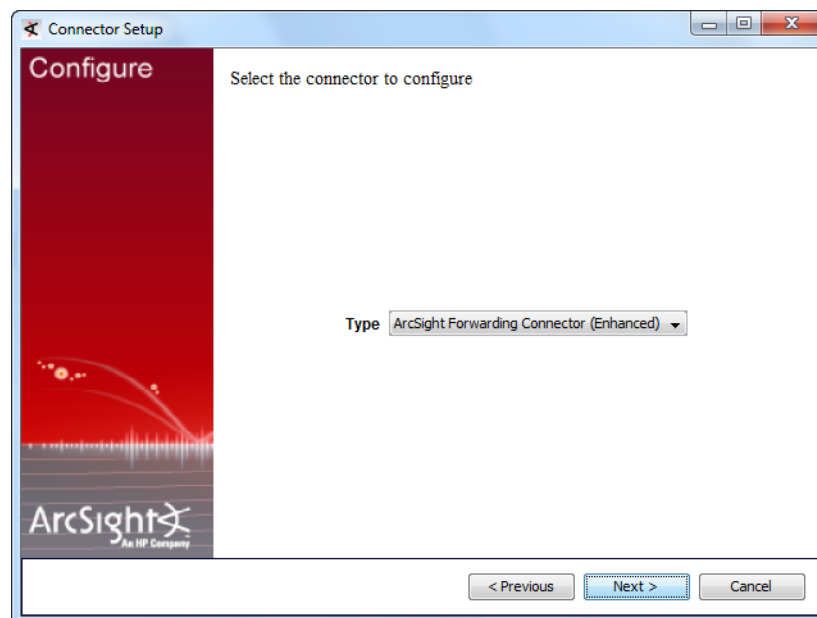
- 1 After you follow the steps in the section ["Installing the Forwarding Connector" on page 11](#), the following window is displayed:



Click **Next**.

- 2 You are given a choice of Forwarding Connector versions to install. Choose the **ArcSight Forwarding Connector (Enhanced)** option.

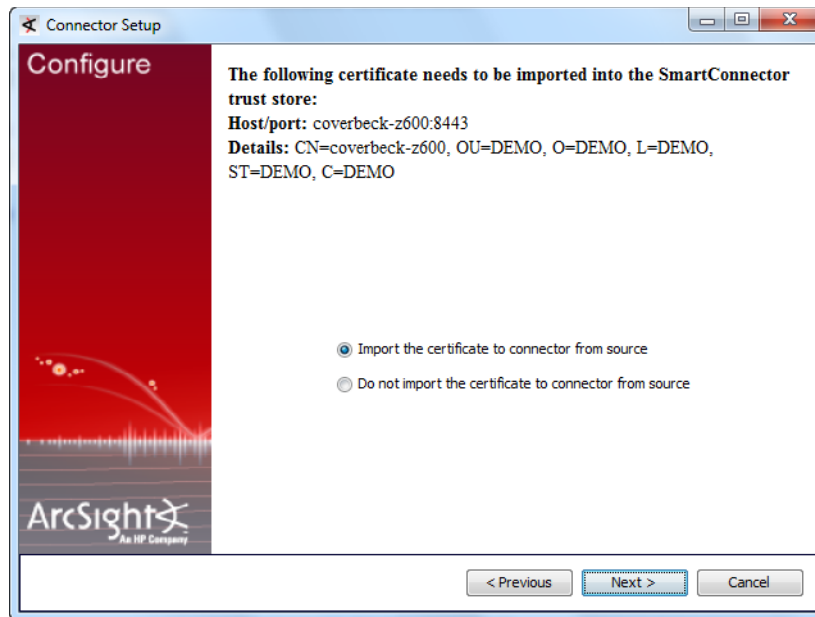
For instructions about how to determine and change your source disk settings, see ["Increasing the FileStore size \(Enhanced version only\)" on page 10](#). Click **Next**.



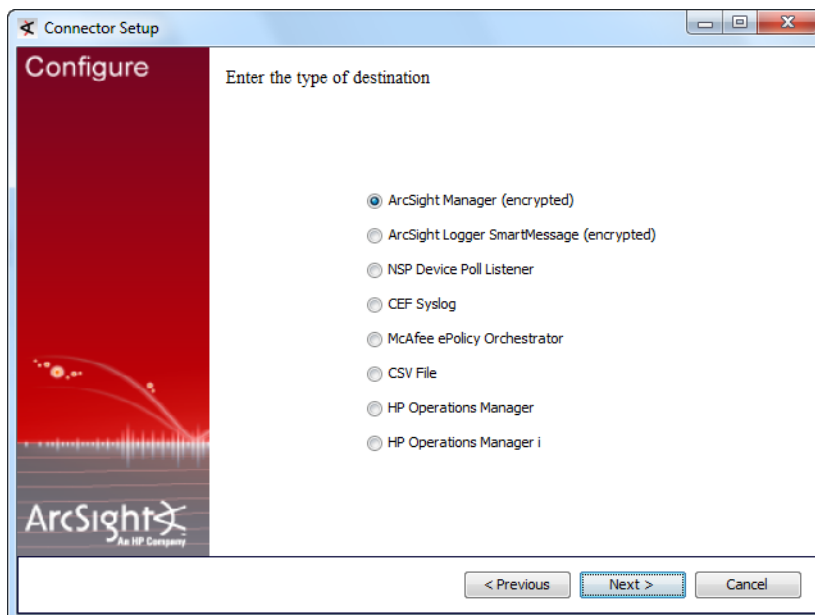
- 3 Enter the information to configure the Forwarding Connector, then click **Next** to continue. This is information about your source Manager, as described in the table below.

Parameter	Description
ArcSight Source Manager Host Name	The host name where the ArcSight ESM Source Manager is installed. In the certificate imported into the Manager, the Common Name (CN) is shown in the subject line. Use this Common Name as the value for ArcSight Source Manager Host Name.
ArcSight Source Manager Port	The network port where the ArcSight ESM Source Manager is accepting requests.
ArcSight Source Manager User Name	The ArcSight user name created with permissions for the Forwarding Connector on the ArcSight ESM Source Manager. Use the Forwarding Connector User Name as the value for the ArcSight Source Manager User Name.
ArcSight Source Manager Password	The ArcSight password that will be used to log this Connector into the ArcSight ESM Source Manager.

- 4 Select **Import the certificate to connector from source**, and click **Next**.



- 5 Select **ArcSight Manager (encrypted)**, and click **Next**.



- 6 You are prompted for **Manager Host Name** and **Manager Port**. This is your destination Manager. Enter the information and click **Next**.

The screenshot shows the 'Connector Setup' window with the 'Configure' tab selected. The title bar reads 'Connector Setup'. The main area is titled 'Enter the destination parameters'. On the left is a red sidebar with the 'ArcSight' logo and 'An HP Company' text. The main content area contains the following fields and controls:

- Manager Hostname:
- Manager Port:
- User:
- Password:
- AUP Master Destination: (dropdown arrow)
- Filter Out All Events: (dropdown arrow)
- Enable Demo CA: (dropdown arrow)

At the bottom right are three buttons: '< Previous', 'Next >' (highlighted with a blue border), and 'Cancel'.

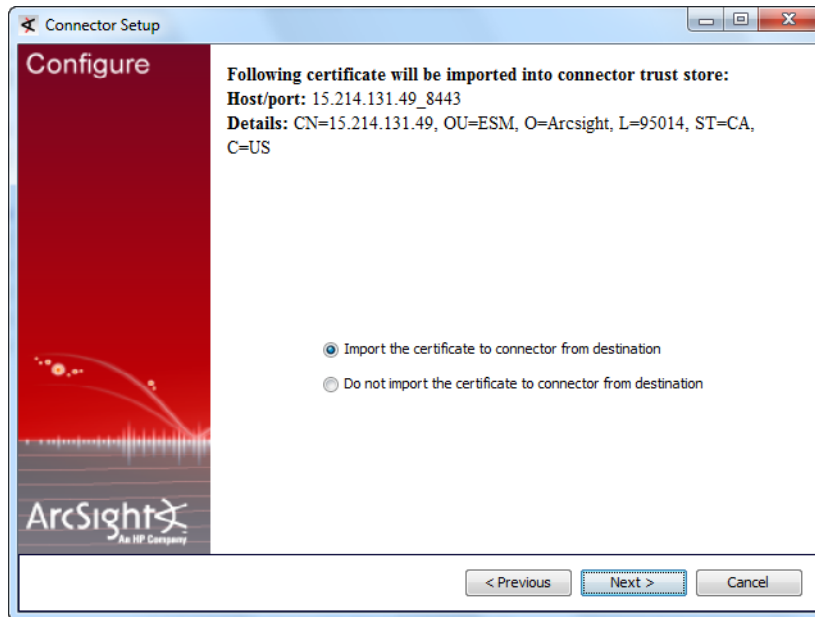
- 7 Enter the connector details and click **Next**.

The screenshot shows the 'Connector Setup' window with the 'Configure' tab selected. The title bar reads 'Connector Setup'. The main area is titled 'Enter the connector details'. On the left is a red sidebar with the 'ArcSight' logo and 'An HP Company' text. The main content area contains the following fields:

- Name:
- Location:
- DeviceLocation:
- Comment:

At the bottom right are three buttons: '< Previous', 'Next >' (highlighted with a blue border), and 'Cancel'.

- 8 Select **Import the certificate from destination**, and click **Next**.



- 9 Read the connector summary; if it is correct, click **Next**. If it is not correct, click **Previous** to make changes before continuing.
- 10 When the connector completes its configuration, click **Next**. The wizard now prompts you to choose whether to run the connector as a process or as a service. If you choose to run the connector as a service, the wizard prompts you to define service parameters for the connector.
- 11 After making your selections, click **Next**. The wizard displays a dialog confirming the connector's setup and service configuration.
- 12 To complete the installation, choose **Exit** and click **Next**. To enable FIPS-compliant mode, choose **Continue** and click **Next**, and continue with [Appendix A, Using the Forwarding Connector with FIPS](#), on page 39.

Forwarding Events to ArcSight Logger

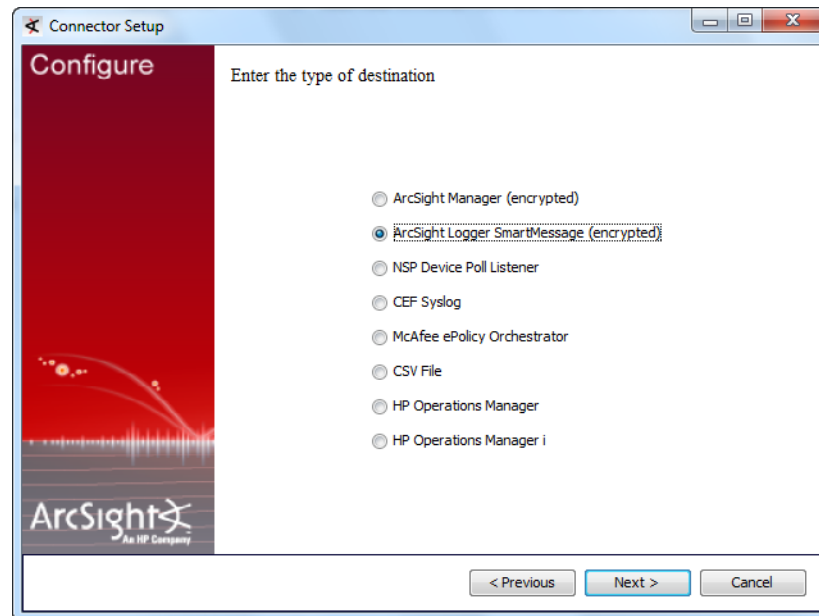


When configuring the Forwarding Connector to send events to a non-ESM destination, you might encounter problems with certificate validation during connector setup. See [“Sending Events to a Non-ESM Location” on page 6](#) for information about certificate validation.

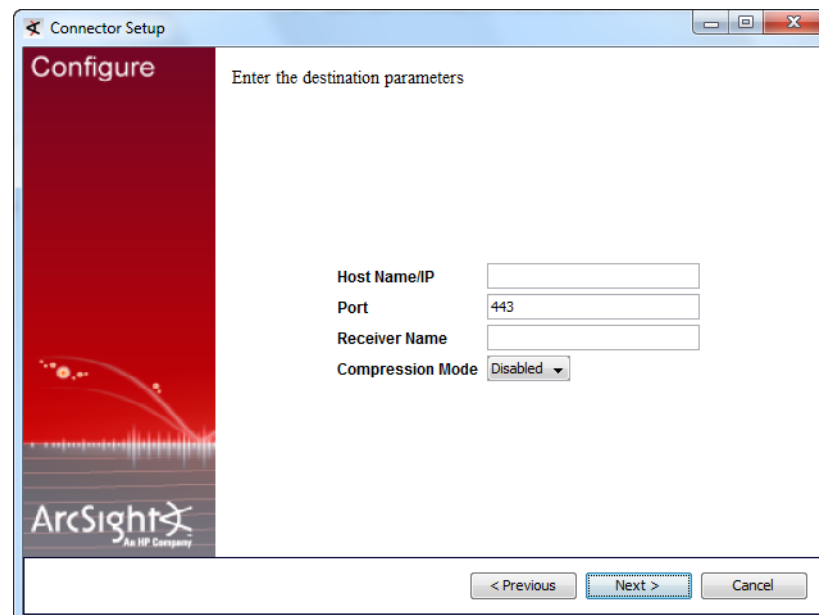
Before you continue connector configuration for forwarding events to an ArcSight Logger, ensure that a SmartMessage Receiver has been set up on ArcSight Logger for the Forwarding Connector (Refer to the ArcSight Logger Administrator's Guide for details).

To continue connector configuration:

- 1 Follow steps 1 through 4 in the procedure [“Forwarding Events to an ArcSight Manager” on page 13](#). Then select **ArcSight Logger SmartMessage (encrypted)** from the following dialog and click **Next**:



- 2 Enter the Logger **Host Name/IP** address, leave the port number at the default value of **443**, and enter the **Receiver Name**. This Receiver Name is the name of the SmartMessage Receiver you set up on ArcSight Logger for the Forwarding Connector. Click **Next** to continue.



- 3 Click **Next** and continue following steps 8 and onward in the procedure [“Forwarding Events to an ArcSight Manager” on page 13](#).

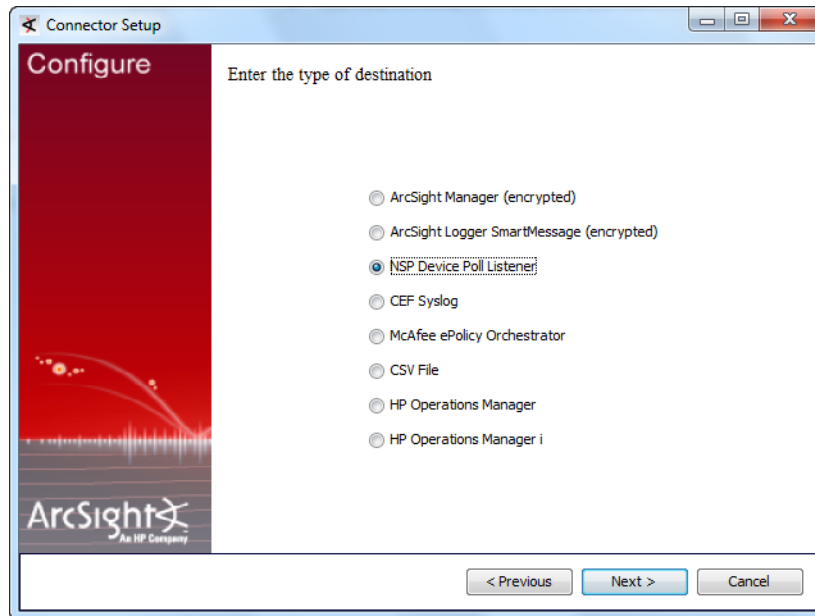
Forwarding Events to NSP Device Poll Listener

**Caution**

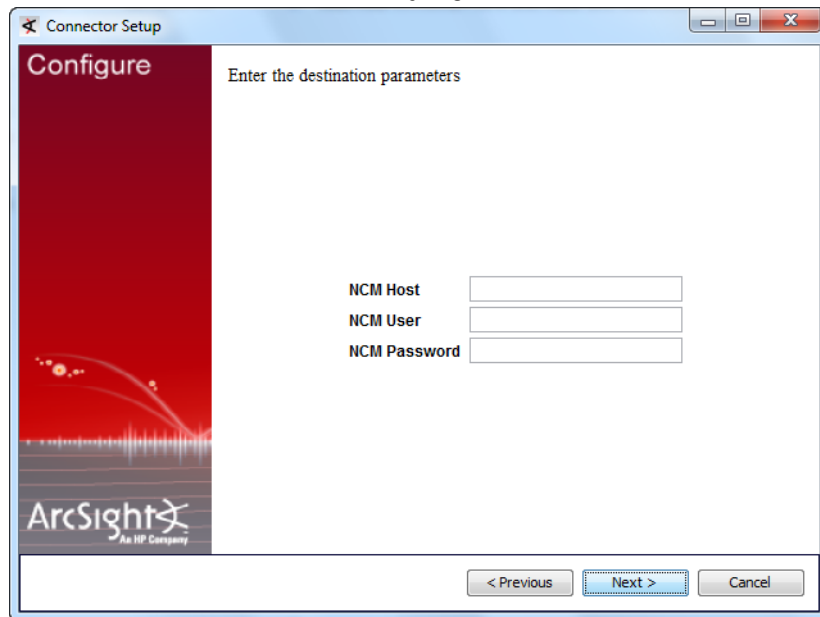
When configuring the Forwarding Connector to send events to a non-ESM destination, you might encounter problems with certificate validation during connector setup. See [“Sending Events to a Non-ESM Location” on page 6](#) for information on certificate validation.

To continue connector configuration for forwarding events to NSP:

- 1 Follow steps 1 through 4 in the procedure [“Forwarding Events to an ArcSight Manager” on page 13](#). Then select **NSP Device Poll Listener** from the selections and click **Next**.



- 2 Provide the NCM/TRM Host name or IP address, and login credentials for the NCM/TRM that will interact with the Syslog Connector.



- 3 Click **Next** and continue following steps 8 and onward in the procedure [“Forwarding Events to an ArcSight Manager” on page 13](#).

For more information about NSP, refer to the ArcSight NSP Installation and Administration Guide.

Forwarding CEF Syslog Events

You can configure the ArcSight Forwarding Connector to send CEF Syslog events to any Syslog receiver (including ArcSight Logger).

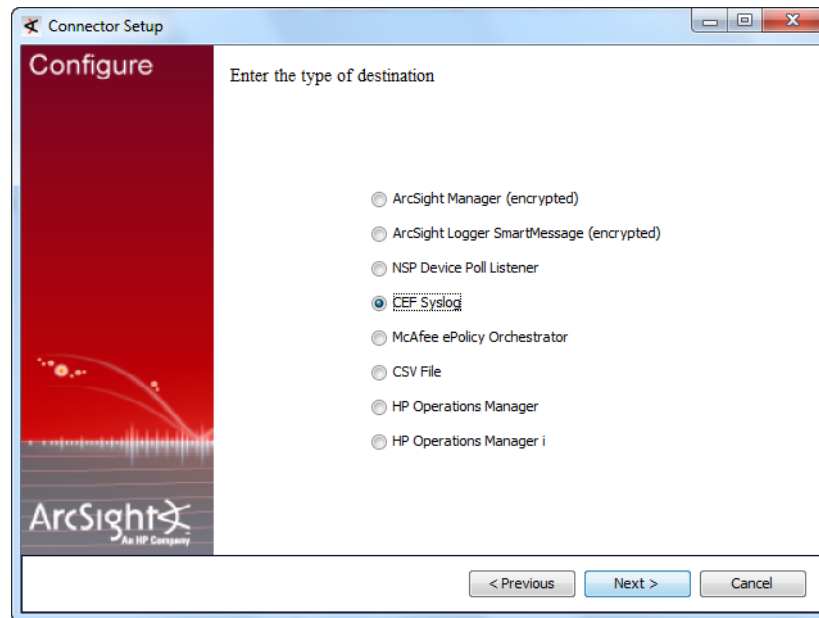


Caution

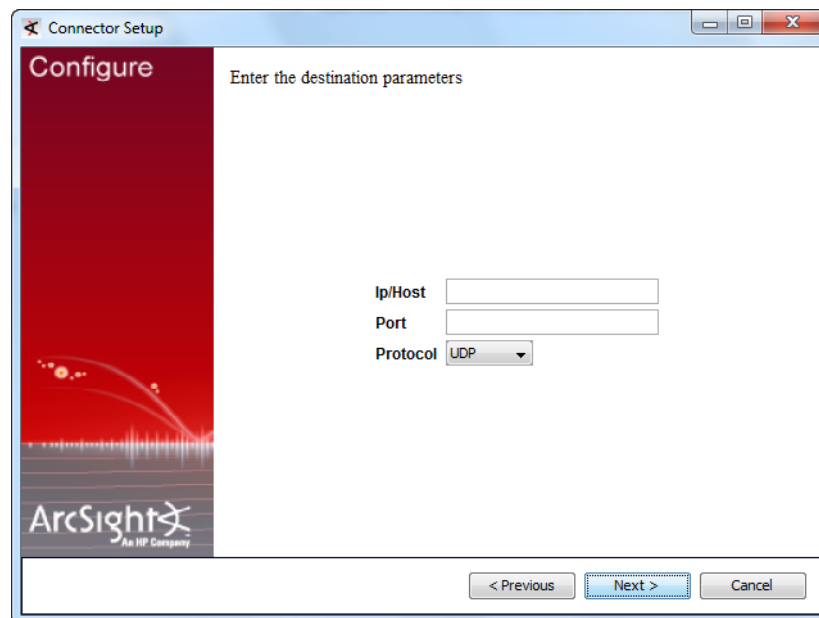
When configuring the Forwarding Connector to send events to a non-ESM destination, you might encounter problems with certificate validation during connector setup. See [“Sending Events to a Non-ESM Location” on page 6](#) for information on certificate validation.

To configure the connector to send CEF Syslog events:

- 1 Follow steps 1 through 4 in the procedure [“Forwarding Events to an ArcSight Manager” on page 13](#). Then select **CEF Syslog** from the following dialog:



- 2 Enter the Logger **host name** or **IP address**, the desired port, and choose **UDP**, **TLS**, or **TCP** output. Click **Next** to continue.



- 3 Click **Next** and continue following steps 8 and onward in the procedure [“Forwarding Events to an ArcSight Manager” on page 13](#).

Forwarding Events to a CSV File

You can capture events a SmartConnector would normally send to the ArcSight Manager and write them to a .csv file. The Excel-compatible comma-separated values (CSV) format allows for comments prefixed by #.

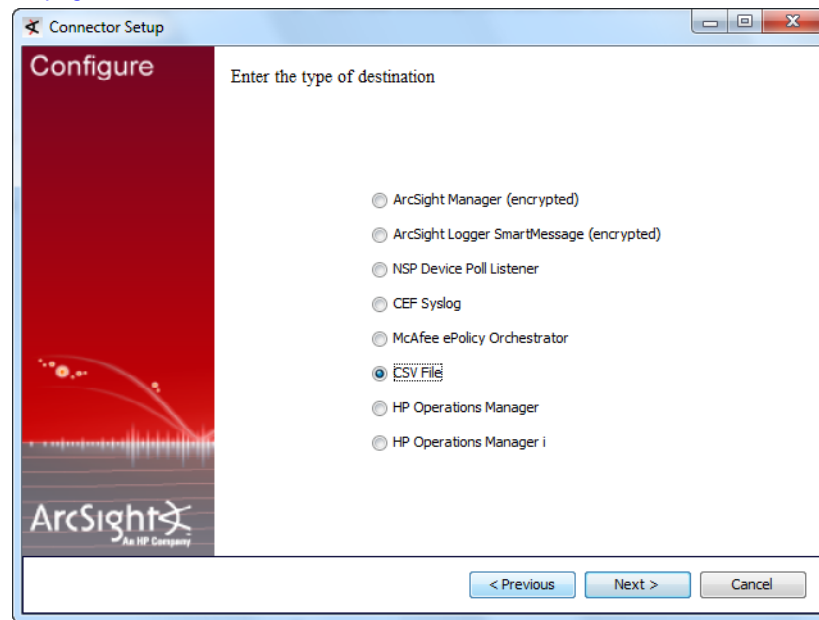


Caution

When configuring the Forwarding Connector to send events to a non-ESM destination, you might encounter problems with certificate validation during connector setup. See [“Sending Events to a Non-ESM Location” on page 6](#) for information on certificate validation.

To forward events to a .csv file:

- 1 Follow steps 1 through 4 in the procedure [“Forwarding Events to an ArcSight Manager” on page 13](#). Then select **CSV File** and click **Next**.



- 2 Enter values as described in the table below.

Parameter	Description
CSV Path	The path to the output folder and the .csv file. For example, C:\CSV_files\events.csv. If a folder does not exist, it is created.
Fields	A comma-delimited string of field names to be sent to the .csv file. Field names are in the form event.<FieldName>.
File rotation interval	The desired file rotation interval, in seconds. The default is 3,600 seconds (one hour).
Write format header	Select true to send a header row with labels for each column, as described above.

- 3 Click **Next** and continue following steps 8 and onward in the procedure [“Forwarding Events to an ArcSight Manager” on page 13](#).

For more information about capturing events and .csv files, refer to the section titled “Capturing Events from SmartConnectors” in the SmartConnector User’s Guide.

Forwarding Events to McAfee ePolicy Orchestrator

This option allows you to forward events to McAfee ePolicy Orchestrator (ePO), a scalable tool for centralized anti-virus and security policy management and enforcement. ePO leverages ESM event filtering/correlation and auditing capabilities to create a single view into security events within ePO.

McAfee ePO v4.0, v4.5, and v.4.6 are currently supported.

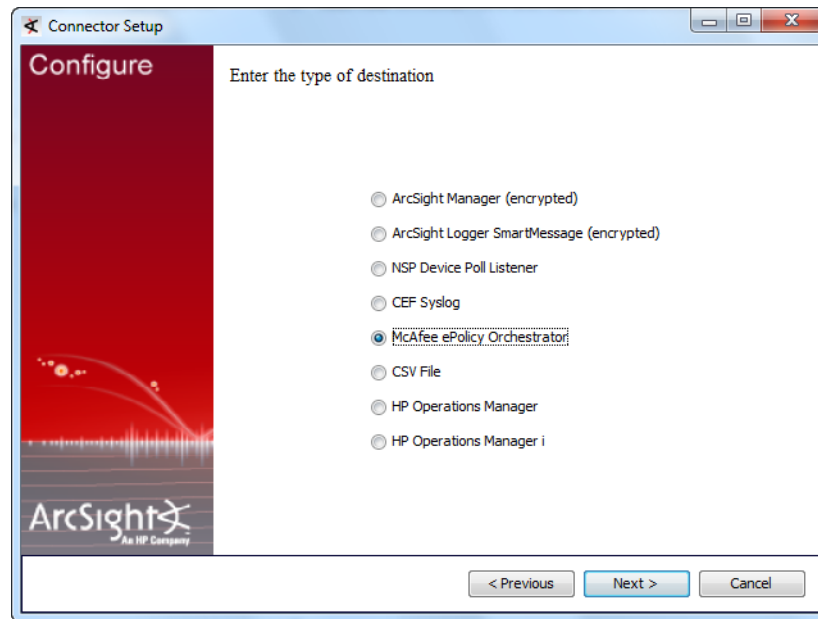


Caution

Use of ePO requires installation of **MS SQL Server 2005 for JDBC driver**. For instructions on downloading, see [“Installing the Microsoft JDBC Driver for SQL Server” on page 26](#).

To forward events to McAfee ePO:

- 1 Follow steps 1 through 4 in the procedure [“Forwarding Events to an ArcSight Manager” on page 13](#). Then select **McAfee ePolicy Orchestrator** and click **Next**.



Caution

When using this transport, the Forwarding Connector is automatically configured to limit the outgoing event rate to 10 events per minute. This is due to a limitation on McAfee ePO's database as specified by McAfee.

- 2 Enter or select values for the ePO database connectivity:



Note

- To log on to the database at this point, only Microsoft SQL Server authentication is supported (Windows authentication is not).
- ArcSight recommends that you create a user dedicated to ArcSight with permissions to execute the stored procedure.

- 3 Click **Next** and continue following steps 8 and onward in the procedure “[Forwarding Events to an ArcSight Manager](#)” on page 13.

Installing the Microsoft JDBC Driver for SQL Server

To download and install a JDBC driver:

- 1 For information about and to download the MS SQL Server JDBC Driver, see:

<http://msdn.microsoft.com/en-us/sqlserver/aa937724>

Different versions of the JDBC driver are required for different SQL Server database versions; be sure to use the correct driver for your database version. The name of the jar file may be different for some JDBC driver versions.

- 2 Install the driver.
- 3 Copy the `sqljdbc.jar` file from the folder `C:\Program Files\Microsoft SQL <driver_version>` to `$ARCSIGHT_HOME/current/user/agent/lib`, where `$ARCSIGHT_HOME` refers to the connector install folder, such as `c:\ArcSight\SmartConnectors` (where `driver_version`) is the correct driver for your database version.
- 4 From `$ARCSIGHT_HOME/current/bin`, double-click `runagentsetup` to return to the SmartConnector Configuration Wizard.

ArcSight Event to McAfee CEF Mappings

The Forwarding Connector translates ArcSight events into McAfee's Common Event Format.



The McAfee CEF field column shown in the following table does not represent fields seen in the Console GUI of McAfee ePolicy Orchestrator. This column represents fields within the database.

The following table lists the field mappings.

McAfee CEF Field	ArcSight Field
AgentGUID	agented (converted to match the AgentGUID format; guaranteed to be unique ONLY within ArcSight)
Analyzer	Fixed value: S_ARST__1000
AnalyzerDATVersion	deviceCustomString6
AnalyzerHostName	deviceHostName
AnalyzerIPV4	deviceAddress
AnalyzerMAC	deviceMacAddress
AnalyzerName	deviceProduct
AnalyzerVersion	deviceVersion
DetectedUTC	deviceReceiptTime
SourceHostName	sourceHostName
SourceIPV4	sourceAddress
SourceMAC	sourceMacAddress
SourceProcessName	sourceProcessName
SourceURL	requestUrl
SourceUserName	sourceUserName
TargetFileName	fileName
TargetHostName	destinationHostName
TargetIPV4	destinationAddress
TargetMAC	destinationMacAddress
TargetPort	destinationPort
TargetProcessName	destinationProcessName
TargetProtocol	applicationProtocol
TargetUserName	destinationUserName
ThreatActionTaken	deviceAction
ThreatCategory	deviceEventCategory

McAfee CEF Field	ArcSight Field
ThreatEventID	agentSeverity 200300 – Unknown 200301 – Low 200302 – Medium 200303 – High 200304 – Very High
ThreatName	name
ThreatType	deviceEventClassId

For more details regarding McAfee ePolicy Orchestrator, refer to the SmartConnector Configuration Guide for McAfee ePolicy Orchestrator DB.

Configuring Multiple Destinations

It is also possible to configure multiple destinations, after installation of the Forwarding Connector, using the ArcSight SmartConnector Configuration Wizard.

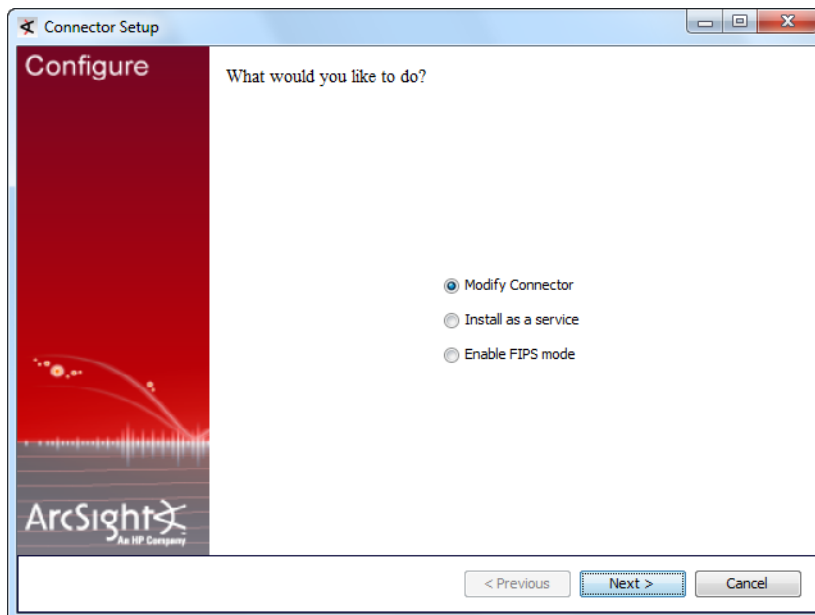
To configure multiple destinations:

- 1 To start the wizard, execute the following command:

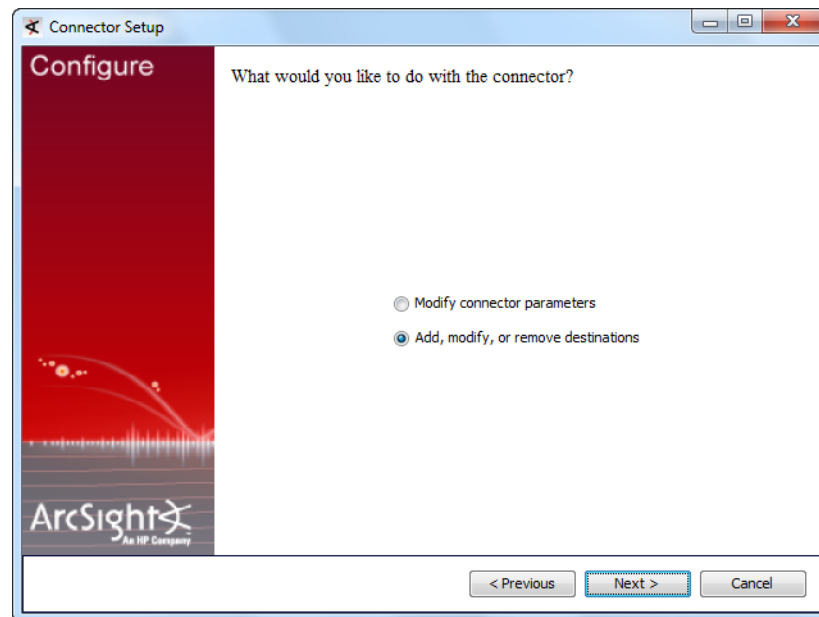
```
$ARCSIGHT_HOME\current\bin\runagentsetup
```

You can either modify the existing destination or add a new destination. The following example shows how to add a second ArcSight Manager.

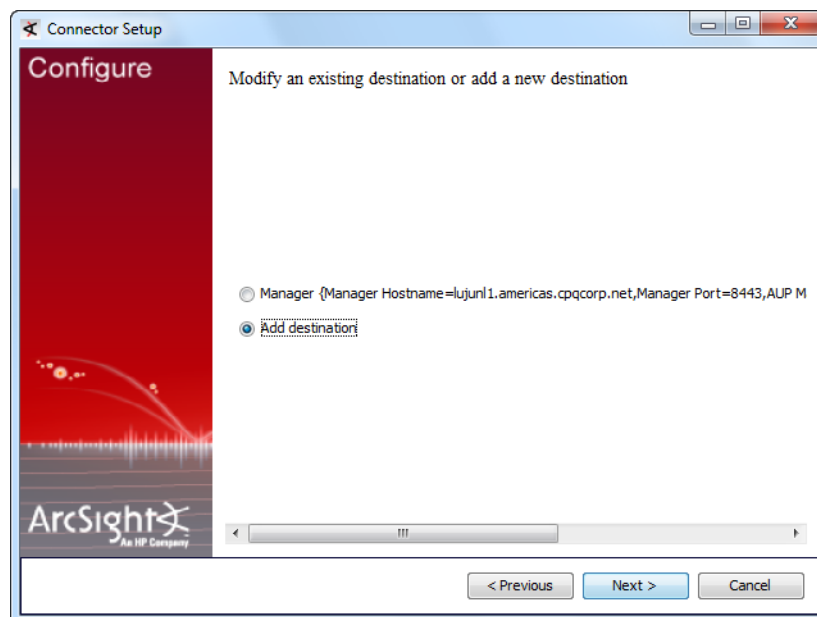
- 2 Select **Modify Connector** and click **Next**.



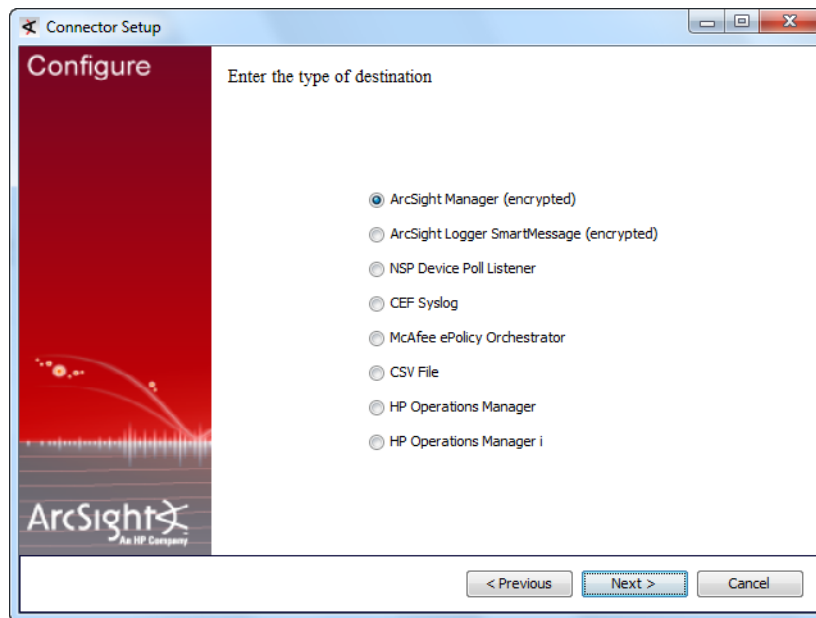
- 3 Select **Add, modify, or remove destinations** and click **Next**.



- 4 Select **Add destination** and click **Next**.

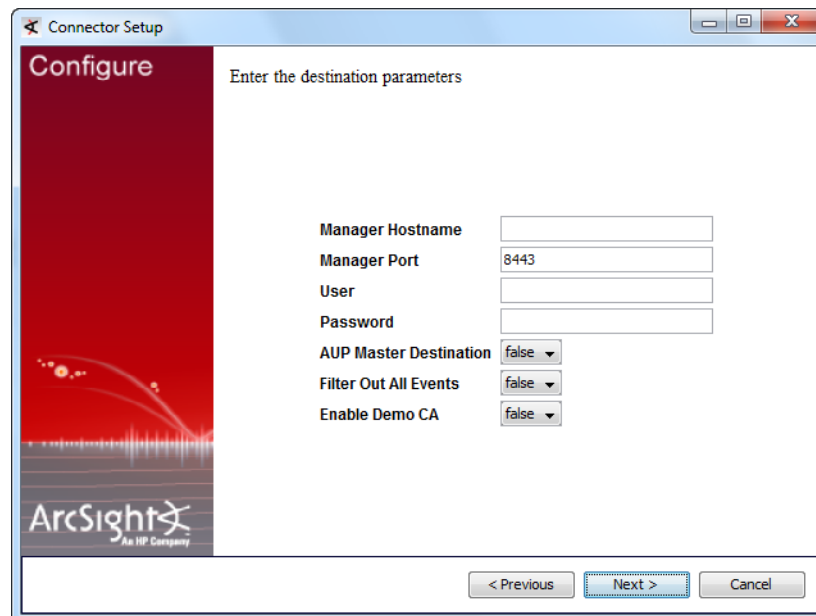


- 5 Select the destination type and click **Next**.



- 6 Choose **Add new destination** to add a new SmartConnector destination and click **Next**.

- 7 Enter or select in the parameters for the destination being added and click **Next**.



- 8 To complete the installation, choose **Exit** and click **Next**.
- 9 To apply your changes, restart the SmartConnector.

Chapter 3

Configuration for HP OM and HP OMi

This chapter provides information on configuring HP Operations Manager and HP Operations Manager i to work with the ArcSight Forwarding Connector.

- ["The ArcSight ESM Source Manager" on page 32](#)
- ["Supported Versions of HP OM and HP OMi" on page 32](#)
- ["Installing the Connector" on page 32](#)
- ["Creating an SNMP Interceptor Policy for HP Operations Manager \(HP OM\)" on page 35](#)
- ["Creating an SNMP Interceptor Policy for HP Operations Manager i \(HP OMi\)" on page 35](#)
- ["Troubleshooting Tips" on page 36](#)
- ["Adjusting the Event Processing Rate for HP OM and HP OMi" on page 36](#)

ArcSight ESM sends correlated security events to IT operation teams to investigate and take measures to reduce or eliminate security risks. The ArcSight Forwarding Connector logs into the source manager, then sends system events and network health information to HP OM from non-SNMP event sources. The ArcSight Forwarding Connector can be used to collect from event sources that support syslog, file, database, API, and other collection methods through ESM.

HP Operations Manager (HP OM) provides comprehensive event management, proactive performance monitoring, and automated alerting, reporting, and graphing for operating systems, middleware, and applications. It is designed to provide service-driven event and performance management of business-critical enterprise systems, applications, and services. The following topics are described.

HP Operations Manager i (HP OMi) enables the HP BSM Operations Management component in BSM. BSM Operations Management provides a complete monitoring solution, consolidating all IT infrastructure monitoring in a central event console, and relating the events to the IT services that depend on that infrastructure. See the HP Business Service Management Operations Manager i Concepts Guide for details on BSM.

HP BSM Integration Adapter is an integration solution that enables you to monitor event sources, and, if certain conditions apply, to forward the detected events as HP Business Service Management (BSM) events directly to BSM Operations Management. See the Using HP BSM Integration Adapter Guide for details on HP BSM Integration Adapter.

The ArcSight ESM Source Manager

Before installing the Forwarding Connector, create a Forwarding Connector account on the Manager. For instructions, see ["Assigning Privileges on the ESM Source Manager" on page 7](#).

Supported Versions of HP OM and HP OMi

The supported versions of HP OM and HP OMi include:

- HP OM for Windows v9.0 and 8.16 (patch level 90)
- HP OM for UNIX v9.10
- HP OM for Linux v9.10
- HP OMi v9.0.1.



Note

OMi users are strongly encouraged to apply the latest patch, OMI_00005 (build 09.01.210), to obtain critical fixes before running this integration.

- HP OMi v9.10

HP OM and HP OMi and Correlation Events

When all rule conditions and thresholds are met, ESM generates an internal event called a **correlation event**. A correlation event represents the events that contributed to the rule being triggered and the relevant data contained in them.

Although most ESM users can use the default settings available for retrieving events, HP OM and HP OMi users commonly require only correlated events to be retrieved from ESM. In such cases, HP OM and HP OMi users can select correlated events. To allow for only correlated events and restrict the retrieval of base events, configure ESM to **retrieve correlated events**, then **allow the forwarding of correlated events**, in that order. For instructions, see ["Forwarding Correlation Events" on page 9](#).

HP OM and HP OMi use a SNMP trap policy to allow ArcSight events to be accepted within the HP OM or HP OMi environment. For instructions on how to create an SNMP interceptor, see ["Creating an SNMP Interceptor Policy for HP Operations Manager \(HP OM\)" on page 35](#) or ["Creating an SNMP Interceptor Policy for HP Operations Manager i \(HP OMi\)" on page 35](#).

Installing the Connector

Before you install the connector, make sure that the ArcSight products with which the connectors will communicate have already been installed correctly and you have assigned appropriate privileges. For data security, ArcSight recommends that you install the connector and the HP Operations Agent on the same system.

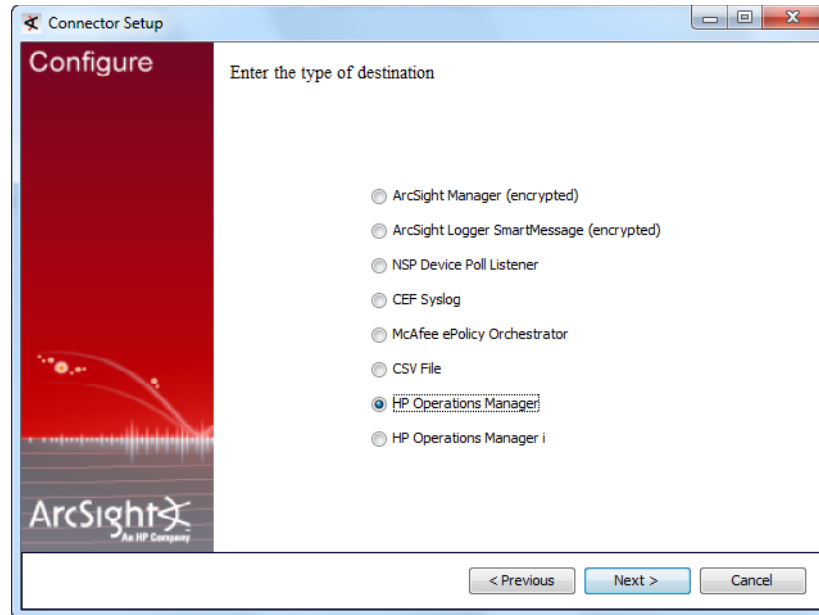
To install the Forwarding Connector:

- 1 Download the install executable for your operating system from the HP SSO site.
- 2 Start the ArcSight Installer by running the executable.

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

Introduction
Choose Install Folder
Choose Install Set
Choose Shortcut Folder
Pre-Installation Summary
Installing...

- 3 Follow steps 1 through 4 in the procedure [“Forwarding Events to an ArcSight Manager” on page 13](#). Then select **HP Operations Manager or HP Operations Manager i**. Click **Next** to continue.



- 4 Fill in the parameter information required for connector configuration. Click **Next** to continue.

Connector Setup

Configure

Enter the destination parameters

Host: 127.0.0.1

Port: 162

Version: SNMP_VERSION_2

Read Community(v2): public

Write Community(v2): public

Authentication Username(v3):

Authentication Password(v3):

Security Level(v3): AuthNoPriv

Authentication Scheme(v3): MD5

Privacy Password(v3):

Context Engine Id(v3):

Context Name(v3):

< Previous Next > Cancel

Parameter	Description
Host	For HP OM, enter the Host name or IP address of the HP OM device. This is the HP OM managed node (the system where the HP Operations Agent is installed, and to which the SNMP interceptor policy is deployed). For HP OMI, enter the Host name or IP address of the HP BSM Integration Adapter.
Port	For HP OM and HP OMI, enter the port to be used by the device to monitor for events by the HP Operations Agent or by the BSM Integration Adapter monitoring for SNMP traps from the ArcSight Logger.
Version	Accept the default value of SNMP_VERSION_2 . SNMP_VERSION_3 is not currently available.
Read Community(v2)	Enter the SNMP Read Community name.
Write Community(v2)	Enter the SNMP Write Community name.
Authentication Username(v3)	For use with SNMP v3. Not currently available.
	Authentication Password(v3)
	Security Level(v3)
	Authentication Scheme(v3)
	Privacy Password(v3)
	Context Engine Id(v3)
	Context name(v3)

- 5 Click **Next** and continue following steps 8 and onward in the procedure [“Forwarding Events to an ArcSight Manager” on page 13](#).

Creating an SNMP Interceptor Policy for HP Operations Manager (HP OM)

An SNMP interceptor policy is a type of HP OM policy, with rules, conditions, and actions. Rules define what a policy should do in response to a specific type of event. Each rule consists of a condition and an action. SNMP interceptor policies monitor SNMP events, and can start actions when an SNMP event contains a specified character pattern. The Forwarding Connector sends security events as SNMP traps to an HP OM SNMP interceptor policy that you will create.

SNMP interceptor policies can be configured on either HP OM UI, HP OM for Windows, or HP OM for UNIX or Linux.

See [“Troubleshooting Tips” on page 36](#) for details if you encounter duplicate or dropped events.

Uploading Interceptor Template

Download the latest policy files from the download site where you obtained the connector.

Refer to the *ArcSight HP OM and HP OMi SNMP Interceptor Policy Readme* for details on uploading the template for Operations Manager for Windows and Operations Manager for UNIX or Linux.

Deploying the Policy

Once you have created your customized SNMP interceptor policy, deploy or assign the policy through the HP OM for Windows or HP OM for UNIX or Linux Administration UI. For details, refer to the HP Operations Manager online help and documentation.

The systems that send the SNMP traps to the Logger must also be set up as nodes in HP OM, because HP OM discards messages from unknown systems. Set up an external node or an SNMP node. For details, refer to the HP Operations Manager online help and documentation.

Also, configure the HP Operations Agent for SNMPv2 by setting the **SNMP_SESSION_MODE** variable using the **ovconfchg** command line tool. Refer to the HP Operations Manager or HP Operations Agent online help and documentation for more information.

Creating an SNMP Interceptor Policy for HP Operations Manager i (HP OMi)

HP BSM Integration Adapter SNMP interceptor policies monitor SNMP events, and respond when a character pattern that you choose is found in an SNMP trap. ArcSight provides a template SNMP interceptor policy for use in creating your own customized SNMP interceptor policy. This template policy should be customized and enhanced to satisfy different needs and requirements with HP BSM Integration Adapter's powerful policy edit features.

See [“Troubleshooting Tips” on page 36](#) for details if you encounter duplicate or dropped events.

Uploading Interceptor Template

Download the latest policy files from the download site where you obtained the connector.

Refer to the *ArcSight HP OM and HP OMi SNMP Interceptor Policy Readme* for details on uploading the template.

Troubleshooting Tips

Duplicate Events (for HP OMi)

If there appear to be duplicate events forwarded to the HP OMi console:

- 1 Check and adjust deduplication options as needed.
- 2 If, after modifying deduplication options, there still appear to be duplicate events, check the Custom Message Attributes (event details and data), and apply rules to differentiate the events.

For HP OMi, Refer to the HP Business Service Management Using Operations Management Guide and help for details.

For HP OM, refer to the HP Operations Manager online help for details.

Dropped Events

If you notice that some events forwarded from ArcSight ESM/Logger are dropped, verify whether the Agent Severity is set correctly in those events. The default SNMP interceptor policy provided by ArcSight in the connector distribution has rules to pick up and forward SNMP Traps from ArcSight ESM/Logger based on the Agent Severity. Events that do not have Agent Severity set are dropped and not forwarded by the SNMP interceptor policy. If the dropped events are correlated events from ESM, make sure that the rules on ESM are set for the correct Agent Severity in the correlated events they generate. If the dropped events are normalized events from devices, then verify that the originating connector that has normalized the event has mapped the Agent Severity correctly from the Device Severity. If the originating connector (that is not setting the Agent Severity) is a FlexConnector, review the mappings and map all of the device severities to one of these Agent Severity values: Low, Medium, High, or Very-High. If the connector is a supported connector, contact customer support.

Adjusting the Event Processing Rate for HP OM and HP OMi

The default event processing rate for forwarding events from ESM to HP OM is **50 eps**. For HP OMi, the default processing rate is **10 eps**. If this rate proves excessive for your system, HP OM or HP OMi might drop some incoming events. If events are being dropped, decrease the event processing rate until you find that all events have arrived.

If this occurs, you can adjust the rate at which events are forwarded to HP OM or HP OMi. To do so, you will need to change the event processing rate within your XML properties file.

To adjust the event processing rate,

- 1 Stop the currently running SmartConnector from operating.
- 2 From a Windows command line, access your XML properties file using the command

```
cd %ARCSIGHT_HOME%/current/user/agent
```

- 3 Use WordPad or any XML Editor to open the .xml file for your HP OM or HP OMi destination, similar to the example below:

```
0Ajv5S8BABCBAeabNXP5Rw==.xml
```

- 4 From within the .xml file, search for the following for HP OM:

```
ProcessingSettings.ThrottleRate="50"
```

or, for HP OMi:

```
ProcessingSettings.ThrottleRate="10"
```

This value controls the current processing event rate.

- 5 Change this value to the desired rate of events per second. For example, to lower the rate of events to 5 eps, change the value after the string to 5:

```
ProcessingSettings.ThrottleRate="5"
```



If there are multiple destinations, repeat the steps above to change the rate for each destination, as required.

-
- 6 Save the .xml file and exit the XML editor.
 - 7 Restart the SmartConnector.

Appendix A

Using the Forwarding Connector with FIPS

The following topics provide information and instructions for enabling FIPS compliance in the use of the Forwarding Connector.

[“What is FIPS?” on page 39](#)

[“ArcSight ESM Installation” on page 39](#)

[“FIPS-Enabled Forwarding Connector Installation” on page 40](#)

[“Using Logger in FIPS Mode” on page 45](#)

What is FIPS?

Under the Information Technology Management Reform Act (Public Law 104-106), the Secretary of Commerce approves standards and guidelines that are developed by the National Institute of Standards and Technology (NIST) for Federal computer systems. These standards and guidelines are issued by NIST as Federal Information Processing Standards (FIPS) for use government-wide. NIST develops FIPS when there are compelling Federal government requirements such as for security and interoperability and there are no acceptable industry standards or solutions.



FIPS compatibility applies only to standard ESM and Logger destinations.

ArcSight ESM Installation

Before you install an ArcSight Forwarding Connector, make sure that ArcSight ESM has already been installed correctly for FIPS compliance. See [“Standard Installation Procedures” on page 7](#) for instructions. Also, ArcSight recommends reading the ArcSight ESM Installation and Configuration Guide before attempting to install a new Forwarding Connector.

For information regarding operating systems and platforms supported, see SmartConnector Product and Platform Support, available from ArcSight Technical Support with each SmartConnector release.

FIPS-Enabled Forwarding Connector Installation

You must manually import the certificate, and then continue the connector configuration in the wizard.

Manually Importing the Certificate

Before continuing with the connector configuration and enabling FIPS Suite B mode, you must manually import the certificates for the source and destination Managers using the commands detailed in these steps. In the commands below, `srcmgrkey` and `destmgrkey` are alias names and `srcmgrkey.cert` and `destmgrkey.cert` are the names with which the certificates from the Managers were saved.

- 1 Use this command to import the source Manager's certificate: `arcsight runcertutil -A -n srcmgrkey -t "CT,C,C" -d user/agent/nssdb.client -i bin/srcmgrkey.cert`

This command will display, in plain text (as shown below), the contents of the source Manager's certificate and can be used to determine the name put into the connector configuration for the source Manager: `arcsight runcertutil -L -n srcmgrkey -t "CT,C,C" -d user/agent/nssdb.client`



To confirm the Manager's certificate name, look under Subject: "CN=*", as shown in the following example.

- 2 Use this command to import the destination Manager's certificate: `arcsight runcertutil -A -n destmgrkey -t "CT,C,C" -d user/agent/nssdb.client -i bin/destmgrkey.cert`

This command displays, in plain text, the contents of the destination Manager's certificate and can be used to determine the name put into the connector configuration for the destination manager: `arcsight runcertutil -L -n destmgrkey -t "CT,C,C" -d user/agent/nssdb.client`

```
ArcSight certutil starting...
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 4524 (0x11ac)
    Signature Algorithm: PKCS #1 MD5 with RSA Encryption
    Issuer: "CN=solar"
    Validity:
      Not Before: Tue Nov 10 03:45:06 2009
      Not After: Wed Feb 10 03:45:06 2010
    Subject: "CN=solar"
    Subject Public Key Info:
      Public Key Algorithm: PKCS #1 RSA Encryption
      RSA Public Key:
        Modulus:
          cd:f2:24:ac:7d:12:f8:3e:0c:42:c8:12:d9:33:1b:b0:
          fd:07:fd:f2:6d:38:5d:e0:9c:1a:e8:10:a7:87:ca:f4:
          7e:21:be:b1:58:f4:d9:f5:7f:8c:a9:49:81:1c:75:48:
          23:10:30:d9:06:15:7a:6c:40:f2:fd:ba:62:0c:e5:81:
          23:09:e7:34:74:3a:00:30:99:a6:8d:3f:fe:e6:8d:45:
          c9:55:78:d5:a6:ef:3b:04:2d:7b:45:c8:0f:9f:d4:9c:
          a2:a6:9d:ca:3a:46:2a:0c:49:cd:c0:82:6b:bc:0f:cd:
          99:e1:ca:a0:b9:d7:84:51:5e:76:39:3b:59:82:2b:dd
        Exponent: 65537 (0x10001)
```



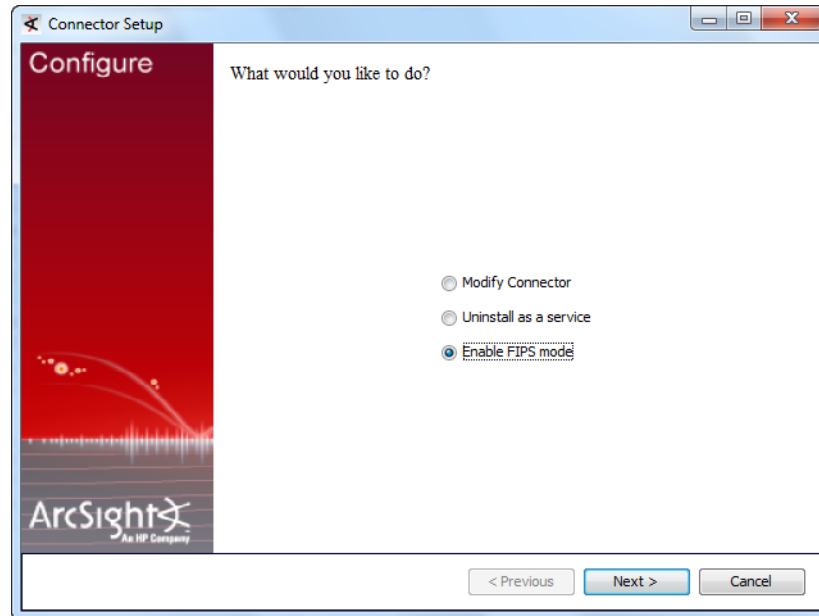
Your **host name** must match the **Manager's certificate name** (circled above as an example) and must be DNS resolvable. If these fields do not match, the connection will fail.

Enabling FIPS Suite B Mode

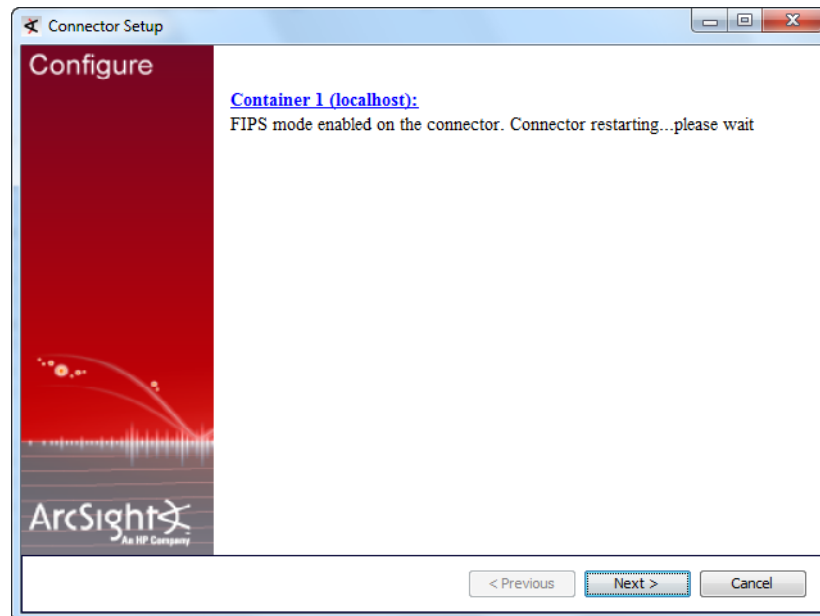
After completion of ArcSight ESM installation follow the instructions under [“Installing the Forwarding Connector” on page 11](#). Do not exit the configuration, and you can continue and configure FIPS for the Forwarding Connector

To install a FIPS-enabled Forwarding Connector:

- 1 After choosing **Continue** and clicking **Next** after connector installation, Choose **Enable FIPS Mode** and click **Next**.

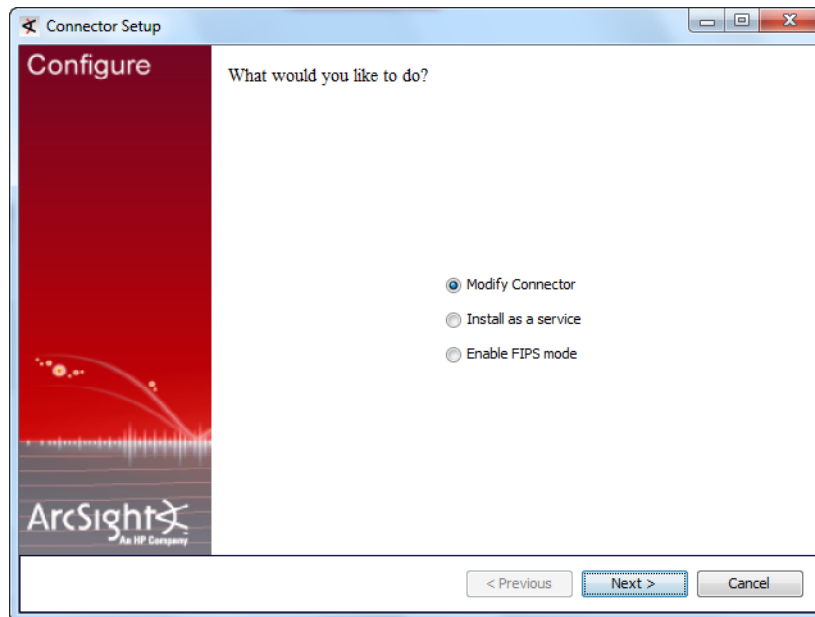


The following window is displayed when FIPS mode is enabled.

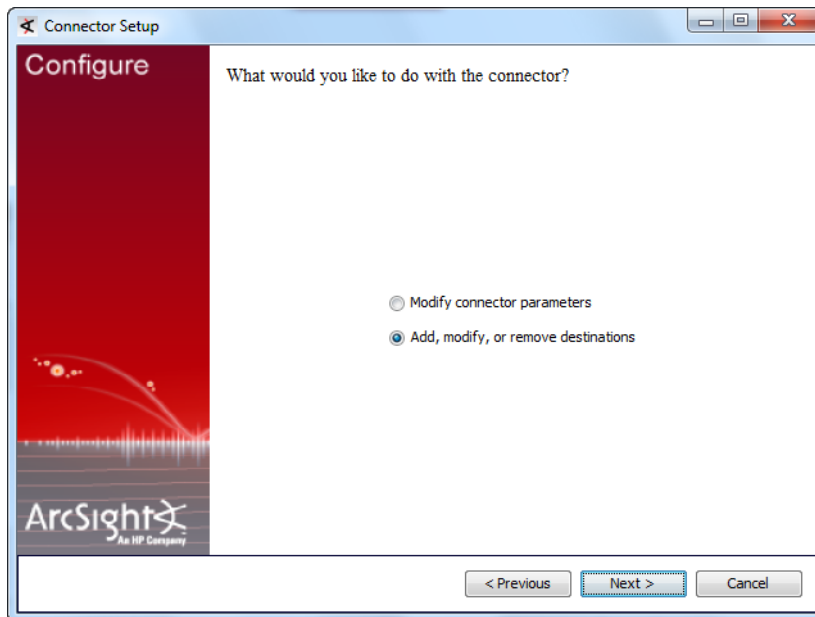


- 2 Click **Next**. To complete installation of FIPS support, click **Exit**. To enable FIPS Suite B mode, click **Continue**.

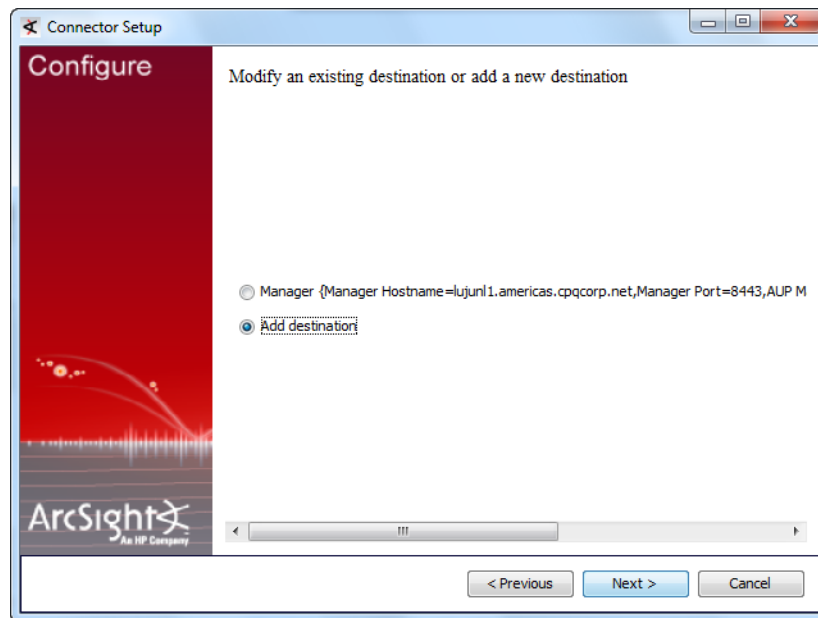
- 3 On the window displayed, select **Modify Connector**.



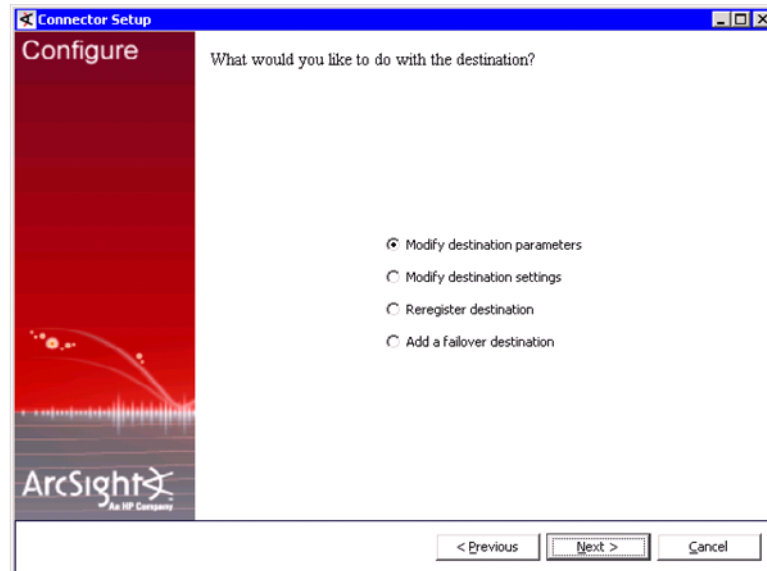
- 4 Select **Add, modify, or remove destinations** and click **Next**.



- 5 Select the destination for which you want to enable FIPS Suite B mode and click **Next**.



- 6 Select **Modify destination parameters** and click **Next**.



- 7 When the parameters window is displayed, select **FIPS with Suite B 128 bits** or **FIPS with Suite B 192 bits** for the **FIPS Cipher Suites** parameter. Click **Next**.

Connector Setup

Configure

Enter these parameters

Manager Hostname: 1.1.1.1

Manager Port: 8443

User:

Password:

AUP Master Destination: false

Filter Out All Events: false

FIPS Cipher Suites: FIPS Default
FIPS with Suite B 128 bits
FIPS with Suite B 192 bits

< Previous Next > Cancel

- 8 The following window shows the editing changes to be made. Confirm and click **Next** to continue. To adjust the changes before confirming, click **Previous**.

Connector Setup

Configure

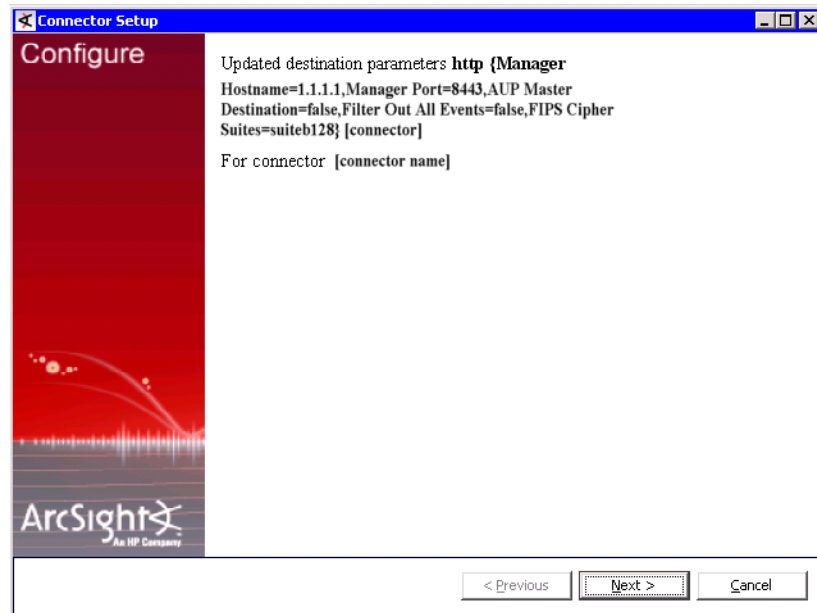
Performing edit destination

- Destination parameters {port=8443, host=1.1.1.1, aupmaster=false, filterevents=false, fipsciphers=suiteb128}

- Connector [Connector name]

< Previous Next > Cancel

- 9 The next window summarizes the configuration changes made. Click **Next** to continue.



- 10 Select **Exit** and click **Next** to exit the configuration wizard.
- 11 Restart the connector.

Using Logger in FIPS Mode

ArcSight Logger supports the Federal Information Processing Standard 140-2 (FIPS 140-2). To use Logger in the FIPS mode, refer to the ArcSight Logger Administrator's Guide and see "Installing or Updating a SmartConnector to be FIPS-compliant" in Chapter 7, "System Admin" for instructions.

