Hewlett Packard
Enterprise

HPE Security ArcSight Forwarding Connector

Software Version: 7.5.0.7986.0

Configuration Guide

March 24, 2017

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise 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. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

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

HPE Security ArcSight products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices.

This document is confidential.

Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise 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.

Copyright Notice

Follow this link to see a complete statement of copyrights and acknowledgements:
https://www.protect724.hpe.com/docs/DOC-13026

Support

Contact Information

Phone	A list of phone numbers is available on the HPE Security ArcSight Technical Support Page: https://softwaresupport.hpe.com/documents/10180/14684/esp-support-contact-list
Support Web Site	https://softwaresupport.hpe.com
Protect 724 Community	https://www.protect724.hpe.com

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
ESM Installation and Configuration Procedures 7
Verifying that ESM is Correctly Installed and Configured 7
Forwarding Correlation Events 7
Forwarding Correlated Events 9
Forwarding Correlated Events On-Demand 9
Automatic Forwarding of Correlated Events 11
Increasing the FileStore Size 12
To Increase the Size of an Existing Filestore 13
Installing the Forwarding Connector 13
Uninstalling a Forwarding Connector 14
Upgrading a Forwarding Connector 15

Chapter 2: Configuration for Forwarding Events 17
Forwarding Events to an ArcSight Manager 17
Forwarding Events to ArcSight Logger 19
Forwarding CEF Syslog Events 20
Forwarding Events to a CSV File 21
Configuring Multiple Destinations 22
Forwarding Events from an ESM High Availability (HA) Cluster 23
Configure the Forwarding Connector in an ESM HA Cluster 23
Create the Startup Script and Move to Shared Location 25

Chapter 3: Configuration for HPE OM and HPE OMi 26
The ArcSight ESM Source Manager 26
Supported Versions of HPE OM and HPE OMi 27
HPE OM and HPE OMi and Correlation Events 27

Installing the Connector 27
Creating an SNMP Interceptor Policy for HPE Operations Manager (HPE OM) 29
Uploading Interceptor Template 29
Deploying the Policy 29
Creating an SNMP Interceptor Policy for HPE Operations Manager i (HPE OMi) 29
Uploading Interceptor Template 30
Troubleshooting Tips 30
Duplicate Events (for HPE OMi) 30
Dropped Events 30
Adjusting the Event Processing Rate for HPE OM and HPE OMi 31

Appendix A: Using the Forwarding Connector with FIPS 32

Send Documentation Feedback 33

Chapter 1: Overview and Installation

This chapter provides information for installing an ArcSight Forwarding Connector for event collection from an ArcSight Manager installation.

See the Support Matrix document available on the Protect 724 site for details on Forwarding Connector supported platforms.

HPE recommends using the Forwarding Connector installer associated with the corresponding ESM or HPE integration release on the HPE SSO download site. 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 version with which this Forwarding Connector is released may not support all Forwarding Connector features. Refer to the ESM release notes for details about what Forwarding Connector features the accompanying ESM supports.

Product Overview

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

The ArcSight Forwarding Connector is capable of forwarding events with IPv4 or IPv6 addresses. If the destination ESM supports both IPv4 and IPv6 addresses, then the address fields like `Attacker`, `Source`, `Target`, and so on will be used. If the destination does not support IPv6 addresses, then the `deviceCustomIPv6Address` fields will be used.

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 such as 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:

- ArcSight Manager (encrypted)
- ArcSight Logger Smart Message (encrypted)
- CEF Syslog
- CSV File

- HPE Operations Manager (IPv4 only)
- HPE Operations Manager i (IPv4 only)

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 17.

Sending Events to ArcSight Logger

ArcSight Logger is a 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 real time monitoring and correlation. Logger now supports the Federal Information Processing Standard 140-2 (FIPS 140-2).

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 19.

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 CEF Syslog events, see "Forwarding CEF Syslog Events" on page 20.

For configuration instructions on forwarding events to a `.csv` file, see "Forwarding Events to a CSV File" on page 21.

For detailed configuration instructions on forwarding events to HPE Operations Manager (HPE OM) and HPE Operations Manager i (HPE OMi), see "Configuration for HPE OM and HPE OMi" on page 26.

ESM Installation and Configuration Procedures

This section describes the standard installation set up for ESM before installing the ArcSight Forwarding Connector.

Verifying that ESM is Correctly Installed and Configured

Before you install the ArcSight Forwarding Connector, make sure that ArcSight Manager and Console have 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 ArcSight Manager, Database, and Console are installed and functioning.
2. Run the ArcSight Manager; to monitor the `server.std.log` file and verify when the Manager has started. 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 Console running when installing the SmartConnector to verify successful installation.

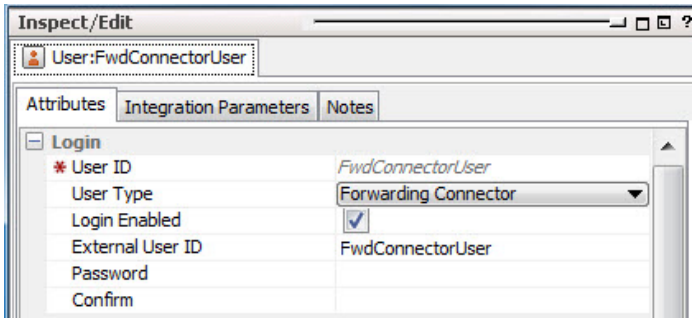
Forwarding Correlation Events

When all rule conditions and thresholds are met, ESM generates a correlation event. A correlation event represents the events that contributed to the rule being triggered and the relevant data contained in them. Before installing the ArcSight Forwarding Connector, create a **Forwarding Connector** account on the source Manager, if you want to forward correlation events to the destination. You can then assign an ArcSight-supplied filter to this account for incoming correlation events.

To create a Forwarding Connector user and assign filter privileges:

1. Log in to the ArcSight Console.
2. On the Navigation panel's Resources tab, choose **Users**.
3. Create a group under an existing user group. In this example, the **FwdConnector** group is created under **Custom User Groups**.
4. Under the group created in **step 3**, create a user. Set the basic required attributes:

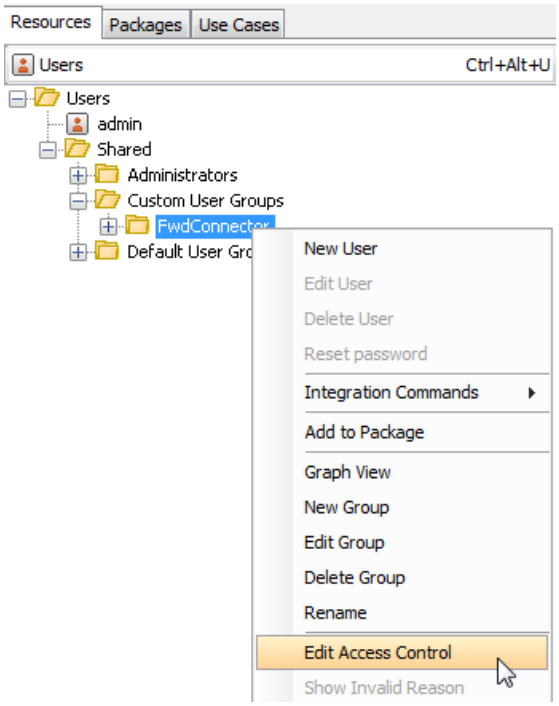
- User ID: Enter a descriptive name. The example uses **FwdConnectorUser**.
- User Type: Forwarding Connector
- Login Enabled: check
- Password: Any alphanumeric string from 6 to 20 characters



Note: Make a note of the Forwarding Connector user. You will be entering the user and password information during Forwarding Connector configuration.

For detailed information on creating users on the ArcSight Console, see "Managing Users and Permissions" in the ArcSight Console User's Guide. By default, user groups have no access to any event filters.

5. On the Resources tab, right-click your custom user group.
6. From the menu, choose **Edit Access Control**.

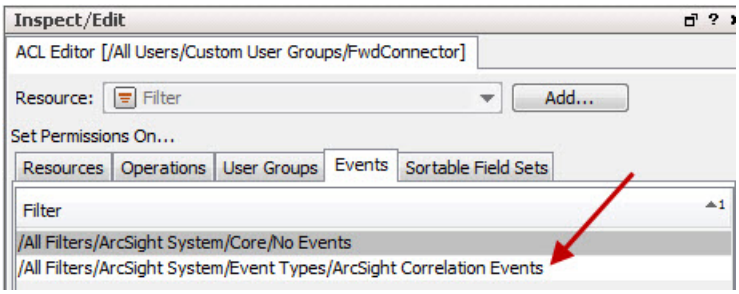


7. On the **Inspect/Edit** window for the ACL Editor:

a. Go to the **Events** tab. The default filter for events is `No Events`.

b. On the **Resource** field, choose **Filter** and click **Add**.

c. On the filter browser, choose `All Filters/ArcSight System/Event Types/ArcSight Correlation Events`. The filter is added and overrides `No Events`, as shown:



On the ArcSight Console's event viewer, correlation events are indicated by a lightning bolt icon.

For detailed information on filters, refer to "Filtering Events" in the ArcSight Console User's Guide.

Forwarding Correlated Events

When a base event matches the condition set in a rule, it becomes a correlated event. There are two methods for forwarding correlated events. You can choose to configure the source Manager to automatically forward all correlation and correlated events, or you can choose to forward correlated events only for specific correlation events as you need them (not automatically, but as you request them). These two methods are mutually exclusive; if you are using one, you cannot also use the other. However, you can try one method and see how it works in your environment, and then elect to use the other method if you think that will serve you better. For example, in an environment where there is a large number of events, you might not want to have all of the related correlated events forwarded, but only want to see specific correlated events. In that case see "Forwarding Correlated Events On-Demand" below. Conversely, you might want the bulk of correlated events automatically forwarded for analysis. In that case see "Automatic Forwarding of Correlated Events" on page 11.

Forwarding Correlated Events On-Demand

In addition to forwarding correlation events, the Forwarding Connector also sends base events that triggered the correlation event. These base events are flagged (annotated) as "correlated."

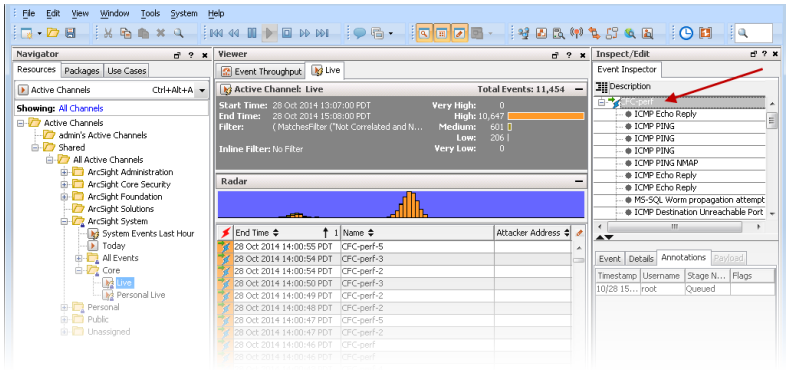
Caution: HPE OM users commonly require only correlated events to be retrieved from ESM.

To show the forwarded correlated events:

Make sure you have completed the instructions in "Forwarding Correlation Events" on page 7.

On the ArcSight Console's event viewer for the destination, correlation events are indicated by a lightning bolt.

1. Right-click on the correlation event in the main viewer and select **Show Event Details**. You can also double-click on the correlation event to see it in the Event Inspector.
2. Double-click on the correlation event in the **Event Inspector** as shown:



Note: You may have to double-click twice on the correlation event in the Event Inspector panel in order to show the correlated events.

Note: Including correlated base events in ESM cases
Once correlated base events are forwarded to the destination, these events can be included in cases.

ESM cases are security-related incidents or tickets that require attention. Suspicious events warrant the creation of a case, which is then assigned to security personnel for tracking and resolution. Rules can automate the creation and updating of cases when certain event conditions are met. These rule actions include the option to include base events in the case. Once this option is selected, the base events are displayed in the case's Events tab.

For details on cases and rules, refer to the topics, "Case Management and Queries" and "Rules Authoring" in the ArcSight Console User's Guide.

Note: An optional setting:

You can view the event annotation flag, `Correlated`, on the base events by setting this flag on the source Manager's `server.properties` file:

```
logger.base-event-annotation.enabled = True
```

Without this setting, the flag is not included for the base event. For instructions on editing the `server.properties` file, see the topic, "Managing and Changing Properties File Settings" in the ESM Administrator's Guide.

Automatic Forwarding of Correlated Events

The Forwarding Connector can 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.

To configure the source Manager:

1. To find the **entityID**, go to `$AGENT_HOME/user/agent/agent.properties` and search for `agents[0].entityid`. For example: `agents[0].entityid=3w+05uiYBABCCLKvzx0stdQ\==`

   Note: For the "==" characters or any other non-alphanumeric character at the end of the userid or agent entityid, use "\" to prefix the character with the backslash escape sequence. For example, if either of these (userid or agent entityid) contain "=", you may prefix it with "\" so it would look like "\=".

   Before translation:

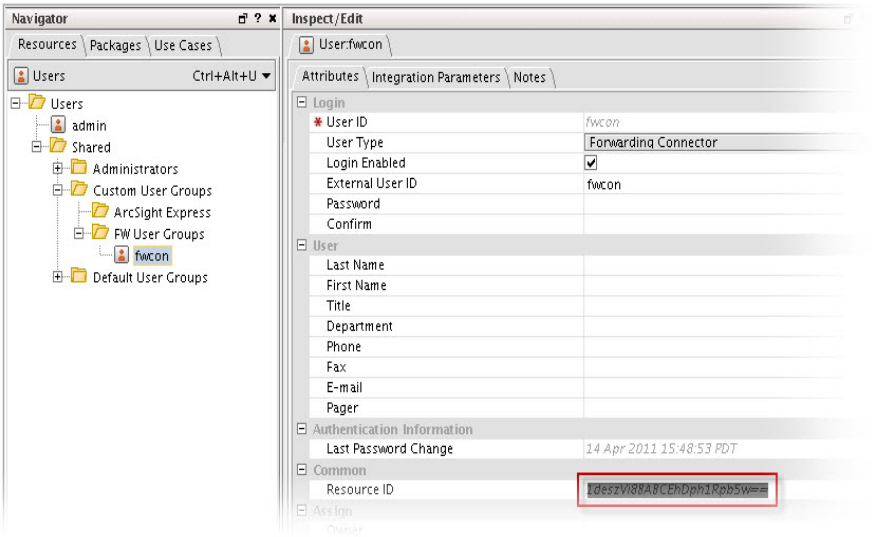
   `eventstream.cfc=Ts9jQkUBABCAAywv9FwewA==.1+0NhKUUBABCAGCfN15kLHA==`

   After translation:

   `eventstream.cfc=Ts9jQkUBABCAAywv9FwewA\=\=.1+0NhKUUBABCAGCfN15kLHA\=\=`

2. To find the **userid**, go to the Console of the **source Manager**.
   a. From to 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`

Note: For instructions on editing the `server.properties` file, see the topic, "Managing and Changing Properties File Settings" in the ESM Administrator's Guide.

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

Increasing the FileStore Size

Installation of the ArcSight Forwarding Connector 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.

The size of new FileStores is configurable:

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:

```
MinutesOfStorage = (((#MB / 1024) * 21,474,833) / 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.

For instructions on editing the `server.properties` file, see the topic, "Managing and Changing Properties File Settings" in the ESM Administrator's Guide.

To Increase the Size of an Existing Filestore

1. Stop the manager.
2. Use the filestore utility to resize the filestore.

   ```
   /opt/arcsight/manager/bin/arcsight filestore -s -fs <new_size_in_bytes> -f
   <path/filestore>
   ```

3. Rename `<filestore> filestore.old`.
4. Rename `filestore.resized filestore`.
5. Start the manager.

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 "Forwarding Correlation Events" on page 7.

To install the Forwarding Connector:

1. Download the installation 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 Shortcut Folder
   - Pre-Installation Summary
   - Installing...

     Your next steps depend upon the destination you will select. Choose from the following options and follow the appropriate link for instructions to complete installation:

   - To forward events to an ArcSight ESM Manager, proceed with "Forwarding Events to an ArcSight Manager" on page 17.

- To forward events to an ArcSight Logger, proceed with "Forwarding Events to ArcSight Logger" on page 19.
- To forward events to a CEF Syslog, proceed with "Forwarding CEF Syslog Events" on page 20.
- To forward events to a .csv file, proceed with "Forwarding Events to a CSV File" on page 21.
- For configuration instructions about forwarding events to HPE Operations Manager or HPE Operations Manager i, see "Configuration for HPE OM and HPE OMi" on page 26.
- For instructions for FIPS-compliant mode with the Forwarding Connector, refer to the SmartConnector User Guide on Protect 724.
- To install the Forwarding Connector in a High Availability (HA) cluster, see "Forwarding Events from an ESM High Availability (HA) Cluster" on page 23.

Uninstalling a Forwarding Connector

Before uninstalling a Forwarding Connector that is running as a service or daemon, first stop the service or daemon. Also, be sure to remove the service files using `$ARCSIGHT_HOME/current/bin/arcsight agentsvc -r` before uninstalling the connector.

Make a note of the entityID. The entityID will be in the agent.properties file. It will be in server.properties file if it was added manually when enabling Forwarding Connector. You will need to search for this in order to clear the cache explained in Clear the Cache After Uninstalling. See "To configure the source Manager:" on page 11 to find the names of the entityID and userID in the server.properties file.

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. 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.

Clear the Cache After Uninstalling

After uninstalling the Forwarding Connector, the cache must be cleared in the source Manager.

1. Go to the server cache folder located in `$ARCSIGHT_HOME/caches/server` for the source Manager.
2. Delete the file that holds the forwarded events for the connector Entity and User. Check that this

file is not in use before deleting it. This file is named based on **<entityID>.<UserID>**. For example, `Ts9jQkUBABCAAywv9FwewA==.1+0NhKUUBABCAGCfN15kLHA==`
This is the file that is mentioned in the Uninstalling steps to make a note.

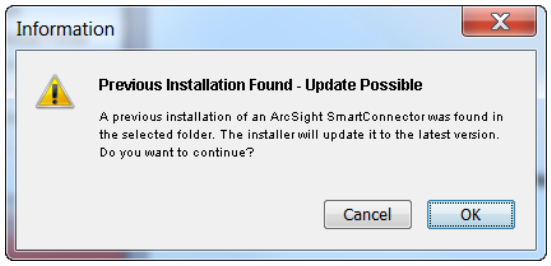
Upgrading a Forwarding Connector

You can upgrade an installed Forwarding Connector to a later version.

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 Forwarding Connector.
2. Run the installation executable for the version of the Forwarding Connector to which you wish to upgrade.
3. During the installation, you are prompted to enter the folder location for the installed connector. Browse to the folder location of the Forwarding Connector you want to upgrade.
4. You will receive this message:



   Click **OK**.
5. Click **Next** to continue the installation.
6. Click **Next** to upgrade your existing SmartConnector configuration and settings.
7. After the successful completion of the upgrade, the SmartConnector Configuration Wizard upgrades the SmartConnector resources in the ArcSight Manager.

   Enter the **User** name and **Password** and click **Next**.
8. Click **Finish**.
9. Select **I do not want to change any setting**. Click **Next**.
10. Select **Exit** and click **Next**.
11. Click **Done** to exit the wizard.

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

To Upgrade the Forwarding Connector when OS is Upgraded

Forwarding Connector is not limited to use the same supported OS versions as the ESM due to not always being installed on the same machine as an ESM. In case the Forwarding Connector that is being upgraded is installed on the same machine as an ESM that will be upgraded, follow this order:

1. Upgrade the OS.
2. Upgrade the ESM source and destination.
3. Upgrade the Forwarding Connector.

Chapter 2: Configuration for Forwarding Events

This chapter provides step-by-step instructions for configuring various Forwarding Connector destinations.

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

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 for forwarding events to a Manager, follow the procedure below.

To continue connector configuration:

1. After you follow the steps in the section "Installing the Forwarding Connector" on page 13, the Add a Connector window is displayed.
2. If you choose to enable FIPS mode or to select a preferred IP address mode (IPv4 or IPv6), select **Set Global Parameters**. (Note that remote management is not available for this connector.) For a list of connectors that support IPv6 addresses, see the *SmartConnectors with IPv6 Mapping Support* document available on Protect 724.
   a. After making your selections, click **Next**.
   b. A summary screen is displayed. Review the summary of your selections and click **Next**.
   c. Click **Continue** to return to the **Add a Connector** window.
3. Select, **Add a Connector** and click **Next**.
4. You are given a choice of Forwarding Connector versions to install. Choose the **ArcSight Forwarding Connector (Enhanced)** option.
5. For instructions about how to determine and change your source disk settings, see "Increasing the FileStore Size" on page 12. Click **Next**.

6. 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.

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.

7. Select **Import the certificate to connector from source**, and click **Next**.
8. Select **ArcSight Manager (encrypted)**, and click **Next**. To view the menu options for destination types, see "The ArcSight ESM Source Manager " on page 5.
9. You are prompted for **Manager Host Name** and **Manager Port**. This is your destination Manager. Enter the information and click **Next**.
10. Enter the connector details as listed in the field description table and click **Next**.

Parameter	Description
Manager Hostname	This is the local host name, IP address, or fully-qualified domain name of the machine where the ArcSight Manager is installed. This name is what all clients (such as ArcSight Console) specify to talk to the Manager. Using a host name and especially a fully-qualified domain name instead of an IP address is recommended for flexibility. The Manager host name is used to generate a self-signed certificate. The Common Name (CN) in the certificate is the Manager host name that you specify in this screen. Although the Manager uses a self-signed certificate by default, you can switch to using a CA signed certificate if needed. See the *ESM Administrator's Guide* for more information.
Manager Port	8443
User	Enter a valid ESM User name.
Password	Enter the password for the ESM user.

Parameter	Description
AUP Master Destination	Default: **false**. A SmartConnector can send events to ESM and Logger simultaneously. In this configuration, it is helpful to use the **AUP Master Destination** feature.
Filter Out All Events	Default: **false**. SmartConnectors can filter and aggregate the events to reduce the volume sent to the ArcSight Manager, ArcSight Logger, or other destinations, which increases ArcSight's efficiency and reduces event processing time.
Enable Demo CA	Default: **false** The ArcSight Manager host name is used to generate a self-signed certificate during ArcSight ESM installation. The Common Name (CN) in the certificate is the Manager host name that you specified during ESM installation. Do not use demo SSL certificates in production. Make sure when switching that you remove the demo CA from **cacerts** on all SmartConnector and ArcSight Consoles.

11. Enter a **Name** for the connector and optionally provide other information identifying the connector's use in your environment in the **Name**, **Device Location**, and **Comment** fields.
12. Select **Import the certificate from destination**, and click **Next**.

    Note: If the ESM destination is reinstalled, the certificate signature changes. You need to manually remove the previous certificate from the trust store to avoid a certificate mismatch error during the configuration.

13. Read the connector summary; if it is correct, click **Next**. If it is not correct, click **Previous** to make changes before continuing.
14. 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.
15. After making your selections, click **Next**. The wizard displays a dialog confirming the connector's setup and service configuration.
16. To complete the installation, choose **Exit** and click **Next**. To enable FIPS-compliant mode, choose **Continue** and click **Next**, and continue with "Using the Forwarding Connector with FIPS " on page 32.

Forwarding Events to 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 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 5 in the procedure "Forwarding Events to an ArcSight Manager" on page 17.
2. Then select **ArcSight Logger SmartMessage (encrypted)** from the destination types and click **Next**. To view the menu options for destination types, see "The ArcSight ESM Source Manager " on page 5.
3. 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.

Parameter	Description
Host Name/IP	The destination host name or IP address.
Port	The destination port 443 for Logger Appliance or 9000 for downloadable Logger.
Receiver Name	The destination receiver name.
Compression Model	The data compression mode checkbox. Select to enable to leave as default for disable.

4. Click **Next** and continue following steps 8 and onward in the procedure "Forwarding Events to an ArcSight Manager" on page 17.

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 5 in the procedure "Forwarding Events to an ArcSight Manager" on page 17.
2. Then select **CEF Syslog** from the destination types. To view the menu options for destination types, see "The ArcSight ESM Source Manager " on page 5.
3. Click **Next**.
4. Enter the **IP/Host** and **Port** information, then choose the appropriate Protocol from the drop-down menu.

   The **CEF Forwarder** mode parameter is **false** by default.

   If the destination is a Syslog Daemon connector and you want to preserve information about the original connector, then the CEF Forwarder mode should be set to true both in this destination and

in the receiving connector. For example, if you have a chain of connectors connected by syslog, syslog NG, or CEF encrypted syslog (UDP), and you want to preserve information about the original connector, the destinations should all have the CEF Forwarder mode set to true (which is implicitly true for CEF Encrypted Syslog (UDP)), and the connectors receiving from them should also have the CEF Forwarder mode set to true.

5. Click **Next** and continue following the steps in the procedure "Forwarding Events to an ArcSight Manager" on page 17.

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 17.
2. Then select **CSV File** from the destination types and click **Next**. To view the menu options for destination types, see "The ArcSight ESM Source Manager " on page 5.
3. Enter values as described in the table.

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.

4. Click **Next** and continue following steps 8 and onward in the procedure "Forwarding Events to an ArcSight Manager" on page 17.

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

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.

1. Select **Modify Connector** and click **Next**.
2. Select **Add, modify, or remove destinations** and click **Next**.
3. Select **Add destination** and click **Next**.
4. Select the destination type and click **Next**. To view the menu options for destination types, see "The ArcSight ESM Source Manager " on page 5.
5. Enter or select in the parameters for the destination being added and click **Next**.

Parameter	Description
Manager Hostname	This is the local host name, IP address, or fully-qualified domain name of the machine where the ArcSight Manager is installed. This name is what all clients (such as ArcSight Console) specify to talk to the Manager. Using a host name and especially a fully-qualified domain name instead of an IP address is recommended for flexibility. The Manager host name is used to generate a self-signed certificate. The Common Name (CN) in the certificate is the Manager host name that you specify in this screen. Although the Manager uses a self-signed certificate by default, you can switch to using a CA signed certificate if needed. See the *ESM Administrator's Guide* for more information.
Manager Port	8443
User	Enter a valid ESM User name.
Password	Enter the password for the ESM user.

Parameter	Description
AUP Master Destination	Default: **false**. A SmartConnector can send events to ESM and Logger simultaneously. In this configuration, it is helpful to use the **AUP Master Destination** feature.
Filter Out All Events	Default: **false**. SmartConnectors can filter and aggregate the events to reduce the volume sent to the ArcSight Manager, ArcSightLogger, or other destinations, which increases ArcSight's efficiency and reduces event processing time.
Enable Demo CA	Default: **false** The ArcSight Manager host name is used to generate a self-signed certificate during ArcSightESM installation. The Common Name (CN) in the certificate is the Manager host name that you specified during ESM installation. Do not use demo SSL certificates in production. Make sure when switching that you remove the demo CA from **cacerts** on all SmartConnector and ArcSight Consoles.

6. To complete the installation, choose **Exit** and click **Next**.
7. To apply your changes, restart the SmartConnector.

Forwarding Events from an ESM High Availability (HA) Cluster

Use the instructions in this section to configure the ArcSight Forwarding Connector in an ESM HA cluster. Installing the ArcSight Forwarding Connector in this manner ensures that it runs on the same host as ESM, even if the HA feature fails over ESM to the other server. This ensures that events continue to be forwarded from ESM HA.

To do this, first set up the Forwarding Connector and then create a Startup script. After the startup script is created, it should be moved to the HA file system resource to be available on both cluster nodes.

This configuration provides the following benefits in Forwarding Connector:

- Fail overs with the ESM service to the active node.
- Auto starts after failover.
- Auto reconnects the connector to the ESM source after a failover.

Configure the Forwarding Connector in an ESM HA Cluster

1. Follow the steps in the "ESM Installation and Configuration Procedures" on page 7 to set up the User Group and User.
2. Follow these tasks only on the **Active Primary Server** to use the ESM HA service.
3. Copy the ArcSight Forwarding Connector binary to the ArcSight users home folder. For example, `/home/arcsight`.

4. Give ownership to the arcsight user and group. For example,

   `chown arcsight:arcsight /home/arcsight/ ArcSight-[releasenumber]-SupperConnector-Linux64.bin`.

5. Set execute permission on the install binary. For example,

   `chmod +x /home/arcsight/ ArcSight-[releasenumber]-SuperConnector-Linux64.bin`

6. Switch to arcsight user:

   `su arcsight`

7. Create a connectors folder within the replicated file system resource:

   `mkdir /opt/arcsight/connectors`

8. As arcsight user run the installer.
9. When prompted for the **Default Install Folder** enter: `/opt/arcsight/connectors/forwarder`
10. When prompted for the **Install Set** , select **1 - Typical**
11. When prompted for a **Link Location** , select **4 – Don't create links**
12. Click **Enter** to confirm your choices and continue.
13. After the file installation has finished, click **Enter** to exit.
14. Run the `runagentsetup` script to setup the connector: `/opt/arcsight/connectors/forwarder/current/bin/runagentsetup`
15. When prompted **What would you like to do?**, select **0 – Add a connector**.
16. When prompted with **Selection Type**, select **0 - ArcSight Forwarding Connector (Enhanced)**.
17. When prompted to confirm choices, click **yes** to confirm.
18. Click **Enter** to accept sensitivity.
19. When prompted for **ArcSight Source Manager Host Name[localhost]:**, click **Enter** for **HA service FQDN**. You will see:

    `cluster.acme.com` (This is the service host name used when configuring ESM and must be resolvable by all ESM clients; for example, connectors, consoles, ArcSight Command Centers.)

20. When prompted for **ArcSight Source Manager Port[8443]:**, click **Enter** for port 8443.
21. When prompted for **ArcSight Source Manager User Name:**, click **Enter** for **FwdConnectorUser**. This is the Forwarding Connector user setup in ESM.
22. When prompted for **ArcSight Source Manager Password:**, click **Enter**. You will see the password for the user in the previous step.
23. When prompted with certificate options, select **0- Import the certificate to connector from source**.
24. Select the destination type for your environment.
25. After the destination is setup, click **Exit** to exit the installation.

Create the Startup Script and Move to Shared Location

These steps must be carried out on the active Primary where the Forwarding Connector is installed.

1. Use `su-` to switch to the Root user.
2. Run the following command:
   `/opt/arcsight/connectors/forwarder/current/bin/arcsight agentsvc -i –uarcsight –sn forwarder`
3. Move the startup script just created in the previous step to the shared file system resource. For example,
   `mv /et/init.d/arc_forwarder /opt/arcsight/connectors`
4. Set the ownership of the script to arcsight user and group. For example,
   `chown arcsight:arcsight /opt/arcsight/connectors/arc_forwarder`

Chapter 3: Configuration for HPE OM and HPE OMi

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

Note: Only IPv4 addresses are supported for the HPE OM and HPE OMi destinations.

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 HPE 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.

HPE Operations Manager (HPE 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.

HPE Operations Manager i (HPE OMi) enables the HPE 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 HPE Business Service Management Operations Manager i Concepts Guide for details on BSM.

HPE 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 HPE Business Service Management (BSM) events directly to BSM Operations Management. See the Using HPE BSM Integration Adapter Guide for details on HPE BSM Integration Adapter.

The ArcSight ESM Source Manager

Before installing the Forwarding Connector, create a Forwarding Connector account on the Manager. For instructions, see "Forwarding Correlation Events" on page 7.

Supported Versions of HPE OM and HPE OMi

Refer to the Forwarding Connector Release Notes for the supported versions of the HPE OM and OMi.

HPE OM and HPE 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, HPE OM and HPE OMi users commonly require only correlated events to be retrieved from ESM. In such cases, HPE OM and HPE 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.

HPE OM and HPE OMi use an SNMP trap policy to allow ArcSight events to be accepted within the HPE OM or HPE OMi environment. For instructions on how to create an SNMP interceptor, see "Creating an SNMP Interceptor Policy for HPE Operations Manager (HPE OM)" on page 29 or "Creating an SNMP Interceptor Policy for HPE Operations Manager i (HPE OMi)" on page 29.

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, HPE recommends that you install the connector and the HPE Operations Agent on the same system.

To install the Forwarding Connector:

1. Download the install executable for your operating system from the HPE 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 Shortcut Folder
   Pre-Installation Summary
   Installing...
3. Follow steps 1 through 5 in the procedure "Forwarding Events to an ArcSight Manager" on page 17.

4. Then select **HPE Operations Manager** or **HPE Operations Manager i.** To view the menu options for destination types, see "The ArcSight ESM Source Manager " on page 5. Click **Next** to continue.
5. Fill in the parameter information required for connector configuration. Click **Next** to continue.

Parameter	Description
Host	For HPE OM, enter the Host name or IP address of the HPE OM device. This is the HPE OM managed node (the system where the HPE Operations Agent is installed, and to which the SNMP interceptor policy is deployed). For HPE OMi, enter the Host name or IP address of the HPE BSM Integration Adapter.
Port	For HPE OM and HPE OMi, enter the port to be used by the device to monitor for events by the HPE 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)	Enter the name that identifies the SNMP v3 user.
Authentication Password(v3)	The type of authentication being used. Select AuthMD5 or AuthSHA. AuthMD5 is the default.
Security Level (v3)	Enter the authentication password.
Authentication Scheme(v3)	The type of privacy being used. Select Priv3DES, PrivAES128, PrivAES192, PrivAES256, or PrivDES. Priv3DES is the default.
Privacy Password(v3)	Enter the privacy password.
Context Engine Id(v3)	Enter an administrative domain. The contextEngineID uniquely identifies an SNMP entity that may realize an instance of a context with a particular contextName.
Context name (v3)	Enter a unique context name. Each contextName must be unique within an SNMP entity.

6. Click **Next** and continue following steps 8 and onward in the procedure "Forwarding Events to an ArcSight Manager" on page 17.

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

An SNMP interceptor policy is a type of HPE 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 HPE OM SNMP interceptor policy that you create.

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

See "Troubleshooting Tips" on the next page 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 HPE OM and HPE 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 HPE OM for Windows or HPE OM for UNIX or Linux Administration UI. For details, refer to the HPE Operations Manager online help and documentation.

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

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

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

HPE BSM Integration Adapter SNMP interceptor policies monitor SNMP events, and respond when a character pattern that you choose is found in an SNMP trap. HPE 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 HPE BSM Integration Adapter's powerful policy edit features.

See "Troubleshooting Tips" below 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 HPE OM and HPE OMi SNMP Interceptor Policy Readme for details on uploading the template.

Troubleshooting Tips

Duplicate Events (for HPE OMi)

If there appear to be duplicate events forwarded to the HPE 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 HPE OMi, Refer to the HPE Business Service Management Using Operations Management Guide and help for details.

   For HPE OM, refer to the HPE 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 HPE OM and HPE OMi

The default event processing rate for forwarding events from ESM to HPE OM is **50 eps**. For HPE OMi, the default processing rate is **10 eps**. If this rate proves excessive for your system, HPE OM or HPE 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 HPE OM or HPE OMi. To do so, 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 HPE OM or HPE OMi destination, similar to the example below:

   `0Ajv5S8BABCAAeabNXP5Rw==.xml`
4. From within the .xml file, search for the following for HPE OM:

   `ProcessingSettings.ThrottleRate="50"`

   or, for HPE 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"`

   Note: 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

For instructions for FIPS-compliant mode with the Forwarding Connector, refer to the appendix for FIPS Compliant SmartConnectors in the *SmartConnector User Guide* on Protect 724.

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 system, click the link above and an email window opens with the following information in the subject line:

Feedback on Configuration Guide (Forwarding Connector 7.5.0.7986.0)

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 arc-doc@hpe.com.

We appreciate your feedback!