
Micro Focus Security ArcSight Forwarding Connector

Software Version: 7.5

Configuration Guide

Document Release Date: May 2021

Software Release Date: May 2021



Legal Notices

Copyright Notice

© Copyright 2001-2021 Micro Focus or one of its affiliates

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

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

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

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

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

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

Support

Contact Information

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

Contents

- Chapter 1: Overview and Installation 5
 - Product Overview 5
 - The ArcSight ESM Source Manager and Destinations 5
 - Sending Events to an ArcSight ESM Destination Manager 6
 - Sending Events to ArcSight Logger 6
 - Sending Events to Transformation Hub 6
 - Sending Events to a Non-ESM Location 7
 - ESM Installation and Configuration Procedures 7
 - Verifying that ESM is Correctly Installed and Configured 7
 - Forwarding Correlation Events 7
 - Forwarding Correlated Events 10
 - Forwarding Correlated Events On-Demand 10
 - Automatic Forwarding of Correlated Events 11
 - Increasing the FileStore Size 13
 - Installing the Forwarding Connector 14
 - Uninstalling a Forwarding Connector 15
 - Upgrading a Forwarding Connector 16

- Chapter 2: Configuration for Forwarding Events 18
 - Forwarding Events to an ArcSight Manager 18
 - Forwarding Events to ArcSight Logger 21
 - Forwarding CEF Syslog Events 21
 - Forwarding Events to a CSV File 22
 - Forwarding Events to Transformation Hub 23
 - Configuring Multiple Destinations 27
 - Forwarding Events from an ESM High Availability (HA) Cluster 28
 - Configure the Forwarding Connector in an ESM HA Cluster 28
 - Create the Startup Script and Move to Shared Location 30

- Appendix A: Using the Forwarding Connector with FIPS 31

- Send Documentation Feedback 32

About this PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format. Because this content was originally created to be viewed as online help in a web browser, some topics may not be formatted properly. Some interactive topics may not be present in this PDF version. Those topics can be successfully printed from within the online help.

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 *ESM Technical Requirements* on the [ESM documentation page](#) for details on Forwarding Connector supported platforms.

Use the Forwarding Connector installer associated with the corresponding ESM or Micro Focus integration release on the 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.

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, Transformation Hub, 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 and Destinations

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
- Transformation Hub

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 18](#).

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 21](#).

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 Transformation Hub

The Transformation Hub destination is used to send events (in CEF, binary, or Avro format) to a topic in the Transformation Hub cluster, which can then further distribute events to real-time analysis and data warehousing systems. Any application that supports retrieving data from Transformation Hub can receive these events (for example, ESM, Recon, Hadoop, and Logger).

For information on configuring a Forwarding Connector to forward events to Transformation Hub, see ["Forwarding Events to Transformation Hub" on page 23](#).

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 21](#).

For configuration instructions on forwarding events to a .csv file, see ["Forwarding Events to a CSV File" on page 22](#).

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.

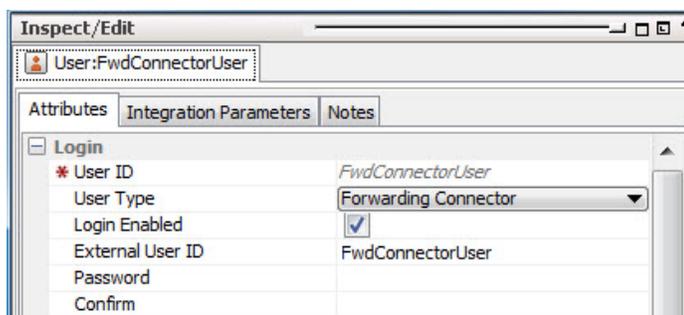
Forwarding Correlation Events

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

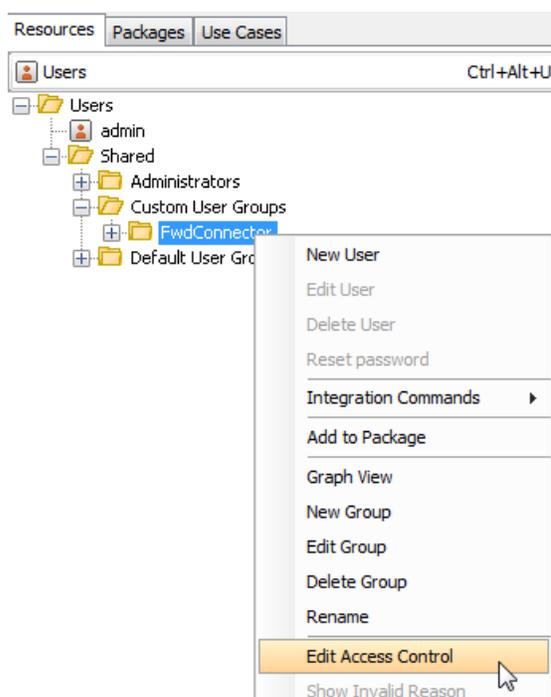


Note: Make a note of the Forwarding Connector user. You will be entering the user and password information during Forwarding Connector configuration.

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.

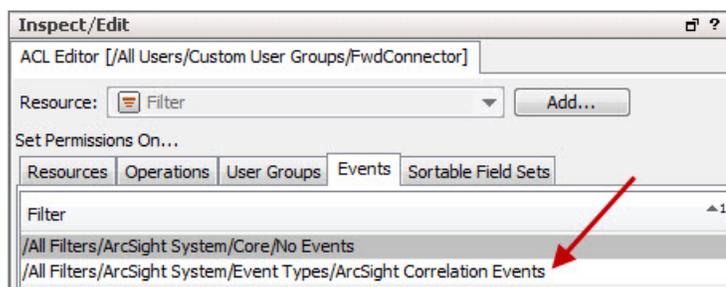
5. On the Resources tab, right-click your custom user group.

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 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](#). Conversely, you might want the bulk of correlated events automatically forwarded for analysis. In that case, see [Automatic Forwarding of Correlated Events](#).

Forwarding Correlated Events On-Demand

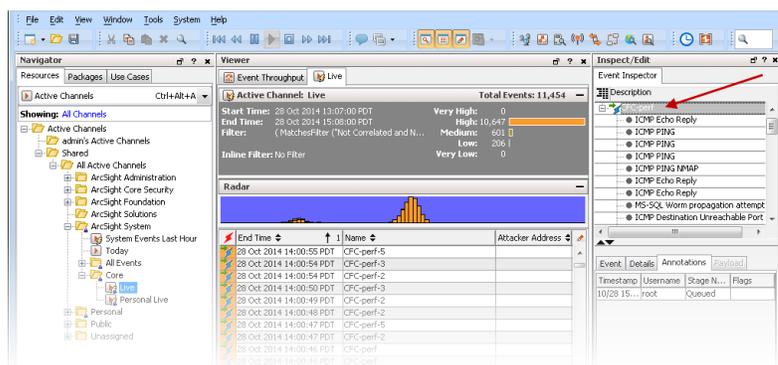
In addition to forwarding correlation events, the Forwarding Connector also sends base events that triggered the correlation event. These base events are flagged (annotated) as “correlated.”

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. 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 “\=”.

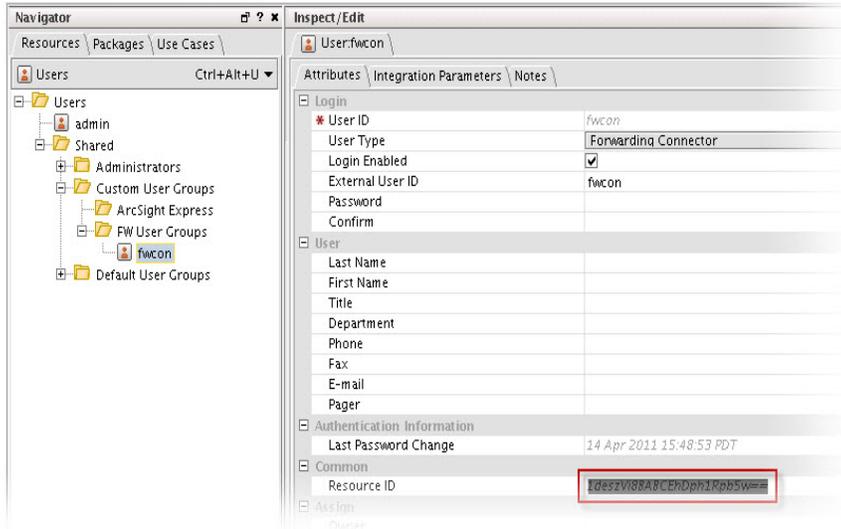
Before translation:

```
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:

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

- 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.

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 18](#).
 - To forward events to an ArcSight Logger, proceed with ["Forwarding Events to ArcSight Logger" on page 21](#).
 - To forward events to a CEF Syslog, proceed with ["Forwarding CEF Syslog Events" on page 21](#).
 - To forward events to a .csv file, proceed with ["Forwarding Events to a CSV File" on page 22](#).
 - To forward events Transformation Hub, proceed with ["Forwarding Events to Transformation Hub" on page 23](#).
 - For instructions for FIPS-compliant mode with the Forwarding Connector, refer to the *SmartConnector User Guide*.
 - To install the Forwarding Connector in a High Availability (HA) cluster, see ["Forwarding Events from an ESM High Availability \(HA\) Cluster" on page 28](#).

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 12](#) 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,
`Ts9jQkUBABCAAyww9FwewA==.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. This topic covers three scenarios:

- Upgrading the Forwarding Connector in a High Availability ESM environment as the source of events
- Upgrading the Forwarding Connector installed in the same server as ESM (locally installed)
- Upgrading the Forwarding Connector when the OS is upgraded

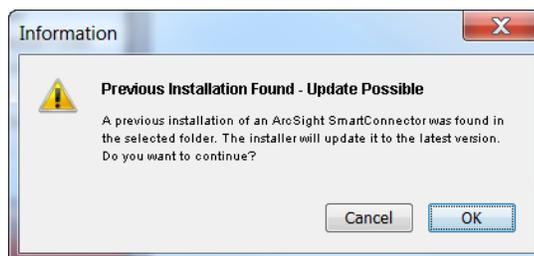
To upgrade the Forwarding Connector in High Availability ESM:

1. Make sure the HA ESM source is already upgraded to the proper ESM version.
2. Log in to the ESM source as **root**.
3. Enter this command:

```
mv /opt/arcsight/connectors/arc_superagent_ng /etc/init.d/
```
4. Follow the steps in the next procedure, [To locally upgrade the Forwarding Connector:](#).
5. Follow the steps in "[Create the Startup Script and Move to Shared Location](#)" on page 30.

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 14](#), 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 [Micro Focus Community](#).
 - 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 13](#). 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 and Destinations" 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 | <p>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.</p> <p>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 <i>ESM Administrator's Guide</i> for more information.</p> |
| Manager Port | 8443 |

| Parameter | Description |
|-------------------------------|---|
| User | Enter a valid ESM User name. |
| Password | Enter the password for the ESM user. |
| 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 31.

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 7](#) 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 18](#).
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 and Destinations" 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 18](#).

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 7](#) 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 18](#).
2. Then select **CEF Syslog** from the destination types. To view the menu options for destination types, see ["The ArcSight ESM Source Manager and Destinations" 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 18](#).

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 7](#) 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 18](#).

- 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 and Destinations" on page 5](#).
- 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. |

- Click **Next** and continue following steps 8 and onward in the procedure ["Forwarding Events to an ArcSight Manager" on page 18](#).

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 Transformation Hub

You can configure the ArcSight Forwarding Connector to send event to Transformation Hub. This destination sends events to a Transformation Hub topic in CEF, binary, or Avro format. After events are in Transformation Hub, other applications can retrieve them.



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 7](#) for information on certificate validation.

For the content format **Avro**, the SmartConnector uses Avro schema to emit the Avro output. Avro schema resides in the Schema Registry of Transformation Hub. The SmartConnector makes an HTTPS call to Transformation Hub to get the schema. The SmartConnector captures the Schema Registry details during the installation and fetches schema during its every restart.



Note : SmartConnector 8.1.0 supports Transformation Hub 3.4. Ensure that you use Transformation Hub 3.4 to install the SmartConnector for emitting Avro output.



Note: During the SmartConnector upgrade, ensure that you install or upgrade to Transformation Hub 3.4 that hosts the schema of the desired version in its Schema Registry.

To forward events to Transformation Hub:

1. Follow steps 1 through 4 in the procedure ["Forwarding Events to an ArcSight Manager" on page 18](#).
2. Then select **Transformation Hub** from the destination types and click **Next**. To view the menu options for destination types, see ["The ArcSight ESM Source Manager and Destinations" on page 5](#).
3. Enter values as described in the following table:

| Parameters | Description |
|--------------------------------------|---|
| Kafka Broker Host (s):Port(s) | <p>This is a mandatory field.</p> <p>You must specify at least one server. If there are multiple servers, then specify a comma-separated list of hostnames and ports to establish a communication with the Transformation Hub cluster. While it is not necessary to list all servers in the cluster, listed, if none of the servers listed can be contacted, the connector cannot send events to Transformation Hub. For example: kafka1.example.com:9093,kafka2.example.com:9093.</p> |
| Kafka Broker on SSL/TLS | <p>Determines whether events are sent with TLS encryption. Select one of the following options:</p> <ul style="list-style-type: none">• false - (Default)• true - Select true to access the Kafka broker on SSL/TLS. <p>If you select true, you must provide the SSL/TLS Truststore Password and the location of the SSL/TLS Truststore File Path.</p> <p>When Kafka Broker on SSL/TLS is set to true, a secure connection will be established with the Kafka broker(s) specified in the Kafka Broker Host(s):Port (s) field.</p> |

| Parameters | Description | | | | | | | | | | |
|-------------------------------|---|----------------|-------------|------|---|----------------|---|-------------------------|---|------------|---|
| Receive Acknowledgment | <p>Select a value to determine if and how the connector waits for acknowledgment from Transformation Hub that it has received the event. Select one of the following options:</p> <ul style="list-style-type: none"> None: (Default) The connector does not wait for acknowledgment. This can result in lost events if the receiving Kafka server fails. However, selecting this option provides a significantly higher throughput. Leader: The connector waits for acknowledgment from the primary Transformation Hub server for the event's partition. This option protects against data loss in most circumstances while providing reasonable performance. However, selecting this option can affect the throughput. All: The connector waits for an acknowledgment from all Transformation Hub servers that contain a backup for the event's partition. This protects against lost events in nearly all circumstances, but significantly reduces throughput. | | | | | | | | | | |
| Content Format | <p>Select any of the following topics for the corresponding content format:</p> <table border="1"> <thead> <tr> <th>Content Format</th> <th>Kafka Topic</th> </tr> </thead> <tbody> <tr> <td>Avro</td> <td> th-arcsight-avro Supports ArcSight 2020.3 or later. Supports Avro events to be sent to Transformation Hub. Note: ArcSight 2020.3 refers to the third release of ArcSight in the year 2020. </td> </tr> <tr> <td>CEF (for IPv4)</td> <td> th-cef Supports IPv4. Use with Logger 6.3.0 or earlier versions. </td> </tr> <tr> <td>CEF (for IPv4 and IPv6)</td> <td> th-cef Supports IPv4 and IPv6. Use with Logger 6.4.0 or later versions. In addition to IPv6 support, this option adds support for long values for Bytes In/Out fields. </td> </tr> <tr> <td>ESM Binary</td> <td> th-binary_esm Supports all versions of ESM. For more information, see the <i>ESM Technical Requirements</i> on the ESM documentation page page. </td> </tr> </tbody> </table> <p>Note: The default Content Format is CEF (for IPv4 and IPv6) and Kafka Topic is th-cef.</p> | Content Format | Kafka Topic | Avro | th-arcsight-avro Supports ArcSight 2020.3 or later. Supports Avro events to be sent to Transformation Hub. Note: ArcSight 2020.3 refers to the third release of ArcSight in the year 2020. | CEF (for IPv4) | th-cef Supports IPv4. Use with Logger 6.3.0 or earlier versions. | CEF (for IPv4 and IPv6) | th-cef Supports IPv4 and IPv6. Use with Logger 6.4.0 or later versions. In addition to IPv6 support, this option adds support for long values for Bytes In/Out fields. | ESM Binary | th-binary_esm Supports all versions of ESM. For more information, see the <i>ESM Technical Requirements</i> on the ESM documentation page page. |
| Content Format | | Kafka Topic | | | | | | | | | |
| Avro | th-arcsight-avro Supports ArcSight 2020.3 or later. Supports Avro events to be sent to Transformation Hub. Note: ArcSight 2020.3 refers to the third release of ArcSight in the year 2020. | | | | | | | | | | |
| CEF (for IPv4) | th-cef Supports IPv4. Use with Logger 6.3.0 or earlier versions. | | | | | | | | | | |
| CEF (for IPv4 and IPv6) | th-cef Supports IPv4 and IPv6. Use with Logger 6.4.0 or later versions. In addition to IPv6 support, this option adds support for long values for Bytes In/Out fields. | | | | | | | | | | |
| ESM Binary | th-binary_esm Supports all versions of ESM. For more information, see the <i>ESM Technical Requirements</i> on the ESM documentation page page. | | | | | | | | | | |
| Kafka Topic | | | | | | | | | | | |

| Parameters | Description |
|--|---|
| Compression Type | <p>Compression reduces disk space and network bandwidth requirements.</p> <p>Select the compression algorithm used (gzip, zstd, none) when Transformation Hub copies events, such as when routing events between Topics.</p> <ul style="list-style-type: none"> • gzip - (Default) Note: The zstd algorithm performs better than gzip, but requires Kafka client library version 2.1.0 or later. • Zstd - only is supported in Transformation Hub 3.3 and SmartConnector 8.0.0. If your Transformation Hub version is 3.2, use gzip as a compression type. This compression type works only for Logger 7.0, ESM 7.2, IDI 1.1, or their later versions. |
| ESM Version for ESM Topic | <p>Select the ESM version number of the desired ESM topic. The default ESM Version for ESM Topic is 7.2.x and above.</p> <p>This field is mandatory when the Content Format is selected as ESM Binary.</p> |
| Schema Registry Host:Port | <p>Specify host:port of the Schema Registry node to fetch schema using HTTPS.</p> <p>This field is mandatory when the Content Format is selected as Avro.</p> |
| SSL/TLS Truststore File Path | <p>Specify the location of the SSL/TLS truststore file. This is required to access HTTPS Schema Registry for Avro or the TLS-based secure communication for the Kafka brokers.</p> <p>It is optional for Text-based communication with Kafka brokers.</p> <p>This field is mandatory when the Content Format is selected as Avro or when Kafka Broker on SSL/TLS is set to true.</p> |
| SSL/TLS Truststore Password | <p>Specify the password for the SSL/TLS truststore file.</p> <p>This field is mandatory when the SSL/TLS Truststore File Path is specified.</p> |
| Use SSL/TLS Client Authentication | <p>Determines whether a client certificate is used for TLS to identify the connector. Select one of the following options:</p> <ul style="list-style-type: none"> • false - (Default) • true - Select true if client authentication is enabled for Kafka broker, Schema Registry, or both. <p>If you select true, ensure that the Kafka Broker on SSL/TLS is enabled. You must also provide values for the SSL/TLS Keystore File Path, SSL/TLS Keystore Password, and SSL/TLS Key Password parameters.</p> |
| SSL/TLS Keystore File Path | <p>Specify the location of the SSL/TLS keystore file path for client authentication.</p> |

4. Click **Next** and continue following steps 8 and onward in the procedure ["Forwarding Events to an ArcSight Manager"](#) on page 18.

For more information about SmartConnectors and Transformation Hub as a destination, refer to the section titled "Connector Destinations" > "Transformation Hub" 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 and Destinations" 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 <i>ESM Administrator's Guide</i> 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-[releasenumbe]-
SupperConnector-Linux64.bin.`
5. Set execute permission on the install binary. For example,
`chmod +x /home/arcsight/ ArcSight-[releasenumbe]-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 a **Link Location** , select **4 – Don't create links**
11. Click **Enter** to confirm your choices and continue.
12. After the file installation has finished, click **Enter** to exit.
13. Run the runagentsetup script to setup the connector:
`/opt/arcsight/connectors/forwarder/current/bin/runagentsetup`
14. When prompted **What would you like to do?**, select **0 – Add a connector**.
15. When prompted with **Selection Type**, select **0 - ArcSight Forwarding Connector (Enhanced)**.
16. When prompted to confirm choices, click **yes** to confirm.
17. Click **Enter** to accept sensitivity.
18. 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.)
19. When prompted for **ArcSight Source Manager Port[8443]:**, click **Enter** for port 8443.
20. When prompted for **ArcSight Source Manager User Name:**, click **Enter** for **FwdConnectorUser**. This is the Forwarding Connector user setup in ESM.
21. When prompted for **ArcSight Source Manager Password:**, click **Enter**. You will see the password for the user in the previous step.

22. When prompted with certificate options, select **0- Import the certificate to connector from source**.
23. Select the destination type for your environment.
24. 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 /etc/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
```

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* .

Send Documentation Feedback

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

Feedback on Configuration Guide (Forwarding Connector 7.5)

Just add your feedback to the email and click send.

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

We appreciate your feedback!