

SmartConnector™ Configuration Guide for

ArcSight™ Forwarding Connector

December, 2010



SmartConnector™ Configuration Guide for ArcSight™ Forwarding Connector

Copyright © 2001-2010 ArcSight, Inc. All rights reserved.

ArcSight, the ArcSight logo, ArcSight TRM, ArcSight NCM, ArcSight Enterprise Security Alliance, ArcSight Enterprise Security Alliance logo, ArcSight Interactive Discovery, ArcSight Pattern Discovery, ArcSight Logger, FlexConnector, SmartConnector, SmartStorage and CounterACT are trademarks of ArcSight, Inc. All other brands, products and company names used herein may be trademarks of their respective owners.

Follow this link to see a complete statement of ArcSight's copyrights, trademarks, and acknowledgements:
<http://www.arcsight.com/company/copyright/>

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

This document is ArcSight Confidential.

Revision History

Date	Product Version
12/2010	Added supported versions for McAfee ePO (4.0 and 4.5), removed build number from the guide, and fixed reported document bugs.
05/26/2010	Updated information on upgrades and forwarding base events.
01/18/2010	Merged FIPS and non-FIPS information.
12/29/2009	Updated screen shots to reflect the current UI.
11/03/2009	Updated to include an enhanced McAfee ePO feature. The new "EPO Version" parameter allows users of newer versions of ePO to drill down and perform actions to the source or target from the ePO console.
3/26/2009	Updates published concurrently with ESM v.4.5 SP1 Release.
02/23/2009	Added fixes and EPO destination. Forwarding Connector build 5242.
08/28/2008	Added updates for "Enhanced" Forwarding Connector. Added new destination options.
09/12/2007	Added information about using the Forwarding Connector to send events to ArcSight Logger.
03/28/2007	Updated connector name and installer name.
01/31/2007	General content update.
09/21/2004	Added Manager version note.
01/20/2003	First release of connector documentation.

Document template version: 1.0.5

ArcSight Customer Support

Phone	1-866-535-3285 (North America) +44 (0)870 141 7487 (EMEA)
E-mail	support@arcsight.com
Support Web Site	http://www.arcsight.com/supportportal/
Protect 724 Community	https://protect724.arcsight.com

Contents

Configuration Guide for ArcSight Forwarding Connector	1
Product Overview	1
What's New	1
The ArcSight ESM Source Manager	2
Forwarding Connector Destination Options	2
Sending Events to an ArcSight ESM Destination Manager	2
Sending Events to a Non-ESM Location	2
Sending Events to ArcSight Logger	3
Standard Installation Procedures	4
Installing ArcSight ESM	4
Assigning Privileges on the ESM Source Manager	4
Forwarding Correlation Events	6
Configuring to Pull Correlated Events	6
Configuring to Allow Forwarding of Correlated Events	6
Increasing the FileStore size (Enhanced version only)	7
Installing the Forwarding Connector	8
Destination Configuration	9
Forwarding Events to an ArcSight ESM Manager	9
Forwarding Events to ArcSight Logger	13
Forwarding Events to NSP Device Poll Listener	14
Forwarding CEF Syslog Events	15
Forwarding Events to a CSV File	16
Forwarding Events to McAfee ePolicy Orchestrator	18
Installing the Microsoft SQL Server 2005 Driver for JDBC	19
ArcSight Event to McAfee CEF Mappings	20
Uninstalling a Connector	21
Upgrading a Connector	21
Rolling Back a Connector	22
Using the Forwarding Connector in FIPS mode	22
What is FIPS?	22
ArcSight ESM Installation	22
FIPS-Enabled Forwarding Connector Installation	23
Enable FIPS Suite B Support	28
Using Logger in FIPS Mode	28

Configuration Guide for ArcSight Forwarding Connector

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

["Product Overview" on page 1](#)
["What's New" on page 1](#)
["The ArcSight ESM Source Manager" on page 2](#)
["Forwarding Connector Destination Options" on page 2](#)
["Standard Installation Procedures" on page 4](#)
["Destination Configuration" on page 9](#)
["Uninstalling a Connector" on page 21](#)
["Upgrading a Connector" on page 21](#)
["Rolling Back a Connector" on page 22](#)
["Using the Forwarding Connector in FIPS mode" on page 22](#)

The ArcSight Forwarding Connector is supported on Windows, Linux, Solaris, and AIX platforms.

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

Product Overview

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

What's New

- The ArcSight Forwarding Connector now provides **FIPS 140-2** and **FIPS Suite B** support. For the details of using the FIPS complaint Forwarding Connector, see ["Using the Forwarding Connector in FIPS mode" on page 22](#).
- One Forwarding Connector per Manager can be configured to automatically forward all *correlated events* (the set of events that triggered a rule) along with the *correlation events* (the events that represent the triggered rules). In previous releases, the only way to forward correlated events to another Manager was to initiate an on-demand

pull of those events manually from the destination Manager. For the details of this feature, see ["Configuring to Allow Forwarding of Correlated Events" on page 6](#).

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 ESM Manager, a non-ESM location or a Logger appliance.



The ESM Source Manager must be of the same version as the ESM Destination Manager.

Forwarding Connector Destination Options

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

- An ArcSight ESM destination Manager
- ArcSight Logger
- NSP Device Poll Listener
- CEF Syslog
- A CSV file
- McAfee ePolicy Orchestrator v4.0 or v4.5.

Sending Events to an ArcSight ESM Destination Manager

The ArcSight Forwarding Connector logs into the source ESM Manager and then forwards events to a destination ESM Manager. For detailed configuration instructions, see ["Forwarding Events to an ArcSight ESM Manager" on page 9](#).



The ESM Destination Manager must be of the same version as the ESM Source Manager.

Sending Events to a Non-ESM Location

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

When configuring the Forwarding Connector to send events to a non-ESM destination, you might encounter a problem with certificate validation during connector setup. Make sure that the demo CA is added to the client trust store to validate the ESM Manager's demo certificate.

To make sure the demo CA is added to the client trust store:

- 1** Install the connector as usual, but stop at the screen that prompts you to select a destination type.

- 2 After the screen prompting you to select the destination type is displayed, run the following command from the `$ARCSIGHT_HOME\current\bin` directory

```
arcsight connector tempca -ac
```

- 3 Return to the wizard and complete the installation.

For detailed configuration instructions on forwarding events to NSP, proceed with ["Forwarding Events to NSP Device Poll Listener" on page 14](#).

For detailed configuration instructions on forwarding CEF Syslog events, proceed with ["Forwarding CEF Syslog Events" on page 15](#).

For detailed configuration instructions on forwarding events to a `.csv` file, proceed with ["Forwarding Events to a CSV File" on page 16](#).

For detailed configuration instructions on forwarding events to McAfee ePolicy Orchestrator (ePO), proceed with ["Forwarding Events to McAfee ePolicy Orchestrator" on page 18](#).



Use of ePO requires installation of **MS SQL Server 2005 for JDBC driver**. For instructions on downloading, see ["Installing the Microsoft SQL Server 2005 Driver for JDBC" on page 19](#).

Sending Events to ArcSight Logger

ArcSight Logger is a hardware storage solution optimized for extremely high event throughput. A typical use for Logger is to collect firewall data and then forward a subset of that data to an ArcSight ESM Manager for realtime monitoring and correlation. ArcSight Logger now supports the Federal Information Processing Standard 140-2 (FIPS 140-2). See ["Using Logger in FIPS Mode" on page 28](#) for details.

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

Before configuring the Forwarding Connector that sends events to the Receiver, you need to 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 13](#).

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 an ESM Manager
- Sending Events from ArcSight ESM to Logger
- Using Logger in FIPS mode

Standard Installation Procedures

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

Installing ArcSight ESM

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

To ensure a successful ArcSight ESM installation:

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

Before you install the SmartConnector, make sure you have the following available:

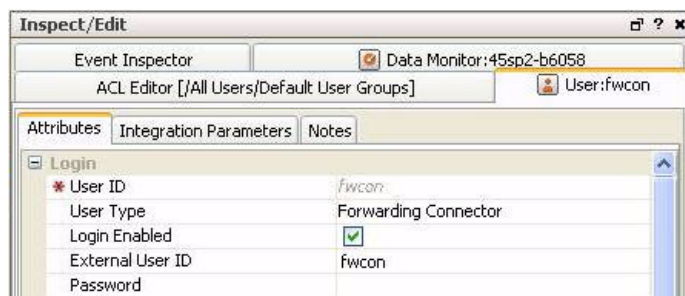
- Local access to the machine where the SmartConnector is to be installed
- Administrator passwords

Assigning Privileges on the ESM Source Manager

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

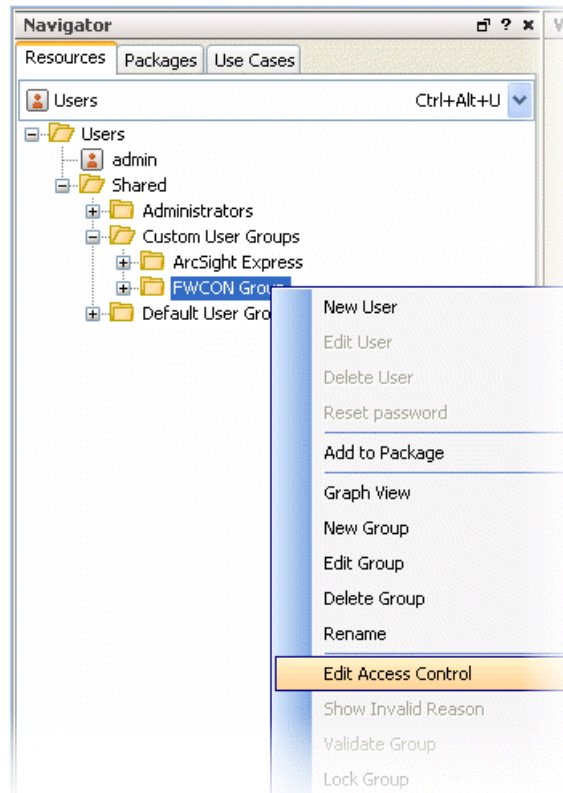
To assign privileges in the ESM Manager:

- 1 Run the ArcSight Console on the ArcSight ESM *Source* Manager.
- 2 From the Navigator **Resources** tab, choose **Users** from the drop-down menu.
- 3 Create a user group under the **Custom User Group**.
- 4 Under the group created in step 1, create a user account of user type **Forwarding Connector**, as shown below.

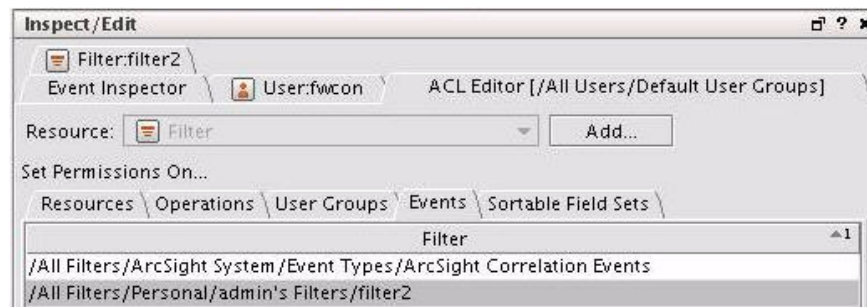


- 5 Returning to the Navigator **Resources** tab, right-click your chosen user group.

- 6 From the resulting menu, choose **Edit Access Control**.



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



For detailed instructions on assigning filters and other Arcsight Console functions, refer to the *ArcSight ESM 5.0 Administrator's Guide*.

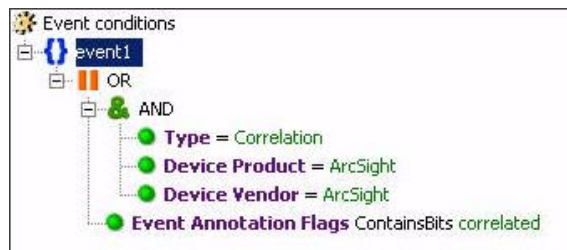
Forwarding Correlation Events

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

Configuring to Pull Correlated Events

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

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



Note

Correlated events pulled on-demand are for viewing only. They are not persisted in the destination Manager.

Configuring to Allow Forwarding of Correlated Events

The Forwarding Connector can also be configured to automatically pull and 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.

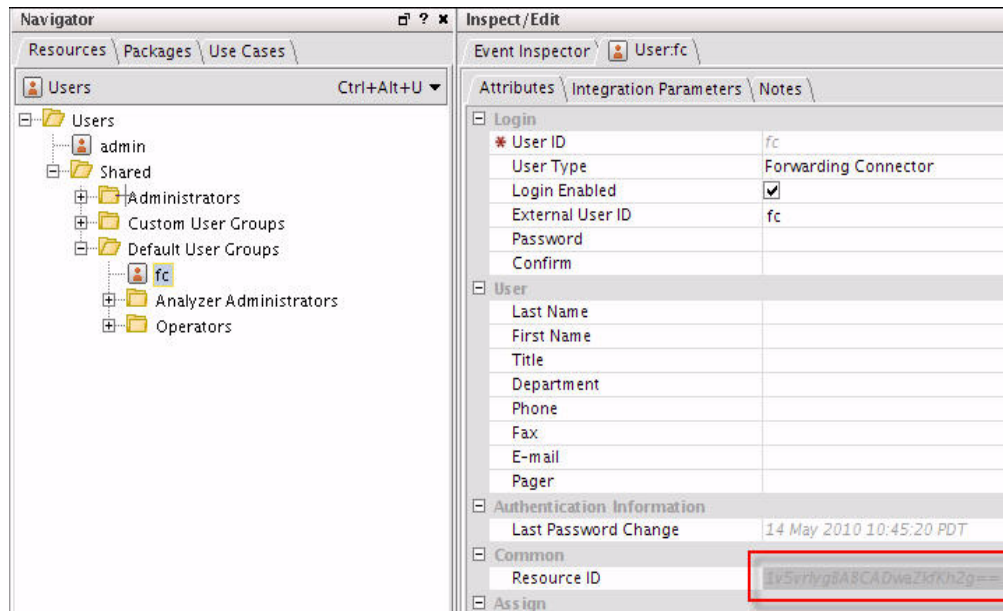
The source Manager keeps track of the events that have been previously forwarded by using the "Forwarded" annotation, disallowing duplicates.

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 **use id**. To begin the configuration, you must locate these two elements and combine them within the `server.properties` file.

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

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

- 2 To find the **userid**, go to the Console of the **source Manager**.
 - a From to the **Navigator** panel, choose the **Resource** tab.
 - b Under **Resources**, 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.



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

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

- 3 Restart the source Manager.

Increasing the FileStore size (Enhanced version only)

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

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

To increase the size of the FileStore:

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

The file displays the current default:

```
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.

Installing the Forwarding Connector

Before installing the ArcSight Forwarding Connector, you need to assign privileges on your ESM Manager. For instructions on how to do this, see ["Assigning Privileges on the ESM Source Manager"](#) on page 4.



Note

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

To install an ArcSight Forwarding Connector:

- 1 Download the ArcSight executable for your operating system from the ArcSight Customer Support Site according to the instructions provided in the connector release notes.
- 2 Start the installer by running the executable for your operating system, then follow the folder selection tasks and installation of the core SmartConnector software:
 - ◆ Introduction
 - ◆ Choose Install Folder
 - ◆ Choose Install Set
 - ◆ Choose Shortcut Folder
 - ◆ Pre-Installation Summary
 - ◆ Installing...

When installation of the connector core component is complete, the following dialog is displayed:



- 3 Choose your ArcSight Forwarding Connector destination.
 - ◆ To forward events to an **ArcSight ESM Manager**, proceed with ["Forwarding Events to an ArcSight ESM Manager"](#) on page 9.

- ◆ To forward events to an **ArcSight Logger**, proceed with ["Forwarding Events to ArcSight Logger" on page 13.](#)
- ◆ To forward events to an **NSP appliance**, proceed with ["Forwarding Events to NSP Device Poll Listener" on page 14.](#)
- ◆ To forward events to a **CEF Syslog**, proceed with ["Forwarding CEF Syslog Events" on page 15.](#)
- ◆ To forward events to a **.csv file**, proceed with ["Forwarding Events to a CSV File" on page 16.](#)
- ◆ To forward events to **McAfee ePolicy Orchestrator (ePO)**, proceed with ["Forwarding Events to McAfee ePolicy Orchestrator" on page 18.](#)



Use of ePO requires installation of **MS SQL Server 2005 for JDBC driver**. For instructions on downloading, see ["Installing the Microsoft SQL Server 2005 Driver for JDBC" on page 19.](#)

Destination Configuration

The following provides step-by-step instructions for configuring Forwarding Connector destinations.

Forwarding Events to an ArcSight ESM Manager

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

To continue connector configuration:

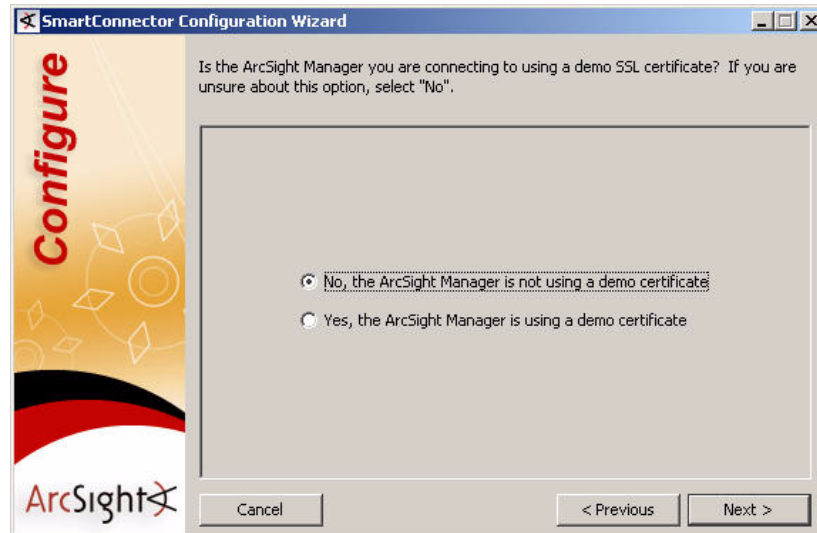
- 1** Select **ArcSight Manager (encrypted)**, and click **Next**.



2 The Wizard first prompts you for Manager certificate information.

- ◆ The default is **No, the ArcSight Manager is not using a demo certificate.**
- ◆ Choose **Yes** if ArcSight Manager is using a demo certificate.

Before selecting this option, make sure the Manager is, in fact, using a demo SSL certificate. If you are unsure, select **No** or consult your system administrator.



If your ArcSight Manager is using a self-signed or CA-signed SSL certificate, select **No, the ArcSight Manager is not using a demo certificate** and click **Next**.



Note

After completing the SmartConnector installation wizard, remember to configure the connector for the type of SSL certificate your Manager is using manually. Refer to the *ArcSight ESM 5.0 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.

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



The screenshot shows the 'SmartConnector Configuration Wizard' window. On the left is a vertical banner with the word 'Configure' in red and the ArcSight logo at the bottom. The main area has a light gray background with the text 'Please complete the following ArcSight Manager information.' Below this are four fields: 'Manager Host Name' with 'localhost' entered, 'Manager Port' with '8443' entered, 'AUP Master Destination' with a dropdown set to 'false', and 'Filter Out All Events' with a dropdown set to 'false'. At the bottom are three buttons: 'Cancel', '< Previous', and 'Next >'.

- 4 Enter a valid ArcSight **User Name** and **Password** and click **Next**.

This is the user name and password for the user account you created on the destination ESM Manager.

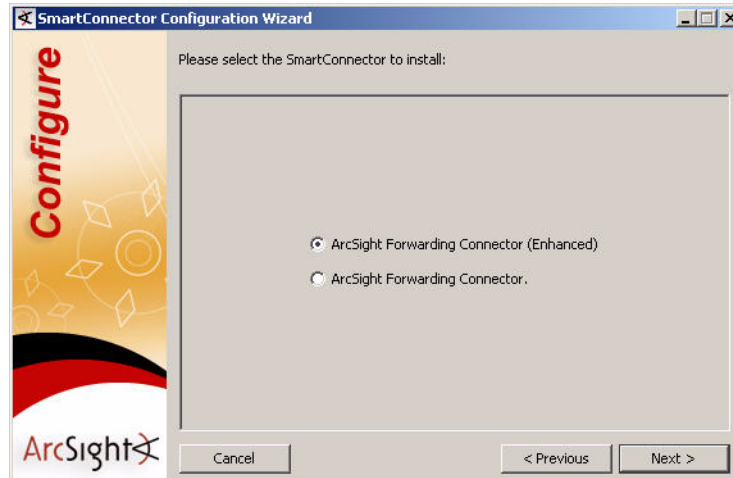


The screenshot shows the 'SmartConnector Configuration Wizard' window. On the left is a vertical banner with the word 'Configure' in red and the ArcSight logo at the bottom. The main area has a light gray background with the text 'In order to configure SmartConnectors, you must login as a user with the appropriate privileges.' Below this are two fields: 'User Name' with 'admin' entered and 'Password' with '*****' entered. At the bottom are three buttons: 'Cancel', '< Previous', and 'Next >'.

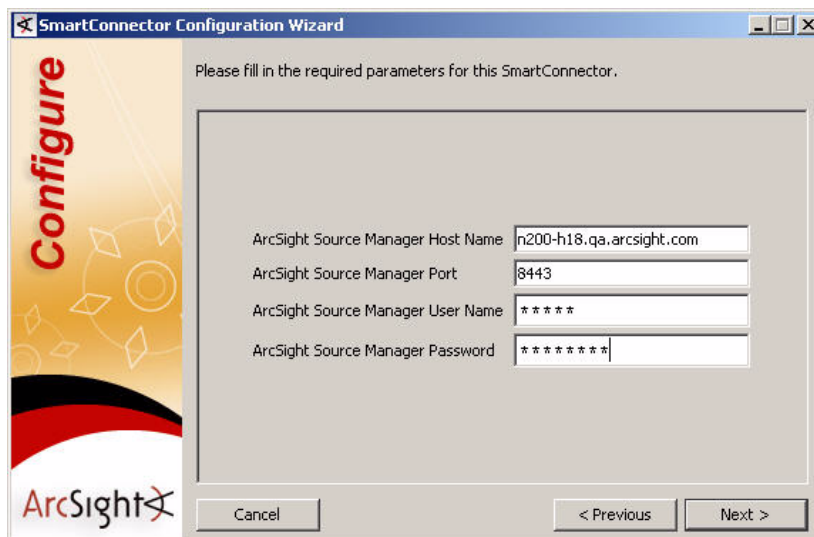
- 5 You are given a choice of Forwarding Connector versions to install. If you are currently using ESM **v4.0 SP3** or later, ArcSight recommends choosing the **ArcSight Forwarding Connector (Enhanced)** option. When choosing which version to use, note the following:
- ◆ The **ArcSight Forwarding Connector** option supports the previous software version and does not include the increased event rate and recoverability features of **ArcSight Forwarding Connector (Enhanced)**. ArcSight recommends using the older option only when communicating with a pre-v4.0 SP3 ESM installation.
 - ◆ Neither Forwarding Connector release is **FIPS compliant**. If you require FIPS compliance, retain your current Forwarding Connector version.

- ◆ The capacity of events that can be stored during a system failure is dependent on the FileStore size of your source ESM Manager. Choosing the **ArcSight Forwarding Connector (Enhanced)** version *requires configuration adjustments on your source ESM Manager.*

For instructions on how to determine and change your source disk settings, see [“Increasing the FileStore size \(Enhanced version only\)” on page 7](#). Click **Next**.



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



Parameter	Description
ArcSight Source Manager Hostname	Hostname where the ArcSight ESM Source Manager is installed.
ArcSight Source Manager Port	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.

Parameter	Description
ArcSight Source Manager Password	ArcSight's password that will be used to log this Connector into the ArcSight ESM Source Manager.

- 7 Enter a name for the connector and provide other information identifying the connector's use in your environment. Click **Next**.
- 8 Read the connector summary; if it is correct, click **Next**. If the summary is not correct, click **Previous** to make changes before continuing.
- 9 When the connector completes its configuration, click **Next**. The wizard now prompts you to choose whether you want 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.
- 10 After making your selections, click **Next**. The wizard displays a dialog confirming the connector's setup and service configuration.
- 11 Click **Finish**.
- 12 Click **Done**.

Forwarding Events to ArcSight Logger

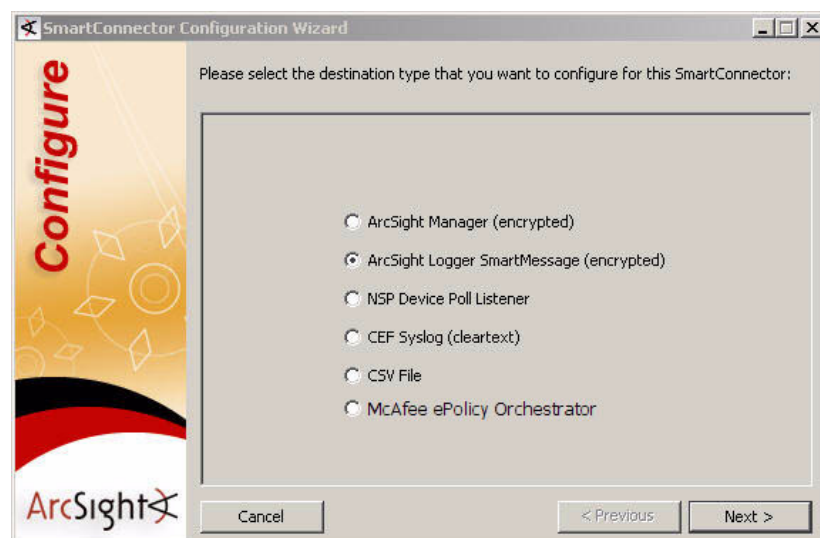


When configuring the Forwarding Connector to send events to a non-ESM destination, you might encounter problems with certificate validation during connector setup. See ["Sending Events to a Non-ESM Location" on page 2](#) for information on certificate validation.

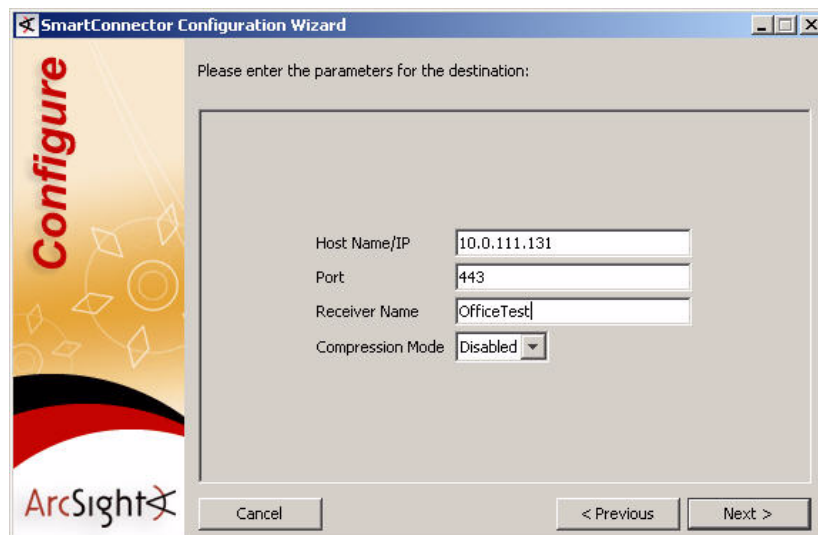
Before you continue connector configuration for forwarding events to an ArcSight Logger, ensure that a SmartMessage Receiver has been set up on ArcSight Logger for the Forwarding Connector (Refer to the *ArcSight Logger Administrator's Guide* for details).

To continue connector configuration:

- 1 Select **ArcSight Logger SmartMessage (encrypted)** from the following dialog:



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



The screenshot shows the 'SmartConnector Configuration Wizard' window. On the left is a vertical banner with the word 'Configure' in red and the ArcSight logo at the bottom. The main area has the text 'Please enter the parameters for the destination:'. Below this are four input fields: 'Host Name/IP' with the value '10.0.111.131', 'Port' with the value '443', 'Receiver Name' with the value 'OfficeTest', and 'Compression Mode' with a dropdown menu set to 'Disabled'. At the bottom are three buttons: 'Cancel', '< Previous', and 'Next >'.

- 3 Click **Next** and continue following the steps to complete your configuration. Refer to the Parameters Table on page 12 for parameter descriptions. When a message confirms that configuration was successful, click **Finish** to exit the wizard.

Forwarding Events to NSP Device Poll Listener



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 2](#) for information on certificate validation.

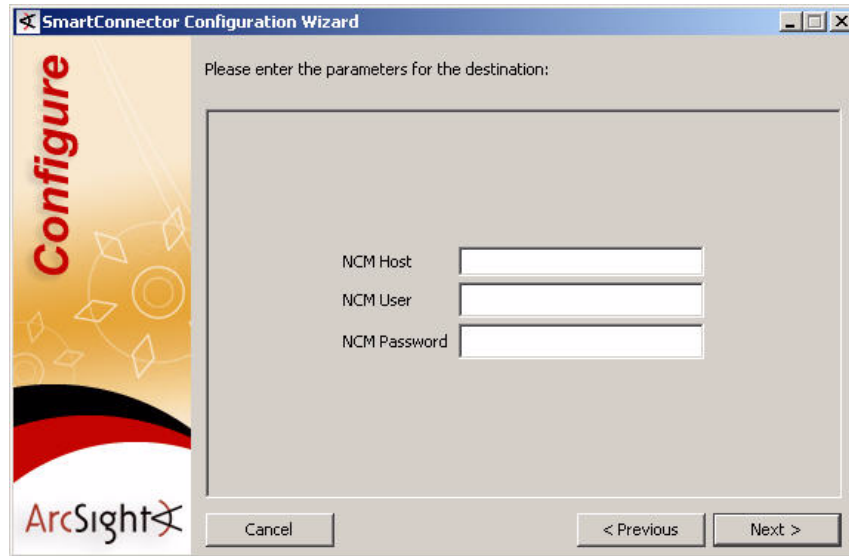
To continue connector configuration for forwarding events to NSP:

- 1 Select **NSP Device Poll Listener** from the selections and click **Next**.



The screenshot shows the 'SmartConnector Configuration Wizard' window. On the left is a vertical banner with the word 'Configure' in red and the ArcSight logo at the bottom. The main area has the text 'Please select the destination type that you want to configure for this SmartConnector:'. Below this are six radio button options: 'ArcSight Manager (encrypted)', 'ArcSight Logger SmartMessage (encrypted)', 'NSP Device Poll Listener' (which is selected), 'CEF Syslog (cleartext)', 'CSV File', and 'McAfee ePolicy Orchestrator'. At the bottom are three buttons: 'Cancel', '< Previous', and 'Next >'.

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

The image shows a 'SmartConnector Configuration Wizard' window. On the left is a vertical banner with the word 'Configure' in red and the ArcSight logo at the bottom. The main area has the text 'Please enter the parameters for the destination:' followed by three input fields labeled 'NCM Host', 'NCM User', and 'NCM Password'. At the bottom are three buttons: 'Cancel', '< Previous', and 'Next >'.

SmartConnector Configuration Wizard

Please enter the parameters for the destination:

NCM Host

NCM User

NCM Password

Cancel < Previous Next >

- 3 Click **Next** and continue following the steps to complete your configuration until a message confirms that it was successful. Click **Finish** to exit the wizard.

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

Forwarding CEF Syslog Events

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



When configuring the Forwarding Connector to send events to a non-ESM destination, you might encounter problems with certificate validation during connector setup. See ["Sending Events to a Non-ESM Location" on page 2](#) for information on certificate validation.

To configure the connector to send CEF Syslog events:

- 1 Select **CEF Syslog (cleartext)** from the following window:



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



- 3 Click **Next** and continue following the Configuration Wizard to complete your configuration until a message confirms that it was successful. Click **Finish** to exit the wizard.

Forwarding Events to a CSV File

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



Caution

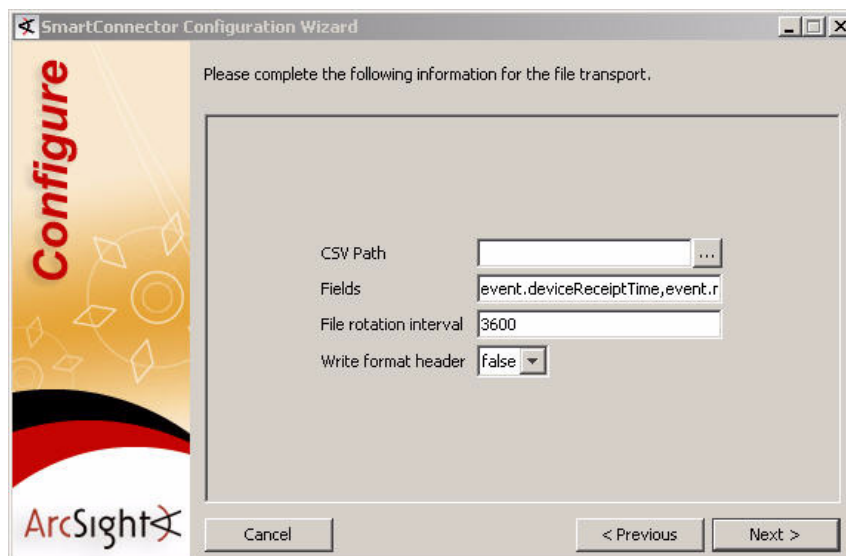
When configuring the Forwarding Connector to send events to a non-ESM destination, you might encounter problems with certificate validation during connector setup. See ["Sending Events to a Non-ESM Location" on page 2](#) for information on certificate validation.

To forward events to a **.CSV** file:

- 1 Select **CSV File** and click **Next**.



- 2 For these options, enter values as described in the table below.



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

- 3 Click **Next** and continue following the steps to complete your configuration until a message confirms that it was successful. Click **Finish** to exit the wizard.

For more information about capturing events and `.csv` files, refer to the section titled "Capturing Events from SmartConnectors (ESM v4.0)" in the *SmartConnector User's Guide*.

Forwarding Events to McAfee ePolicy Orchestrator

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

McAfee ePO v4.0 and v4.5 are supported currently.



Use of ePO requires installation of **MS SQL Server 2005 for JDBC driver**. For instructions on downloading, see ["Installing the Microsoft SQL Server 2005 Driver for JDBC" on page 19](#).

To forward events to McAfee ePO:

- 1 On the destination selection window displayed, select **McAfee ePolicy Orchestrator** and click **Next**.



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

- 2 Enter values for the ePO database connectivity on the window displayed:

SmartConnector Configuration Wizard

Please complete the following information for the epodb transport.

EPO DB Host	10.10.10.10
EPO DB Port	1433
EPO DB Name	ePO_DEMO
EPO DB User Name	*****
EPO DB Password	*****
EPO Version	At least 4.0 Patch 5 or 4.5 Patch 1 Older than 4.0 Patch 5 or 4.5 Patch 1 At least 4.0 Patch 5 or 4.5 Patch 1

Buttons: Cancel, < Previous, Next >



Tip

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

- 3 Click **Next** to complete your configuration and verify that it is successful. Click **Finish** to exit the wizard.



Caution

Rolling back the connector to **build 5116** or earlier disallows use of the McAfee ePolicy Orchestrator destination.

Installing the Microsoft SQL Server 2005 Driver for JDBC

To download and install a JDBC driver:

- 1 Download the **MS SQL Server 2005 JDBC Driver 1.2** from Microsoft at:
<http://www.microsoft.com/downloads/details.aspx?FamilyId=C47053EB-3B64-4794-950D-81E1EC91C1BA&displaylang=en>
- 2 Install the driver.
- 3 Copy the `sqljdbc.jar` jar file from the folder `C:\Program Files\Microsoft SQL Server 2005 JDBC Driver\sqljdbc_1.2\enu` to `$ARCSIGHT_HOME/current/user/agent/lib`, where `$ARCSIGHT_HOME` refers to the connector install folder, such as `c:\ArcSight\SmartConnectors`.
- 4 From `$ARCSIGHT_HOME/current/bin`, double-click `runagentsetup` to return to the SmartConnector Configuration Wizard.

ArcSight Event to McAfee CEF Mappings

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



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

The following table describes how the fields are mapped:

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

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

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

Uninstalling a Connector

Before uninstalling a connector that is running as a service or daemon, first stop the service or daemon. To uninstall on Windows, open the **Start** menu. Run the **Uninstall SmartConnectors** program located under **All Programs, ArcSight SmartConnectors**. If Connectors are not installed on the **Start** menu, locate the \$ARCSIGHT_HOME\UninstallerData folder and run:

```
Uninstall ArcSightAgents.exe
```

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

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

Upgrading a Connector

To locally upgrade the Forwarding Connector:

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

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

`$ARCSIGHT_HOME\current`



During upgrade, the "Default User Groups" user group is updated and adds the `/All Filters/ArcSight System/Core/No Events` filter to the events ACL. If the Forwarding Connector user is in that group, the connector cannot send events to the destination Manager. To prevent this problem, edit the access control for the Forwarding Connector's parent user group and select a filter that gives permission to the subset of events for which the user has access.

Alternatively, if the user has access to all the events, delete the `/All Filters/ArcSight System/Core/No Events` filter.



The ArcSight Forwarding Connectors must be of the same version as the source ESM.

Rolling Back a Connector

To roll back a connector:

- 1 Stop the upgraded connector, which is under `current`.
- 2 Rename the current folder to a name based upon the build version of the upgraded connector.
- 3 Rename the old connector build folder to `current`.
- 4 Start the connector.



Rolling back the connector to **build 5116** or earlier disallows use of the McAfee ePolicy Orchestrator destination.

Using the Forwarding Connector in FIPS mode

What is FIPS?

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

ArcSight ESM Installation

Before you install an ArcSight Forwarding Connector, make sure that ArcSight ESM has already been installed correctly for FIPS compliance. See "[Standard Installation Procedures](#)" on [page 4](#) for instructions. Also, ArcSight recommends reading the *ArcSight ESM Installation and Configuration Guide* before attempting to install a new Forwarding Connector.

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

FIPS-Enabled Forwarding Connector Installation

After completion of ArcSight ESM installation (which includes assigning privileges on the ESM source manager, allowing the forwarding of correlation events, and so on), follow the instructions under ["Installing the Forwarding Connector" on page 8](#) up to and including step 2.

When the installation is complete after step 2, the following dialog is displayed:



- 1 Click **Cancel** to exit connector setup in order to perform configuration of the NSS DB, a necessary step for installing the connector in FIPS-compliant mode. (You will return to the wizard after performing these configuration steps.)
- 2 Create a properties file using the following location:
`$ARCSIGHT_HOME/user/agent/agent.properties`
- 3 Add the following line within the file: `fips.enabled=true`
- 4 Copy your key files for source and destination Managers (in this example, `srcmgrkey.cert` and `destmgrkey.cert`) into the `$ARCSIGHT_HOME\current\bin` directory.
- 5 Turn off FIPS enablement on the new installation using the following command:
`arcsight runmodutil -fips false -dbdir user/agent/nssdb.client`
- 6 Import the certificates for the source and destination Managers. To do this, see the detailed instructions below:

Where `srcmgrkey` and `destmgrkey` are alias names and `srcmgrkey.cert` and `destmgrkey.cert` are the names with which the certificates from the Managers were saved, import the certificates for the source and destination Managers, using the following commands:

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

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



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

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

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

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



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

- 7** Re-enable FIPS using the following command: `arcsight runmodutil -fips true -dbdir user/agent/nssdb.client`
- 8** Return to connector setup by entering the following command from the `$ARCSIGHT_HOME\current\bin` directory:
`arcsight connectorsetup`
- 9** When prompted to start in Wizard Mode, click **Yes**.

- 10 The Destination selection window is again displayed. Make sure **ArcSight Manager (encrypted)** is selected and click **Next**.



- 11 You are prompted for **Manager Host Name** and **Manager Port**.



The **host name** and **manager's certificate name** must match and be DNS resolvable. If these fields do not match, the connection will be unsuccessful.

This is your destination ESM Manager. Enter the information and click **Next**.



- 12** Enter a valid ArcSight **User Name** and **Password**, and click **Next**. This should be the user name and password for the user account you created on the destination ESM Manager.



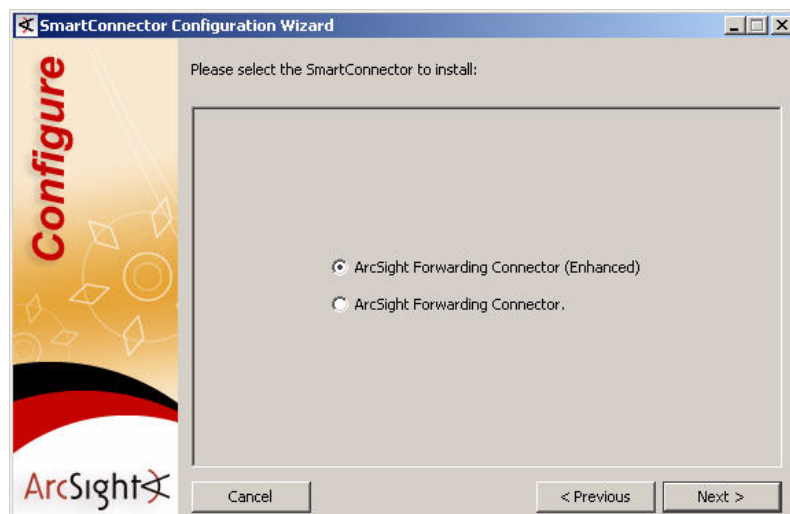
The screenshot shows the 'SmartConnector Configuration Wizard' window. On the left is a vertical banner with the word 'Configure' in red and the ArcSight logo at the bottom. The main area contains the text: 'In order to configure SmartConnectors, you must login as a user with the appropriate privileges.' Below this are two input fields: 'User Name' with 'admin' entered, and 'Password' with '*****' entered. At the bottom are three buttons: 'Cancel', '< Previous', and 'Next >'.

- 13** You are given a choice of Forwarding Connector versions to install. If you are currently using ESM **v4.0 SP3** or later, ArcSight recommends choosing the **ArcSight Forwarding Connector (Enhanced)** option.

When choosing which version to use, note the following:

- ◆ The **ArcSight Forwarding Connector** option supports the previous software version and does not include the increased event rate and recoverability features of **ArcSight Forwarding Connector (Enhanced)**. ArcSight recommends using the older option only when communicating with a pre-v4.0 SP3 ESM installation.
- ◆ The capacity of events that can be stored during a system failure is dependent on the FileStore size of your source ESM Manager. Choosing the **ArcSight Forwarding Connector (Enhanced)** version *requires configuration adjustments on your source ESM Manager*.

For instructions on how to determine and change your source disk settings, see ["Increasing the FileStore size \(Enhanced version only\)" on page 7](#). Click **Next**.



The screenshot shows the 'SmartConnector Configuration Wizard' window at the selection step. The left banner is the same as in the previous image. The main area contains the text: 'Please select the SmartConnector to install:'. Below this are two radio button options: 'ArcSight Forwarding Connector (Enhanced)' (which is selected) and 'ArcSight Forwarding Connector.'. At the bottom are three buttons: 'Cancel', '< Previous', and 'Next >'.

14 Enter the information to configure the Forwarding Connector.

The **host name** and **manager certificate name** must match and be DNS resolvable. If these fields do not match, the connection will be unsuccessful.

This is information about your source ESM Manager, as described in the table below.

Click **Next** to continue.

Parameter	Description
ArcSight Source Manager Hostname	Hostname where the ArcSight ESM Source Manager is installed.
ArcSight Source Manager Port	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.
ArcSight Source Manager Password	ArcSight's password that will be used to log this Connector into the ArcSight ESM Source Manager.

- 15** Enter a name for the connector and provide other information identifying the connector's use in your environment. Click **Next**.
- 16** Read the connector summary; if it is correct, click **Next**. If the summary is not correct, click **Previous** to make changes before continuing.
- 17** When the connector completes its configuration, click **Next**. The wizard now prompts you to choose whether you want 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.
- 18** After making your selections, click **Next**. The wizard displays a dialog confirming the connector's setup and service configuration.
- 19** Click **Finish**.

Enable FIPS Suite B Support

If you have installed a SmartConnector in FIPS-compliant mode, you can enable FIPS Suite B support by modifying the ESM destination parameters.



The ESM Manager must also be installed in FIPS Suite B mode.

To enable FIPS Suite B support:

- 1 From `$ARCSIGHT_HOME\current\user\agent`, open `agent.properties` to edit.
- 2 Locate the following property for ESM destination parameters (approximately, line 10 in the file):

```
agents[0].destination[0].params=<?xml version=\"1.0\"
encoding=\"UTF-8\"?>\n<ParameterValues>\n    <Parameter
Name=\"port\" Value=\"8443\"/>\n    <Parameter
Name=\"filterevents\" Value=\"false\"/>\n    <Parameter
Name=\"host\" Value=\"samplehost.sv.arcsight.com\"/>\n
<Parameter Name=\"aupmaster\" Value=\"false\"/>\n    <Parameter
Name=\"fipsciphers\"
Value=\"fipsDefault\"/>\n</ParameterValues>\n
```
- 3 The destination parameters are specified here as an XML string where each element is one parameter. Based upon the Suite B mode of the ESM Manager, change `fipsDefault` to `suiteb128` (for 128-bit security) or `suiteb192` (for 192-bit security).
- 4 Save and exit `agent.properties`.

Using Logger in FIPS Mode

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