

# **SmartConnector™ Configuration Guide for**

---

ArcSight™ Forwarding Connector

December 1, 2008



## SmartConnector™ Configuration Guide for ArcSight™ Forwarding Connector

Copyright © 2003 – 2008 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/copyrightnotice/>

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	Description
12/01/2008	Updated for ArcSight Express.
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.

Template version: 1.0.1

### ArcSight Customer Support

<b>Phone</b>	1-866-535-3285 (North America) +44 (0)870 141 7487 (EMEA)
<b>E-mail</b>	<a href="mailto:support@arcsight.com">support@arcsight.com</a>
<b>Support Web Site</b>	<a href="https://support.arcsight.com">https://support.arcsight.com</a>
<b>Customer Forum</b>	<a href="https://forum.arcsight.com">https://forum.arcsight.com</a>

# Contents

---

<b>Configuration Guide for ArcSight Forwarding Connector .....</b>	<b>1</b>
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 .....	2
Standard Installation Procedures .....	3
Installing ArcSight ESM .....	3
Assigning Privileges on the ESM Source Manager .....	3
Configuring to Allow Forwarding of Correlation Events .....	5
Increasing the FileStore size (Enhanced version only) .....	5
Installing the Forwarding Connector .....	5
Destination Configuration .....	7
Forwarding Events to an ArcSight ESM Manager .....	7
Forwarding Events to ArcSight Logger .....	10
Forwarding events to NSP Device Poll Listener .....	11
Forwarding CEF Syslog Events .....	13
Forwarding events to a CSV File .....	14
Uninstalling a Connector .....	15
Upgrading a Connector .....	15

---

# 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 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 base Forwarding Connector for ESM v4.5 is **ArcSight-4.6.6.5173.0-SuperConnector**.



The Forwarding Connector version number need not match those of the other ESM components.

---



This Arcsight Forwarding Connector release is **not FIPS compliant**. If you require FIPS compliance, please retain your current Forwarding Connector version.

---

## 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 (Enhanced) offers these updates:

- Supports higher event forwarding rates ranging towards thousands of events per second.
- Improved recoverability. In the event of a system failure, events are fully recoverable and accessed via a source Manager cache.



The capacity of events that can be stored during a system failure is dependent on the FileStore size of the source ESM Manager. For instructions on how to determine and change your source disk settings on an ArcSight ESM Manager, see ["Increasing the FileStore size \(Enhanced version only\)" on page 5](#).

---

## 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.

## Forwarding Connector Destination Options

With data originating from an ArcSight ESM Source Manager, the ArcSight Forwarding Connector provides three destination options for forwarding events. These options include

- an ArcSight ESM destination Manager
- a non-ESM location
- an ArcSight Logger

## 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 7](#).

## 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 may encounter a problem with certificate validation during connector setup. To make sure that the demo CA is added to the client trust store to validate the ESM Manager's demo certificate, do the following:

- 1** Install the connector as usual, but stop at the screen that asks you to select a destination type.
- 2** Once the screen asking 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 11](#).

For detailed configuration instructions on forwarding CEF Syslog events, proceed with [“Forwarding CEF Syslog Events” on page 13](#).

For detailed configuration instructions on forwarding events to a .csv file, proceed with [“Forwarding events to a CSV File” on page 14](#).

## 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.

**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, receiving events from the many devices supported by ArcSight SmartConnectors, 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**. Once this Receiver is created, you can configure the SmartConnector to send events to Logger.

For detailed configuration instructions on configuring a Forwarding Connector to forward events to Logger, see ["Forwarding Events to ArcSight Logger" on page 10](#).

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

## Standard Installation Procedures

### Installing ArcSight ESM

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

For a successful installation of ArcSight ESM:

- 1 Ensure 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 installing the SmartConnector, be sure the following are available:

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

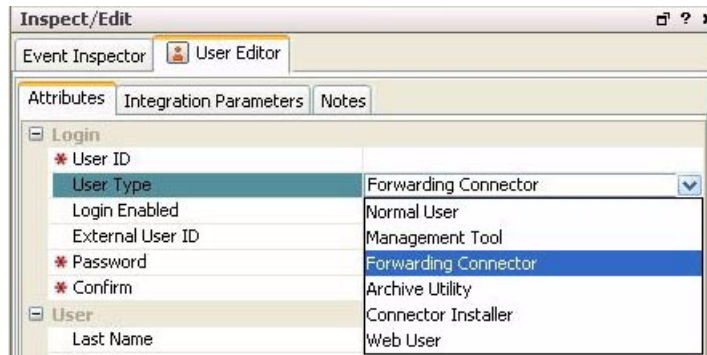
### Assigning Privileges on the ESM Source Manager

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.

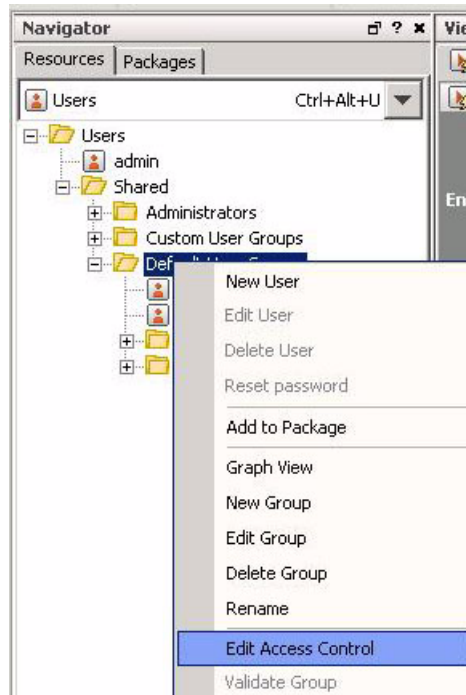
To assign privileges in the ESM Manager, do the following:

- 1 Run the ArcSight Console on the ArcSight ESM *Source* Manager.
- 2 From the Navigator **Resources** tab, choose a user group.

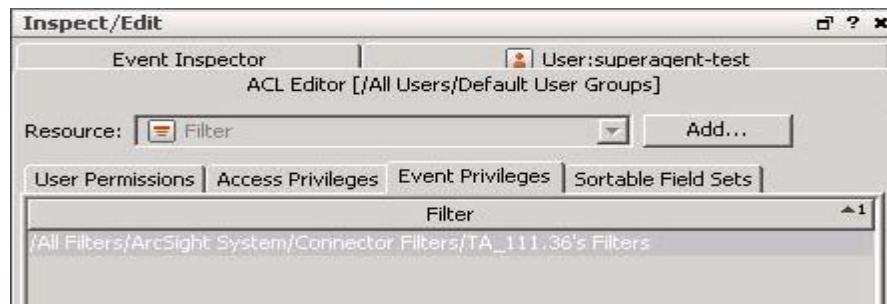
- 3 Create a user account of user type **Forwarding Connector**.



- 4 From the Navigator **Resources** tab, right-click your chosen user group.
- 5 From the resulting menu, choose **Edit Access Control**.



- 6 From the **Inspect/Edit** window, click the **Event Privileges** 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 4.0 Administrator's Guide*.



## Configuring to Allow Forwarding of Correlation Events

The ArcSight Forwarding Connector can forward events based upon the ACL assigned to the User Group on the source ESM Manager. The Forwarding 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 also can be configured to allow for viewing of the detailed chain of the forwarded correlation event, which can include the original base event.

To configure the source Manager to send both correlation events and on-demand base 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 base events from the correlation events that are forwarded to the target ESM 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 by doing the following:

- 1 Open the properties file `server.defaults.properties`, found under `$ARCSIGHT_HOME\config`.  
 The file displays the current default  
`filestore.disksize.max.megabytes.int=1024`
- 2 Use the following formula to determine the appropriate rate for minutes of storage for 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 the 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 3](#).



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 per the instructions provided in the connector release notes.
- 2 Start the installer by running the executable for your operating system.

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

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

When the installation of connector core component software is finished, the following window is displayed:



- 3 Choose your ArcSight Forwarding Connector destination, which includes **ArcSight Manager (encrypted)**, **ArcSight Logger SmartMessage (encrypted)**, **NSP Device Poll Listener**, **CEF Syslog (cleartext)** or a **.csv file**.

To forward events to an **ArcSight ESM Manager**, proceed with ["Forwarding Events to an ArcSight ESM Manager" on page 7](#).

To forward events to an **ArcSight Logger**, proceed with ["Forwarding Events to ArcSight Logger" on page 10](#).

To forward events to an **NSP appliance**, proceed with ["Forwarding events to NSP Device Poll Listener" on page 11](#).

To forward events to a **CEF Syslog**, proceed with ["Forwarding CEF Syslog Events" on page 13](#).

To forward events to a **.csv file**, proceed with ["Forwarding events to a CSV File" on page 14](#).

## Destination Configuration

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

### Forwarding Events to an ArcSight ESM Manager

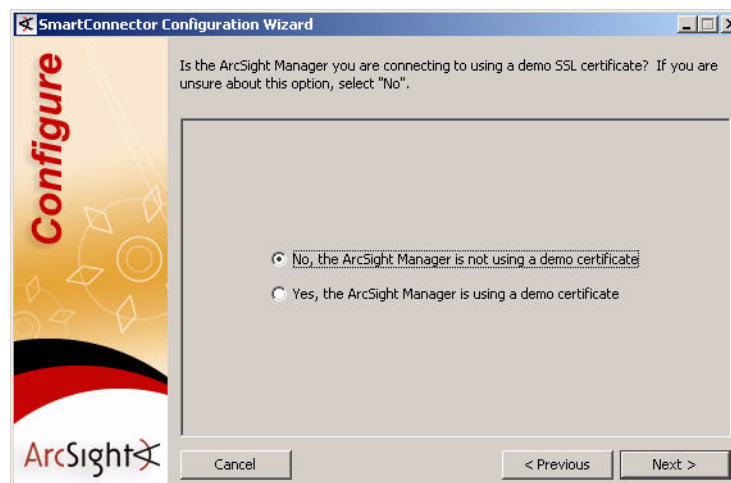
To continue connector configuration for forwarding events to an ESM Manager:

- 1 Select **ArcSight Manager (encrypted)** from the following dialog box; click **Next**.



- 2 The Wizard first prompts you for Manager certificate information.

The default selection 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**.



After completing the SmartConnector installation wizard, remember to manually configure the connector for the type of SSL certificate your Manager is using. Refer to the *ArcSight ESM 4.5 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 the text 'Please complete the following ArcSight Manager information.' Below this are four fields: 'Manager Host Name' with 'localhost', 'Manager Port' with '8443', 'AUP Master Destination' with a dropdown set to 'false', and 'Filter Out All Events' with a dropdown set to 'false'. At the bottom are 'Cancel', '< Previous', and 'Next >' buttons.

- 4 Enter a valid ArcSight **User Name** and **Password**. This should be the user name and password for the user account you created with permissions for the Forwarding Connector 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 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' and 'Password' with '\*\*\*\*\*'. At the bottom are 'Cancel', '< Previous', and 'Next >' buttons.

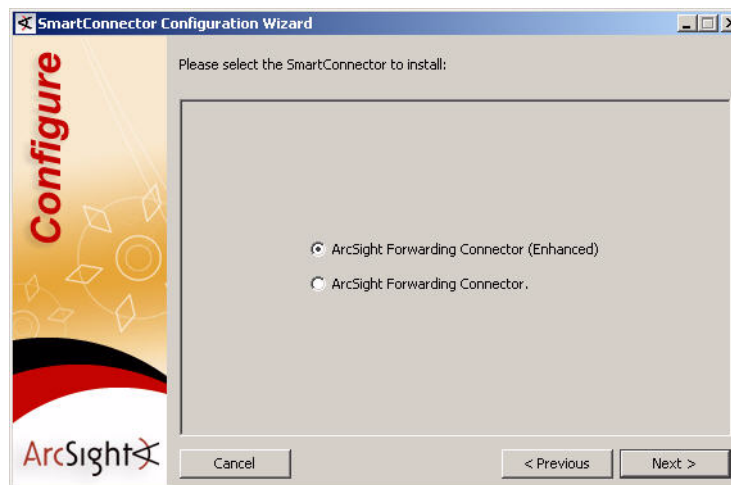
Click **Next**.

- 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.

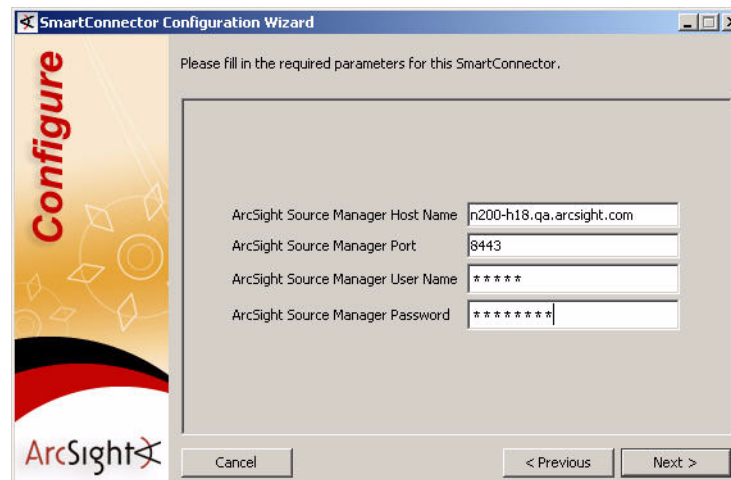
When choosing which version to use, note the following:

- ◆ 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 an ESM installation prior to **v4.0 SP3**.
- ◆ Neither Forwarding Connector release is **FIPS compliant**. If you require FIPS compliance, please 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 5](#). Click **Next**.



- 6 Enter the parameters below to configure the Forwarding Connector. This is information regarding your source ESM Manager.



Click **Next** to continue.

Parameter	Description
<b>ArcSight Source Manager Hostname</b>	Hostname where the ArcSight ESM Source Manager is installed.
<b>ArcSight Source Manager Port</b>	Network Port where the ArcSight ESM Source Manager is accepting requests.
<b>ArcSight Source Manager User Name</b>	ArcSight's user name that will be used to log this Connector into the ArcSight ESM Source Manager.
<b>ArcSight Source Manager Password</b>	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 **Back** 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**.

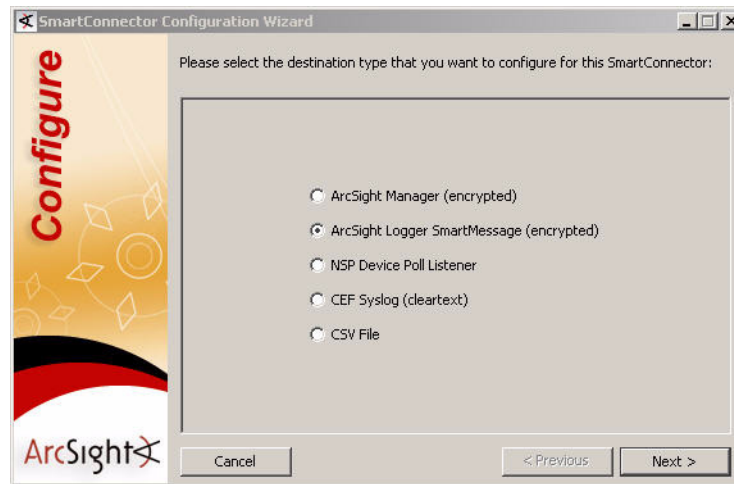
## Forwarding Events to ArcSight Logger



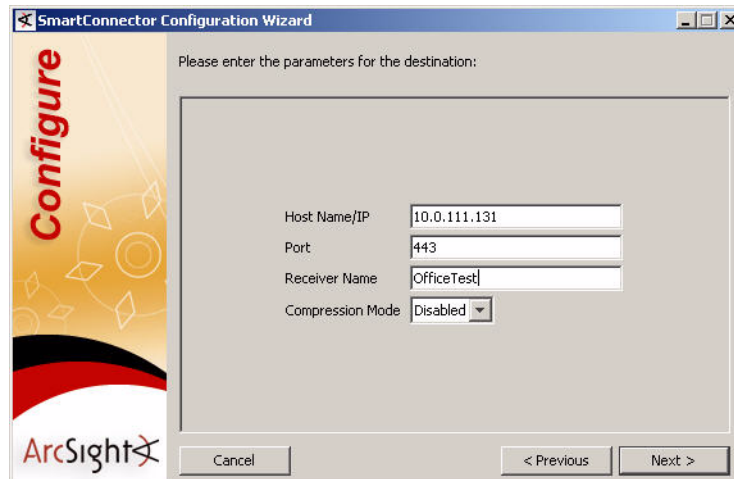
When configuring the Forwarding Connector to send events to a non-ESM destination, you may encounter problems with certificate validation during connector setup. See ["Sending Events to a Non-ESM Location" on page 2](#) for information on certificate validation.

To continue connector configuration for forwarding events to an ArcSight Logger, first 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). Then continue connector configuration as follows:

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



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



- 3 Click **Next** and continue following the Configuration Wizard to complete your configuration until a message confirms that it 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 may 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**.



- 2 Enter the **NCM Host** name or IP address, the **NCM/TRM User**, and the **NCM/TRM Password**. The **NCM/TRM Host** is the IP address or hostname of the NCM/TRM system that will interact with the syslog connector. The **NCM/TRM User** and **NCM/TRM Password** are the user name and password credentials you use to log into the NCM/TRM system.



- 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.

For more details regarding 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.)

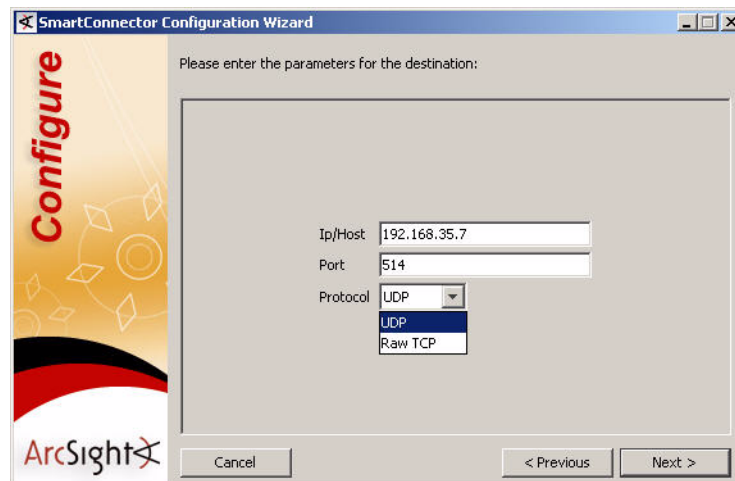


When configuring the Forwarding Connector to send events to a non-ESM destination, you may encounter problems with certificate validation during connector setup. See ["Sending Events to a Non-ESM Location"](#) on page 2 for information on certificate validation.

- 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 ‘#.’



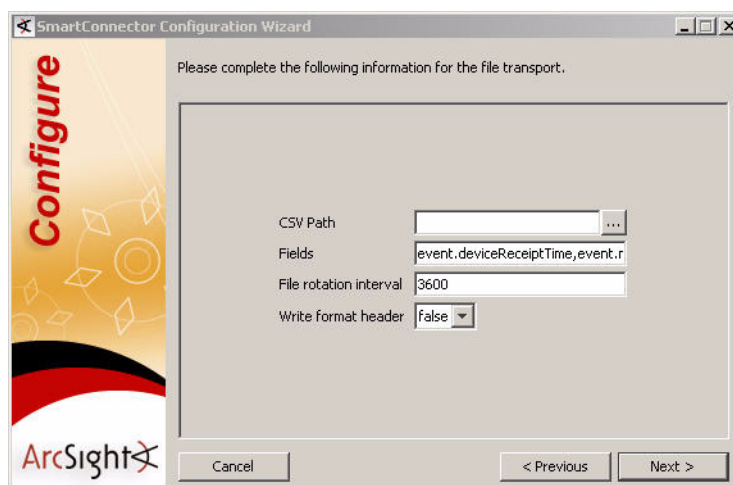
When configuring the Forwarding Connector to send events to a non-ESM destination, you may encounter problems with certificate validation during connector setup. See [“Sending Events to a Non-ESM Location” on page 2](#) for information on certificate validation.

To forward events to a .csv file:

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



- 2 For these parameters, enter the values below.



Parameter	Description
<b>CSV Path</b>	The path to the output folder. If one does not exist, a folder is created.

Parameter	Description
<b>Fields</b>	A comma-delimited string of field names to be sent to the .csv file. Field names are in the form event.targetPort.
<b>File rotation interval</b>	The desired file rotation interval, in seconds. The default is 3,600 (one hour).
<b>Write format header</b>	Select <b>true</b> to send a header row with labels for each column, as described above.

- 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.

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

## 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 found under **All Programs, ArcSight SmartConnectors**. If Connectors were 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
```



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. Do you want to upgrade?" Select the option to continue and upgrade the connector.

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

To rollback the 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.