Micro Focus Security ArcSight Connectors

SmartConnector for ArcSight CEF Cisco FireSIGHT Syslog

Configuration Guide

January 16, 2020

Configuration Guide

SmartConnector for ArcSight CEF Cisco FireSIGHT Syslog

January 16, 2020

Legal Notices

Micro Focus

The Lawn

22-30 Old Bath Road

Newbury, Berkshire RG14 1QN

UK

https://www.microfocus.com.

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.

Documentation Updates

The title page of this document contains the following identifying information:

*** Software Version number**

*** Document Release Date, which changes each time the document is updated**

*** Software Release Date, which indicates the release date of this version of the software**

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

https://community.microfocus.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

Revision History

Date	Description
10/17/2017	Added encryption parameters to Global Parameters.
09/12/2017	Updated link to sample perl script for configuring the CEF Agent.
04/15/2017	Updated "Configure the CEF Agent" section.
02/15/2017	Updated configuration information for Configuring CEF Agent.
11/30/2016	Updated installation procedure for setting preferred IP address mode. Updated Client configuration information.
08/30/2016	Expanded overview and configuration information.
06/30/2016	First edition of this Configuration Guide.

SmartConnector for ArcSight CEF Cisco FireSIGHT Syslog

This guide provides information for installing the SmartConnector for ArcSight CEF Cisco FireSIGHT Syslog and configuring the device for syslog event collection. FireSIGHT versions 5.4 and 6.0 are supported.

For Common Event Format (CEF) mappings, see the configuration guide for the CEF Certified connector available from the vendor. (https://community.microfocus.com/t5/ArcSight-Connectors/ArcSight-Common-Event-Format-CEF-Implementation-Standard/ta-p/1645557).

Product Overview

The Cisco FireSIGHT Management Center centrally manages network security and operational functions, including event monitoring, analysis, incident prioritization, and reporting. It streamlines operations and automates many commonly recurring security analysis and management tasks.

The SmartConnector for ArcSight CEF Cisco FireSIGHT is a single connector solution for retrieving event and payload information from FireSIGHT. This connector is based on Syslog Daemon and incorporates payload retrieval. The FireSIGHT DB is queried using the event ID and Sensor Name as input for payload retrieval.

Payload Retrieval

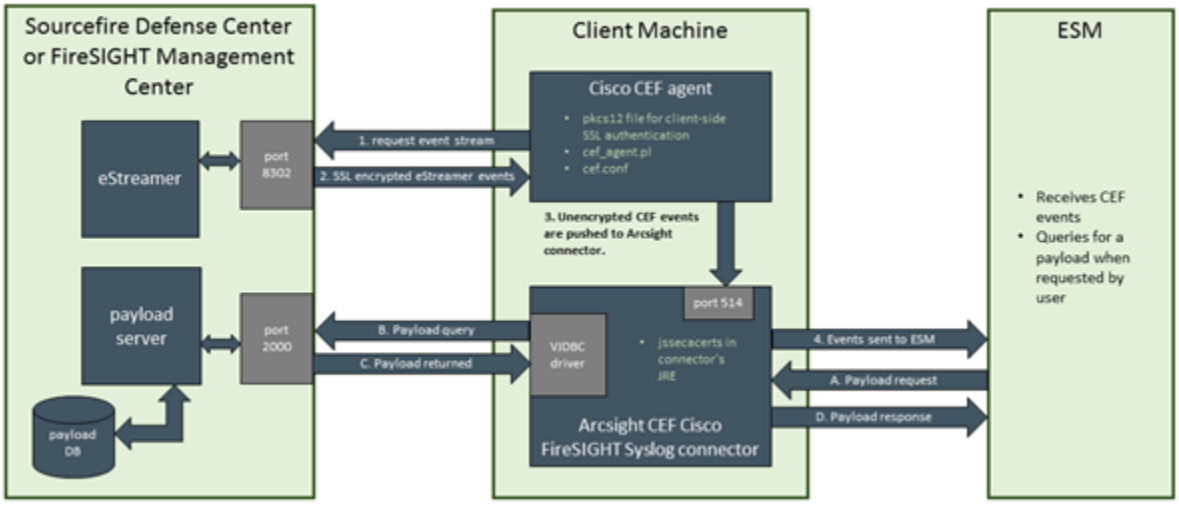
An event "payload" is the information carried in the body of the event's network packet, as distinct from the packet's header data. While security event detection and analysis usually centers on header data, packet payload can also be significant for historical analysis purposes.

Typically, devices discard payloads after a certain period of time. As described in "Working with Event Payloads" in the *ArcSight Console User's Guide*, (https://community.microfocus.com/t5/ESM-and-ESM-Express/ESM-7-2-ArcSight-Console-User-s-Guide/ta-p/1661010) you can retrieve, preserve, view, or discard payloads using the ArcSight Console. If the payload is still held on the device, the SmartConnector retrieves it and sends it to the Console. For more information about monitoring payload, see "Payload" in the "Data Monitors" section of the *ArcSight Console User's Guide*.

SmartConnector Data Flow

The three major components are involved in event collection are the Sourcefire Defense Center or FireSIGHT Management Center, the Client Machine, and ArcSight ESM.

The following figure illustrates the data flow.



Sourcefire Defense Center or FireSIGHT Management Center

The Defense or Management Center is comprised of both an eStreamer Server and a Payload Server.

eStreamer Server

When requested, this server sends data via port 8302 (default) to the Cisco CEF agent (the Client machine). The port number is configurable. See "Configure eStreamer Event Types" for information about selecting the types of events you want eStreamer to capture.

Payload Server

The payload server collects data from the payload database and forwards it via port 2000 to the SmartConnector for ArcSight CEF Cisco FireSIGHT Syslog. "Configure Database Access" provides steps for creating a database user account, enabling database access, downloading the JDBC driver, and downloading the SSL certificate so you will be able to access the database for payload information.

Client Machine

Micro Focus recommends the Cisco CEF agent and the SmartConnector be installed on the same Client Machine.

Cisco CEF agent

The Cisco CEF agent receives SSL encrypted events and pushes them to the SmartConnector via port 514 (default). The port number is configurable. For client-side SSL authentication, a pkcs12 file is required. See "Configure CEF Agent" for steps to follow to obtain this file.

ArcSight CEF Cisco FireSIGHT Syslog connector

Unencrypted CEF events are pushed to the SmartConnector. Events are sent to ESM. The connector requests payload data from Payload Server and payload is returned via the VJDBC driver. For authentication, a jssecacerts file is required.

ESM

ArcSight ESM receives the CEF events. It also queries for a payload when requested by the user and receives payload response.

Configuration

The eStreamer server (see "Configure eStreamer Event Types"), the payload server (see "Configure Database Access"), and the client (see "Configure CEF Agent") all require setup for the SmartConnector to work as expected.

The information in this section has been derived from the *Cisco FireSIGHT System Database Access Guide*. For complete configuration information, see the Cisco documentation: (http://www.cisco.com/c/en/us/td/docs/security/firesight/540/api/db-access/Database_Access.html).

Configure eStreamer Event Types

You can control which types of events the eStreamer server can transmit to the SmartConnector To select the event types you want the eStreamer server to transmit to the connector:

1. Select System -> Local -> Registration.
2. Click eStreamer. The eStreamer page with the eStreamer Event Configuration menu is displayed.
3. From the eStreamer Event Configuration menu, select the check boxes next to the types of events you want captured and forwarded to the connector. Note that, if a check box is currently cleared, that data is not being captured, and clearing a check box does not delete data that has already been captured.
4. Click Save.

Configure Database Access

To configure database access:

- Create a database user account
- Enable database access
- Dowload the JDBC driver

Create a Database User Account

To configure access to the FireSIGHT system database, first create a user account and assign it the External Database User permission. (Users assigned the predefined Administrator role have the External Database User permission by default.) Locally created and authenticated

External Database users can change their passwords in the Defense Center web interface. See the *FireSIGHT System User Guide* for more information.

Enable Database Access on the Defense Center

After creating an External Database user, configure the Defense Center to allow access to the database on the appliance. You must also configure a database access list on the appliance and add all host IP addresses that will query the external database.

To enable database access, as Admin:

1. **On the Defense Center, select System -> Local -> Configuration.**
2. **Click Database. The Database Settings menu is displayed.**
3. **Select the Allow External Database Access check box. The Access List field is displayed.**
4. **Enter the fully qualified domain name (FQDN) or IPv4 Address of the Defense Center in the Server Hostname field. You cannot use an IPv6 address as this cannot be used to install a certificate. If you enter an FQDN, make sure the client can resolve the FQDN of the Defense Center. If you enter an IP address, make sure the client can connect to the Defense Center using the IP address.**
5. **To add database access for one or more IP address, click Add Hosts. An IP Address field is displayed in the Access List field.**
6. **In the IP Address field, you can add an exact IP address, an IP address range, or any to designate any IP address.**
7. **Click Add. The IP address is added to the database access list.**
8. **Click Save. The database access settings are saved.**

Download the JDBC Driver

After creating an external database user and configuring the Defense Center to allow database access, download the JDBC driver. This JDBC driver must be used to connect to the database.

To download the JDBC Driver, as Admin:

1. **On the Defense Center, select System -> Local -> Configuration.**
2. **Click Database. The Database Settings menu is displayed.**
3. **Next to Client JDBC Driver, click Download and follow the prompts to download the client.zip package.**
4. **Unpack the ZIP package. Note the location. Make sure you preserve the file structure of the package. The package contains the following directories:** `bin`, `lib`, **and** `src`. **The**

`lib` **directory contains the JDBC driver JAR files that will be needed by the SmartConnector.**

You will copy the `.jar` ***files to*** `$ARCSIGHT_HOME/current/user/agent/lib` ***after you have completed installation of the connector core software. See "Copy Files to SmartConnector Folders" following "Install Core Software" in the SmartConnector installation section of this guide.***

Install the Client SSL Certificate

Use the Cisco-provided program named InstallCert to accept and install the SSL certificate from the Defense Center. The SmartConnector and the Defense Center communicate securely with the certificate authentication. When you accept the certificate, your computer adds it to the keystore (jssecacerts) in the security directory of the currently running JRE:

```
$JAVA_HOME/jre[version]/lib/security
```

The following are common locations of the keystore for computers running Microsoft Windows and UNIX, respectively:

```
C:\Program Files\Java\jre[version]\lib\security\jssecacerts
/var/jre[version]/lib/security/jssecacerts
```

To install the SSL certificate using InstallCert:

1. **Open a command line interface.**
2. **At the command prompt, change to the bin directory created when you unpacked the ZIP package.**
3. **To install the Defense Center's SSL certificate, enter the following:**

   ```
   java InstallCert <defense_center>
   ```

   where `<defense_center>` **is either the FQDN or the IP address of the Defense Center.**

   You are prompted to view the certificate.

5. **Optionally, view the certificate. You are prompted to accept the certificate.**
6. **Accept the certificate.**

You will copy the certificate file `jssecacerts` ***to*** `$ARCSIGHT_HOME/current/jre/lib/security` ***after you have completed installation of the connector core software. See "Copy Files to SmartConnector Folders" following "Install Core Software" in the SmartConnector installation section of this guide.***

Connect to the Database

After you install the certificate, you can query the database on a Defense Center using any third-party client that supports JDBC SSL connections. The following lists information needed to configure a connection between your client and the Defense Center.

JDBC URL: The following JDBC URL identifies the Cisco database so the JDBC driver on your client can establish connection with it:

```
jdbc:vjdbc:rmi://defense_center:2000/VJdbc,eqe
```

where defense_center is either the FQDN or the IP address for the Defense Center.

JDBC Driver JAR Files: Use the following JAR files when you configure a connection to the Cisco database:

```
vjdbc.jar commons-logging-1.1.jar
```

These files are located in the lib subdirectory where you unpacked the client.zip file you downloaded and unpacked as described in "Downloading the JDBC Driver."

JDBC Driver Class: Use the following driver class when you configure a connection to the Cisco database:

```
com.sourcefire.vjdbc.VirtualDriver
```

User name and password: Use the user account you created in "Create a User Database Account."

Configure CEF Agent (eStreamer Client)

There are two tasks to be completed to configure the CEF Agent

- **Add Authentication for the CEF Agent**
- **Configure the CEF Agent**

Add Authentication for the CEF Agent

Before eStreamer can send events to a client, you must add the client to the eStreamer server's peers database. You also must copy the authentication certificate generated by the eStreamer server to the CEF Agent.

To add the eStreamer client (CEF Agent)

1. **Select Local > Registration > eStreamer. The eStreamer page is displayed.**
2. **Click Create Client. The Create Client page is displayed.**

3 In the Hostname field, enter the host name of IP address of the host running the eStreamer client. If you use a host name, the host input serber must be able to resolve the host to an IP address. If you have not configured DNS resolution, configure it first or use an IP address.

4 To encrypt the certificate file, enter a password in the Password field.

5 Click Save.

6 Click the download icon next to the certificate file.

7 Save the certificate file. Youi will copy this file to the appropriate folder during the "Configure the CEF Agent" procedure below.

Configure the CEF Agent

Note that the Cisco CEF agent is a Perl script; therefore, Perl must be installed on the machine hosting the eStreamer Client (CEF Agent). When the Perl script is being executed, it sends a request to the server, including current time on client machine, and the server returns events having a start time later than that time sent by the client.

If there are no new events on the eStreamer server, the client does not receive events. The Perl script can be modified so the client will request events having a start time from somewhere in the past (long enough to make sure all events are received from the eStreamer server). Knowledge of perl is required to make changes to this script.

To configure the CEF client:

1 Download the sample perl file, cef_forwarder-master-d35283bd625ed63e215680d2381ddcef55f2c121.zip, from Protect724: https://community.microfocus.com/t5/ArcSight-Connectors/Sample-perl-script-for-ArcSight-CEF-Cisco-FireSIGHT-Syslog/ta-p/1613532 and modify as needed to suit your organization's environment. The forwarder is an eStreamer client that converts eStreamer data collected from FireSIGHT into ArcSight's Common Event Format (CEF) for input into ArcSight ESM. The purpose of this script is to do the conversion to CEF and then send to the syslog connector.

2 Unzip the file.

3 Copy the `PKCS12` file you downloaded in "Add Authenticatiojn for the CEF Agent" to the directory where you unzipped the file.

4 Modify the `cef.conf` file according to your environment.

The following settings are required:

```
estreamer_server=<hostname or ip address>
pkcs12_file=<filename>
cef_server=<hostname or ip address>
```

To change the ports used from the default values, modify the following settings:

```
estreamer_port=8302 cef_port=514
```

Run the CEF Client

To start the client, change to the directory where the script was installed, and run the script as follows:

```
./cef_agent.pl
```

If you want the script to run in the background or as a service, set the daemon option in the configuration file to 1.

Install the SmartConnector

The following sections provide instructions for installing and configuring your selected SmartConnector.

Prepare to Install Connector

Before you install any SmartConnectors, make sure that the ArcSight products with which the connectors will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger).

For complete product information, read the *Administrator's Guide* as well as the *Installation and Configuration* guide for your ArcSight product before installing a new SmartConnector. If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* for instructions, and start the installation procedure at "Set Global Parameters (optional)" or "Select Connector and Add Parameter Information."

Before installing the SmartConnector, be sure the following are available:

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

Install Core Software

Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms; for the complete list, see the *SmartConnector Product and Platform Support* document, available from the Micro Focus SSO and Protect 724 sites.

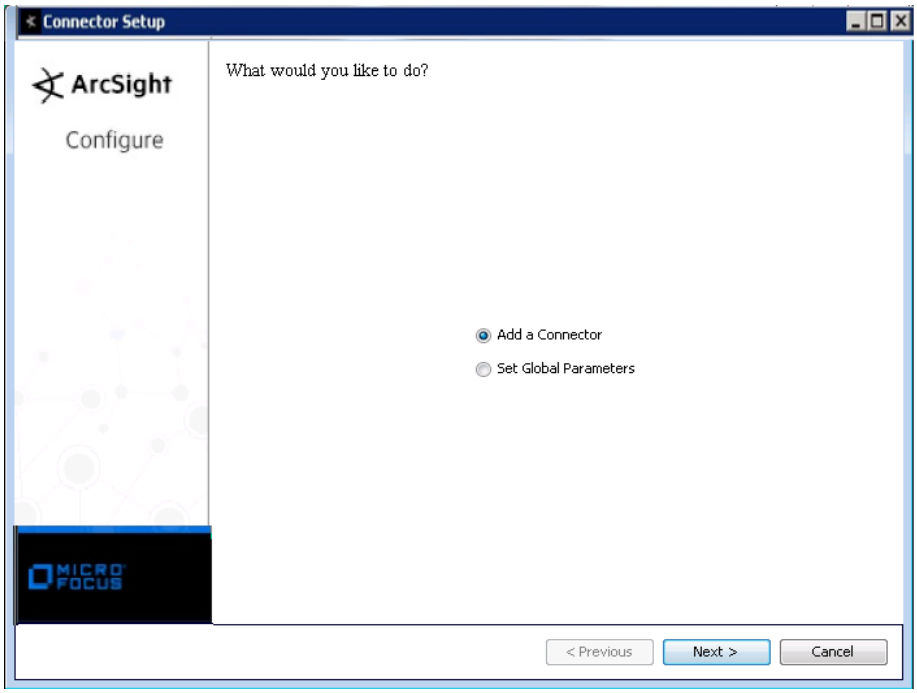
1 **Download the SmartConnector executable for your operating system from the Micro Focus SSO site.**

2 **Start the SmartConnector installation and configuration wizard by running the executable.**

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

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

3 **When the installation of SmartConnector core component software is finished, the following window is displayed:**



Copy Files to SmartConnector Folders

Leave the wizard at this point to copy certificate and JDBC files to SmartConnector folders as follows.

1 **Copy the certificate (`jssecacerts`) that you installed during device configuration (see "Install the Client SSL Certificate") to the connector folder `$ARCSIGHT_HOME/current/jre/lib/security`.**

> **When upgrading the connector, this file is overwritten and the certificate must be recopied to the folder.**

2 **Copy the** `vjdbc.jar` **and** `commons-logging-1.1.jar` **files to the connector folder** `$ARCSIGHT_HOME/current/user/agent/lib`**. These files are located in the** `lib` **directory that was created when you downloaded the JDBC driver and unzipped the package. See "Download the JDBC Driver."**

3 **From** `$ARCSIGHT_HOME/current/bin`**, double-click** `runagentsetup` **to return to the SmartConnector Configuration Wizard.**

Set Global Parameters (optional)

If you choose to perform any of the operations shown in the following table, do so before adding your connector. You can set the following parameters:

Parameter	Setting
FIPS mode	Select 'Enabled' to enable FIPS compliant mode. To enable FIPS Suite B Mode, see the SmartConnector User Guide under "Modifying Connector Parameters" for instructions. Initially, this value is set to 'Disabled'.
Remote Management	Select 'Enabled' to enable remote management from ArcSight Management Center. When queried by the remote management device, the values you specify here for enabling remote management and the port number will be used. Initially, this value is set to 'Disabled'.
Remote Management Listener Port	The remote management device will listen to the port specified in this field. The default port number is 9001.
Preferred IP Version	When both IPv4 and IPv6 IP addresses are available for the local host (the machine on which the connector is installed), you can choose which version is preferred. Otherwise, you will see only one selection. The initial setting is IPv4.

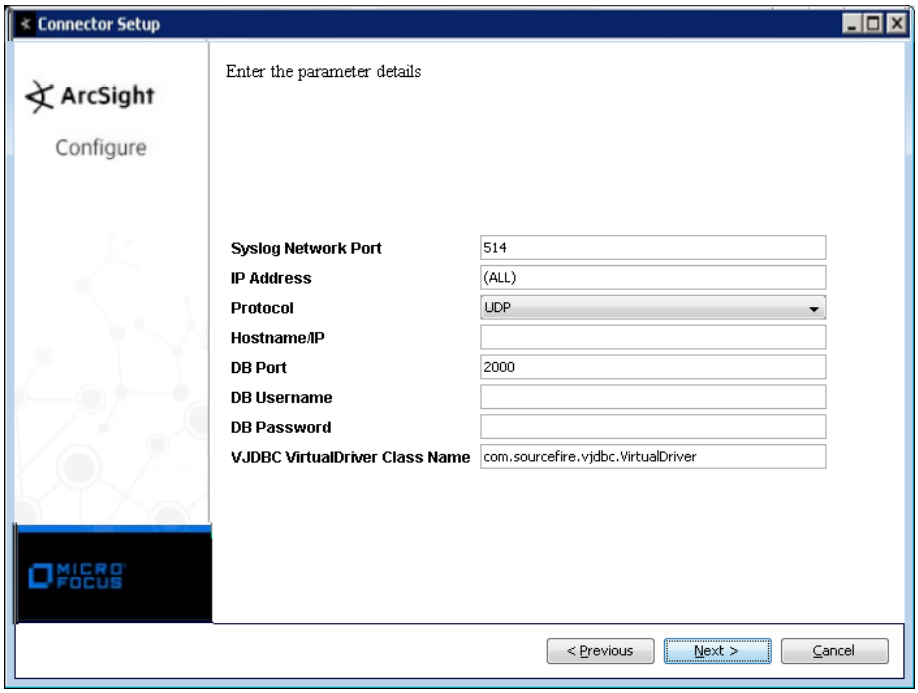
The following parameters should be configured only if you are using Micro Focus SecureData solutions to provide encryption. See the *Micro Focus SecureData Architecture Guide* for more information.

Parameter	Setting
Format Preserving Encryption	Data leaving the connector machine to a specified destination can be encrypted by selecting 'Enabled' to encrypt the fields identified in 'Event Fields to Encrypt' before forwarding events. If encryption is enabled, it cannot be disabled. Changing any of the encryption parameters again will require a fresh installation of the connector.
Format Preserving Policy URL	Enter the URL where the Micro Focus SecureData Server is installed.
Proxy Server (https)	Enter the proxy host for https connection if any proxy is enabled for this machine.
Proxy Port	Enter the proxy port for https connection if any proxy is enabled for this machine.
Format Preserving Identity	The Micro Focus SecureData client software allows client applications to protect and access data based on key names. This key name is referred to as the identity. Enter the user identity configured for Micro Focus SecureData.
Format Preserving Secret	Enter the secret configured for Micro Focus SecureData to use for encryption.
Event Fields to Encrypt	Recommended fields for encryption are listed; delete any fields you do not want encrypted and add any string or numeric fields you want encrypted. Encrypting more fields can affect performance, with 20 fields being the maximum recommended. Also, because encryption changes the value, rules or categorization could also be affected. Once encryption is enabled, the list of event fields cannot be edited.

After making your selections, click Next. A summary screen is displayed. Review the summary of your selections and click Next. Click Continue to return to proceed with "Add a Connector" window. Continue the installation procedure with "Select Connector and Add Parameter Information."

Select Connector and Add Parameter Information

1. **Select Add a Connector and click Next. If applicable, you can enable FIPS mode and enable remote management later in the wizard after SmartConnector configuration.**
2. **Select ArcSight CEF Cisco FireSIGHT Syslog and click Next.**
3. **Enter the required SmartConnector parameters to configure the SmartConnector, then click Next.**



Parameter	Description
Syslog Network Port	Enter the number of the port where the syslog connector will listen for incoming messages. The default value is 514.
IP Address	Enter the IP address where the connector will listen for incoming messages. The default value is (ALL), meaning the connector listens to all IP addresses on the specified port.
Protocol	Select the protocol to be used to receive incoming messages. Options are UDP or Raw TCP. UDP is the default value.
Hostname/IP	Enter the host name or IP address for the FireSIGHT DB.
DB Port	Enter the port number for the FireSIGHT DB. The default value is 2000.
DB Username	Enter the FireSIGHT DB User Name.
DB Password	Enter the password for the FireSIGHT DB user.

Parameter	Description
VJDBC Virtual Driver Class Name	Enter the FireSIGHT Qualified VJDBC Virtual Driver Class Name. The default value is com.sourcefire.vjdbc.VirtualDriver.

Select a Destination

1. The next window asks for the destination type; select a destination and click Next. For information about the destinations listed, see the *ArcSight SmartConnector User Guide*.
2. Enter values for the destination. For the ArcSight Manager destination, the values you enter for User and Password should be the same ArcSight user name and password you created during the ArcSight Manager installation. Click Next.
3. Enter a name for the SmartConnector and provide other information identifying the connector's use in your environment. Click Next. The connector starts the registration process.
4. If you have selected ArcSight Manager as the destination, the certificate import window for the ArcSight Manager is displayed. Select Import the certificate to the connector from destination and click Next. (If you select Do not import the certificate to connector from destination, the connector installation will end.) The certificate is imported and the Add connector Summary window is displayed.

Complete Installation and Configuration

1. Review the Add Connector Summary and click Next. If the summary is incorrect, click Previous to make changes.
2. The wizard now prompts you to choose whether you want to run the SmartConnector as a stand-alone process or as a service. If you choose to run the connector as a stand-alone process, select Leave as a standalone application, click Next, and continue with step 5.
3. If you chose to run the connector as a service, with Install as a service selected, click Next. The wizard prompts you to define service parameters. Enter values for Service Internal Name and Service Display Name and select Yes or No for Start the service automatically. The Install Service Summary window is displayed when you click Next.
4. Click Next on the summary window.
5. To complete the installation, choose Exit and Click Next.

For instructions about upgrading the connector or modifying parameters, see the *SmartConnector User Guide*.

Run the SmartConnector

SmartConnectors can be installed and run in stand-alone mode, on Windows platforms as a Windows service, or on UNIX platforms as a UNIX daemon, depending upon the platform

supported. On Windows platforms, SmartConnectors also can be run using shortcuts and optional Start menu entries.

If the connector is installed in stand-alone mode, it must be started manually and is not automatically active when a host is restarted. If installed as a service or daemon, the connector runs automatically when the host is restarted. For information about connectors running as services or daemons, see the *ArcSight SmartConnector User Guide*.

To run all SmartConnectors installed in stand-alone mode on a particular host, open a command window, go to `$ARCSIGHT_HOME\current\bin` **and run:** `arcsight connectors`

To view the SmartConnector log, read the file `$ARCSIGHT_HOME\current\logs\agent.log`**; to stop all SmartConnectors, enter** `Ctrl+C` **in the command window.**