# Micro Focus Security ArcSight SmartConnectors

Software Version: 8.3.0

## Configuration Guide for ArcSight CEF Cisco FireSIGHT Syslog SmartConnector

Document Release Date: February 2022
Software Release Date: February 2022

# Legal Notices

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

https://www.microfocus.com

# Copyright Notice



# Trademark Notices



# 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://www.microfocus.com/support-and-services/documentation

# Support

## Contact Information

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

# About this PDF Version of Online Help

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

# Contents

Configuration Guide for ArcSight CEF Cisco FireSIGHT Syslog SmartConnector

# Configuration Guide for ArcSight CEF Cisco FireSIGHT Syslog SmartConnector

This guide provides information to install the SmartConnector for ArcSight CEF Cisco FireSIGHT Syslog and configure the device for syslog event collection. For higher versions, refer to the Cisco Event Streamer ( https://marketplace.microfocus.com/arcsight/content/cisco-firepower ).

# 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 to retrieve event and payload information from FireSIGHT. This connector is based on Syslog Daemon and incorporates payload retrieval. For payload retrieval, it queries the FireSIGHT DB by using the event ID and Sensor Name as input.

**Payload Retrieval**

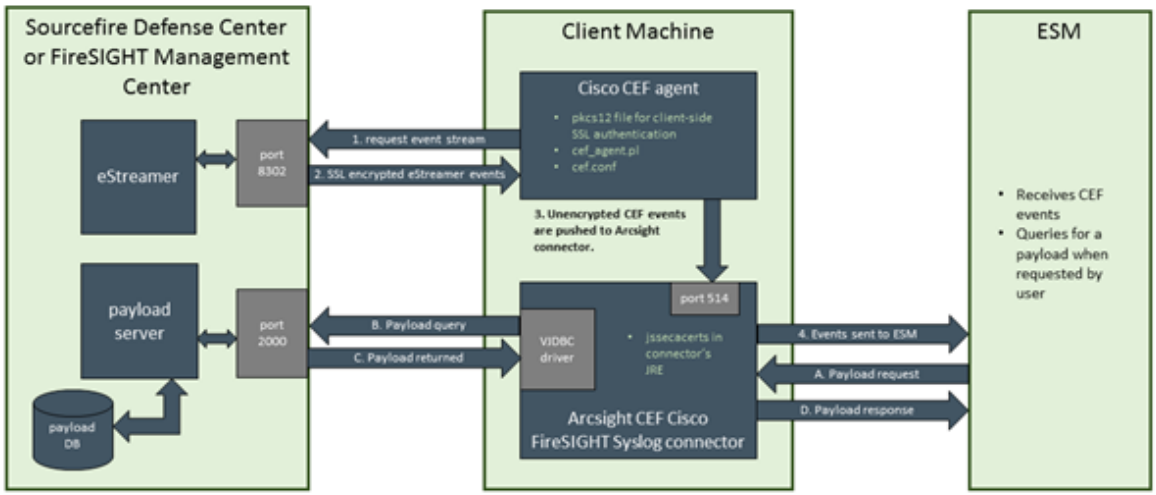
Payload for an event is the information carried in the body of the network packet of an event. It is distinct from the packet's header data. While security event detection and analysis usually centers around the header data, packet payload provides significant information related to historical analysis.

Typically, devices discard payloads after a certain period of time. 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 in the *ArcSight Console User's Guide*.

**Data Flow During Event Collection**

The following figure illustrates how the data flows during event collection:

Configuration Guide for ArcSight CEF Cisco FireSIGHT Syslog SmartConnector




The following components are involved in event collection:

- **Sourcefire Defense Center or FireSIGHT Management Center:** The Defense or Management Center is comprised of eStreamer Server and a Payload Server:
  - **eStreamer Server:** When requested, this server sends data through 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 through 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 that 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.
- **ArcSight ESM:** ArcSight ESM receives the CEF events. It also queries for a payload when requested by the user and receives payload response.

Configuration Guide for ArcSight CEF Cisco FireSIGHT Syslog SmartConnector

# Common Event Format Implementation

The Common Event Format (CEF) standard format, developed by ArcSight, lets vendors and their customers quickly integrate their product information into ESM. CEF is an open log management standard that simplifies log management, letting third parties create their own device schema that are compatible with a standard that is used industry-wide for normalizing security events. Technology companies and customers can use the standardized CEF format to facilitate data collection and aggregation, for later analysis by an enterprise management system.

For more information about CEF, see the *Implementing ArcSight Common Event Format (CEF)* Guide. It defines the CEF protocol and provides details about how to implement the standard. It details the header and predefined extensions used within the standard as well as how to create user defined extensions. It also includes a list of CEF mappings as well as supported date formats.

# Configuring the Device for Event Collection

You must configure the eStreamer server, the payload server, and the client for the SmartConnector to work as expected.

The information in this section is derived from the *Cisco FireSIGHT System Database Access Guide*. For complete configuration information, see the Cisco documentation.

**Configuring eStreamer Event Types**

You can control the types of events that are transmitted from the eStreamer server 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 that you want forwarded to the SmartConnector, then click **Save**.

   **Note:** If you clear a check box that was selected earlier, it stops capturing that type of data, but does not delete data that has already been captured.

**Configuring Database Access**

Configuration Guide for ArcSight CEF Cisco FireSIGHT Syslog SmartConnector

To configure database access, complete the following procedures:

1. Create a database user account
2. Enable database access
3. Download the JDBC driver
4. Install the Client SSL Certificate
5. Connect to the Database

**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. If the user is assigned the predefined Administrator role, then External Database User permission is assigned by default. Locally created and authenticated External Database users can change their passwords in the Defense Center web interface. For more information, see the *FireSIGHT System User Guide*.

**Enable Database Access on the Defense Center**

You must 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. Make sure that the client can resolve the FQDN of the Defense Center or the client can connect to the Defense Center using the IP address.
5. Click **Add Hosts**, to add database access for one or more IP address.
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** to add the IP address to the database access list.
8. Click **Save** to save the database access settings.

**Download the JDBC Driver**

The JDBC driver is used to connect to the database.

To download the JDBC Driver, as admin:

Configuration Guide for ArcSight CEF Cisco FireSIGHT Syslog SmartConnector

1. On the Defense Center, select **System > Local > Configuration**.
2. Click **Database**. The **Database Settings** menu is displayed.
3. Download and unpack the .zip package.

   Make sure you note down the path to the file and 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.

**Install the Client SSL Certificate**

The SmartConnector and the Defense Center communicate securely with the certificate authentication.

Use the InstallCert program provided by Cisco to accept and install the SSL certificate from the Defense Center.

To install the SSL certificate using InstallCert:

1. Open a command line interface.
2. Change to the bin directory created when you unpacked the .zip package.
3. Enter the following command to install the Defense Center's SSL certificate:

   `java InstallCert <defense_center>`

   where `<defense_center>` is either the FQDN or the IP address of the Defense Center.
4. View and accept the certificate.

   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 default locations of the keystore:

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

   **Note:** Note the location of the *`jssecacerts`* certificate file as you need to copy it to the installation directory of the SmartConnector.

**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 information is needed to configure a connection between your client and the Defense Center.

Configuration Guide for ArcSight CEF Cisco FireSIGHT Syslog SmartConnector

- **JDBC URL:** The following JDBC URL identifies the Cisco database so that the JDBC driver on your client can establish a 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 sub-directory where you unpacked the client.zip file.
- **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 that you created in Create a User Database Account.

**Configuring CEF Agent (eStreamer Client)**

Complete the following procedures to configure the CEF Agent:

- Add Authentication for the CEF Agent
- Configure the CEF Agent
- Run 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**.
2. Click **Create Client**.
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 server 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**.

Configuration Guide for ArcSight CEF Cisco FireSIGHT Syslog SmartConnector

6. Click the download icon next to the certificate file.
7. Save the certificate file. You must copy this file to the appropriate folder during the Configure the CEF Agent procedure.

# Configure the CEF Agent

Cisco CEF agent is a Perl script. You must install the Perl script on the machine hosting the eStreamer Client (CEF Agent). When the Perl script is executed, it sends a request to the server, including current time on the client machine, and the server returns all events with the start time later than the time sent by the client. If there are no new events on the eStreamer server, the client does not receive any events.

The Perl script can be modified to request events with a start time in the past, so that all events are received from the eStreamer server. To make changes to the Perl scrip, knowledge of Perl is necessary.

To configure the CEF client:

1. Download the sample Perl file, cef_forwarder-master-d35283bd625ed63e215680d2381ddcef55f2c121.zip, from Protect724 and modify it as per the need of your organization. The forwarder is an eStreamer client that converts eStreamer data collected from FireSIGHT into ArcSight's CEF format to input into ArcSight ESM. The script converts data to CEF and then sends it to the syslog connector.
2. Extract the contents of the file.
3. Copy the PKCS12 file you downloaded in Add Authentication for the CEF Agent to the directory where you unzipped the file.
4. Modify the `cef.conf` file according to your environment.
5. Specify the following settings:

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

6. To change default values used for ports, 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, then specify the following command to run the script:

```
./cef_agent.pl
```

Configuration Guide for ArcSight CEF Cisco FireSIGHT Syslog SmartConnector

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

# Preparing to Install the SmartConnector

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

For complete product information, refer to the *Administrator's Guide to ArcSight Platform*, available on ArcSight Documentation.

If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* available on ArcSight Documentation for instructions.

Before installing the SmartConnector, make sure that the following are available:

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

# Installing and Configuring the SmartConnector

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.
3. Exit the installation wizard.
4. Copy certificate and JDBC files to SmartConnector folders as follows:
   - Copy the `jssecacerts` certificate that you installed during the device configuration to the SmartConnector installation folder `$ARCSIGHT_HOME/current/jre/lib/security`.

     **Note:** You must copy this file again to the installation folder after upgrading the SmartConnector as this file gets overwritten during the upgrade process.

   - Copy the `vjdbc.jar` and `commons-logging-1.1.jar` files to the SmartConnectorinstallation 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.

Configuration Guide for ArcSight CEF Cisco FireSIGHT Syslog SmartConnector

5. Browse `to $ARCSIGHT_HOME/current/bin`, then double-click `runagentsetup.bat` file to start the SmartConnector Configuration Wizard.
6. Specify the relevant Global Parameters, when prompted.
1. Select **ArcSight CEF Cisco FireSIGHT Syslog** and click **Next**.
2. Enter the required 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. |
| VJDBC Virtual Driver Class Name | Enter the FireSIGHT Qualified VJDBC Virtual Driver Class Name. The default value is com.sourcefire.vjdbc.VirtualDriver. |

3. Select a destination and configure parameters.
4. Specify a name for the connector.
5. 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.
6. Select whether you want to run the connector as a service or in the standalone mode.
7. Complete the installation.
8. Run the SmartConnector.

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

# Send Documentation Feedback

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

**Feedback on Configuration Guide for ArcSight CEF Cisco FireSIGHT Syslog SmartConnector (SmartConnectors 8.3.0)**

Just add your feedback to the email and click send.

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

We appreciate your feedback!