Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for ArcSight Common Event Format File

Configuration Guide

October 17, 2017

Configuration Guide

SmartConnector for ArcSight Common Event Format File

October 17, 2017

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise Development LP shall not be liable for technical or editorial omissions contained herein. The information contained herein is subject to change without notice. The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only. Hewlett Packard Enterprise Development LP products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices. This document is confidential.

Restricted Rights Legend

Follow this link to see a complete statement of Hewlett Packard Enterprise Development LP copyrights, trademarks and acknowledgements: https://community.saas.hpe.com/t5/Discussions/Third-Party-Copyright-Notices-and-License-Terms/td-p/1589228.

Revision History

Date	Description
10/17/2017	Added encryption parameters to Global Parameters.
08/15/2017	Updated link to CEF Implementation Standard.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
05/16/2016	Added overview information about the CEF Implementation Standard.
08/15/2014	Removed device event mappings to ArcSight fields with referral to vendor CEF documentation.
11/15/2013	Added new screen capture of parameters screen and added Log Rotation Type section.
09/28/2012	Added Request Context and Device Payload ID mappings.
05/15/2012	Added new installation procedure.
02/15/2012	Added reference and link to ArcSight Common Event Format certified connectors.

SmartConnector for ArcSight Common Event Format File

This guide provides information for installing the SmartConnector for ArcSight CEF File.

Product Overview

The Common Event Format (CEF) is an open log management standard that improves the interoperability of security-related information from different security and network devices and applications. CEF is based upon ArcSight's expertise from building over 230 connectors across 30 different solution categories, and is the first log management standard to support a broad range of device types.

The CEF connector lets ArcSight ESM connect to, aggregate, filter, correlate, and analyze events from applications and devices with CEF standard log output. You can use this powerful, text-based log format to collect logs from customized applications when you modify the output to the CEF standard.

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 schemas 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.

The ArcSight Common Event Format (CEF) Guide, also known as "Implementing ArcSight Common Event Format (CEF)" 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.

To access this standard, go to https://community.saas.hpe.com/t5/ArcSight-Connectors/ArcSight-Common-Event-Format-CEF-Guide/ta-p/1589306 .

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 HPE SSO and Protect 724 sites.

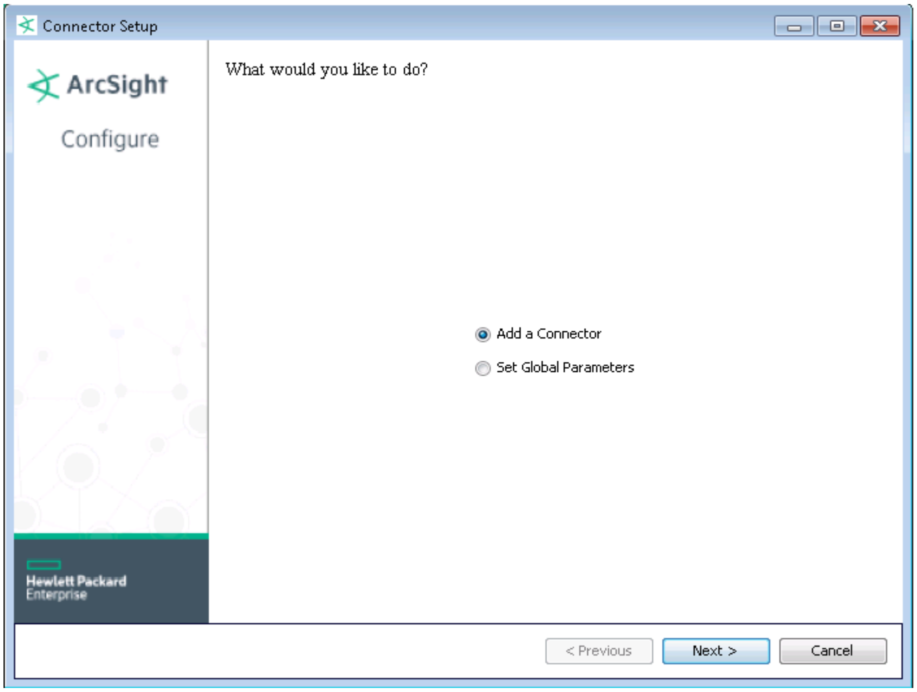
1. Download the SmartConnector executable for your operating system from the HPE SSO site.

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:



What would you like to do?

● Add a Connector
○ Set Global Parameters

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 HPE SecureData solutions to provide encryption. See the *HPE 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 HPE 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 HPE 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 HPE SecureData.
Format Preserving Secret	Enter the secret configured for HPE 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.

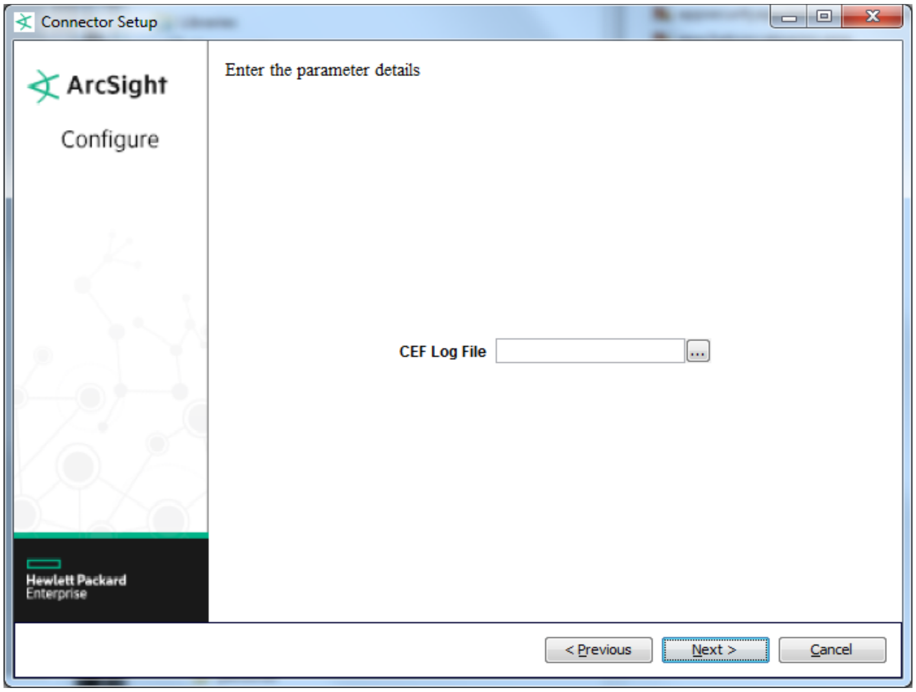
After making your selections, click **Next**. A summary screen is displayed. Review the summary of your selections and click **Next**. Click **Continue** to return to proceed with "Add a Connector" window. Continue the installation procedure with "Select Connector and Add Parameter Information."

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 Common Event Format File** and click **Next**.

3 Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



Enter the parameter details

CEF Log File

Parameter	Description
CEF Log File	Enter the name of the CEF log file.

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*.

Log Rotation Types

See the section Access Advanced Parameters for details on modifying the parameters discussed in this section.

There are three mechanisms for rotating log files:

Name Following Log Rotation: An example would be, the device writes to xyz.log. At rotation time, the device renames xyz.log to xyz1.log and creates a new xyz.log and begins to write to it. The connector detects the drop in size of xyz.log and terminates the reader thread to the old xyz.log after processing is completed. The connector creates a new reader thread to the new xyz.log and begins processing that file. To enable this log rotation, set `followexternalrotation` to true.

Daily Rotation: A typical scenario could be, the device writes to xyz.timestamp.log on a daily basis. At a specified time, the device creates a new daily log and begins to write to it. The connector detects the new log and terminates the reader thread to the previous log after processing is complete. The connector then creates a new reader thread to the new xyz.timestamp.log and begins processing that file. To enable this log rotation, set `rotationscheme` to Daily, and set `rotationschemeparams`, as shown in the example below:

```
agents[x].rotationscheme="Daily"
agents[x].rotationschemeparams="FilePrefix,DateFormat,FileSuffix"
```

Where for a data file name of `foo.2013-09-23.log`

```
FilePrefix = foo
DateFormat = yyyy-mm-dd
FileSuffix = .log
```

Index Rotation: In this case, the device writes to indexed files - xyz.log.001, xyz.log.002, xyz.log.003 and so forth. At startup, the connector processes the log with highest index. When the device creates a log with a greater index, the connector terminates the reader thread to the previous log after processing completes, creates a thread to the new log and begins processing that log. To enable this log rotation, set `rotationscheme` to Index. To enable this log rotation, set `rotationscheme` to Index, and set `rotationschemeparams`, as shown in the example below:

```
agents[x].rotationscheme="Index"
agents[x].rotationschemeparams="FilePrefix,FileSuffix,Digits,Count,Option
al true or false"
```

Where for a data file name of `foo.log.%03d,001,999,false`

```
FilePrefix = foo
FileSuffix = .log
Digits = (%03d) Number of digits allowed after .log in the file name. In
this example, 3 digits.
Count = (001,999) How high to count in the index. In this example, the
file rotation could go to foo.log.999.
Optional true or false = Default is false, which means missing indexes
are not allowed, and the connector does not stop reading the current file
until the log file with the  next index appears. When true, specifies
that the connector keeps rpocessing if there is a missing file.
```

Access Advanced Parameters

After SmartConnector installation, you can access the connector's advanced parameters by editing the `agent.properties` file located at `$ARCSIGHT_HOME\current\user\agent`.

Modify rotationscheme, rotationschemeparams, or followexternalrotation Parameters

To modify the parameters as needed:

1. Access advanced parameters as described above.
2. Locate the `rotationscheme`, `rotationschemeparams`, or the `followexternalrotation` parameter and change the default values as described in the Log Rotation Types section.
3. Save the file and restart the connector for your changes to take effect.

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.

Device Event Mapping to ArcSight Data Fields

Refer to vendor CEF documentation for device mappings for that vendor's product.

Information from vendors is formatted according to the CEF standard and sent to the ArcSight SmartConnector, which translates the data into an ArcSight event.

In a key value parser strings do not require tokenization. They work by default.