Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for ArcSight CEF Folder Follower Scanner

Configuration Guide

October 17, 2017

Configuration Guide

SmartConnector for ArcSight CEF Folder Follower Scanner

October 17, 2017

Warranty

Restricted Rights Legend

Revision History

Date	Description
10/17/2017	Added encryption parameters to Global Parameters.
08/15/2017	Updated link to CEF Implementation Standard.
05/15/2017	Updated parameter description for CEF Log File Directory to mention the log files containing the CEF events must be UTF-8 encoded.
02/15/2017	First edition for new connector.

Contents

SmartConnector for ArcSight CEF Folder Follower Scanner

This guide provides information for installing the SmartConnector for ArcSight CEF Folder Follower Scanner.

Product Overview

This connector collects and processes CEF events, written to plain text log files, deposited in a log folder. During the processing of the CEF events, it extracts scanner and vulnerability information from it in order to send to ArcSight Enterprise Security Manager (ESM).

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 connectors let ESM connect to, aggregate, filter, correlate, and analyze events from applications and devices with CEF standard log output.

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 and 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 .

Asset and Vulnerability Extraction

The SmartConnector for ArcSight CEF Folder Follower Scanner supports asset and vulnerability extraction from CEF events to populate the assets on ArcSight Enterprise Security Manager (ESM).

The guidelines that follow allow the connector framework to extract the asset and vulnerability information from CEF events in a consistent manner.

Each event in the set of retrieved events is described according to the CEF standard. The specific CEF event fields that are used depend on the vendor’s product capabilities and the information the event is describing.

For purposes of representing asset and vulnerability information, the following guidelines must be adhered to. These guidelines specify a small set of CEF fields and conventions. Only these fields are used to produce the asset and vulnerability information. Any other CEF fields in the event are used for their normal role in describing the event.

For the SmartConnector for ArcSight CEF Folder Follower Scanner, the **Destination Host** field is used to identify assets. The CEF abbreviations for this field is `dhost`. The set of unique destination hosts or addresses identified in each set of events is collected by the connector framework.

Three categories of information are currently processed by the connector framework: open port, URI, and vulnerability. When a CEF event includes the `categoryTechnique` field with a value indicating one of these categories, the data in the other specified fields further characterize the asset. For events that do not include the `categoryTechnique` field, no asset information is extracted.

Required Event Fields

The following sections document the required event fields for each type of vulnerability.

Open Port

CEF Field	Value	Description
`name`	Open Port	– Note: This field is part of the pipe-delimited header and is not a key=value field.)
`dhost`	<Destination Host Name>	The destination host name.
`dst`	<Destination Host IP Address>	The Destination IP address.
`dpt or portList`	<Port> (and optionally <Port1, Port1, ….>)	If the event concerns a single port, the port number is specified by dpt. Alternatively, a list of open ports can be specified using portList. Because portList is not a defined CEF key, the key and its value will be CEF “additional data‘.
`categoryTechnique`	/scanner/device/openport	–
`proto`	<Protocol>	The protocol; for example TCP or UDP.

Open port example:

```
CEF:0|Acme Inc|Acme Scanner|4.0.157-1|acme-open-port|Open Port|Low|
categoryTechnique=/scanner/device/openport dst=10.0.0.1
dhost=testhost.abc.com dpt=445 proto=UDP
```

URI

CEF Field	Value	Description
`name`	URI	– Note: This field is part of the pipe-delimited header and is not a key=value field.
`dhost`	<Destination Host Name>	The destination host name.
`dst`	<Destination Host IP Address>	The Destination IP address.
`categoryTechnique`	/scanner/device/uri	–

CEF Field	Value	Description
`filePath`	<URI#URI#URI>	A list of URIs separated by the hash mark (#) character.

URI example:

```
CEF:0|Acme Inc|Acme Scanner|4.0.157-1|acme-uri|URI|Medium|
categoryTechnique=/scanner/device/uri dhost=testhost.abc.com dst=10.0.0.1
filePath=/Site Asset Categories/Operating System/Solaris 8
```

Vulnerability

CEF Field	Value	Description
`name`	URI	– Note: This field is part of the pipe-delimited header and is not a key=value field.
`dhost`	<Destination Host Name>	The destination host name.
`dst`	<Destination Host IP Address>	The Destination IP address.
`categoryTechnique`	/scanner/device/vulnerability	–
`Device Event Class ID`	<VulnerabillityNativeIdentifier=VulnerabilityNativeID #VulnerabilityNativeName #VulnerabilityNativeSeverity #VulnerabilityNativeDescription%CVE=CVE-ID #CVENAME #CVESEVERITY #CVEDESCRIPTION%…>	The percent sign (%) is used to separate vulnerability entries; the hash mark (#) is used to separate different fields of one vulnerability entry. Everything except the NativeID is optional. Note: this field is part of the pipe-delimited header and is not a key=value field.

Vulnerability example:

```
CEF:0|VulnVendor|Vulnproduct|10.x|X-Force=100641#Adobe Flash Player code
execution#9.3#Adobe Flash Player could allow a remote attacker to execute
arbitrary code on the system, caused by a use- after-free error related
to the ByteArray. By persuading a victim to visit a specially-crafted Web
site, a remote attacker could exploit this vulnerability using drive-by-
download attacks against systems running Microsoft Internet Explorer and
Mozilla Firefox on Windows 8.1 and prior to execute arbitrary code on the
system with the privileges of the victim or cause the application to
crash.%X- Force=1006411#Adobe Flash Player code execution#9.3#Adobe Flash
Player could allow a remote attacker to execute arbitrary code on the
system, caused by a use-after-free error related to the ByteArray. By
persuading a victim to visit a specially-crafted Web site, a remote
attacker could exploit this vulnerability using drive-by-download attacks
```

```
against systems running Microsoft Internet Explorer and Mozilla Firefox
on Windows 8.1 and prior to execute arbitrary code on the system with the
privileges of the victim or cause the application to
crash.|VulnEventName|High|categoryTechnique=/scanner/device/vulnerability
dhost=testhost.abc.com dst=10.0.0.1
```

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

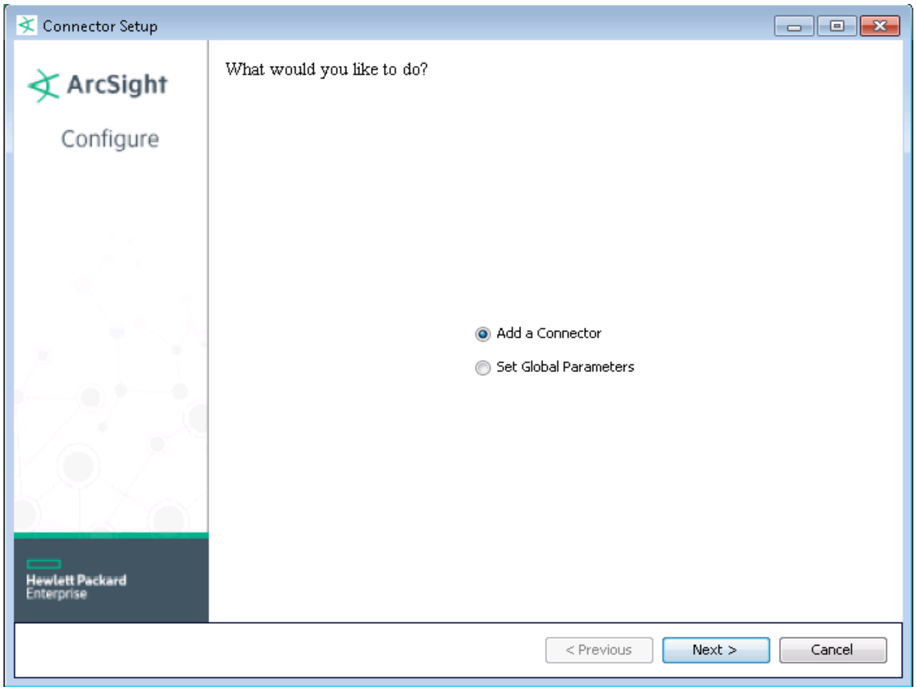
Install Core Software

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 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.

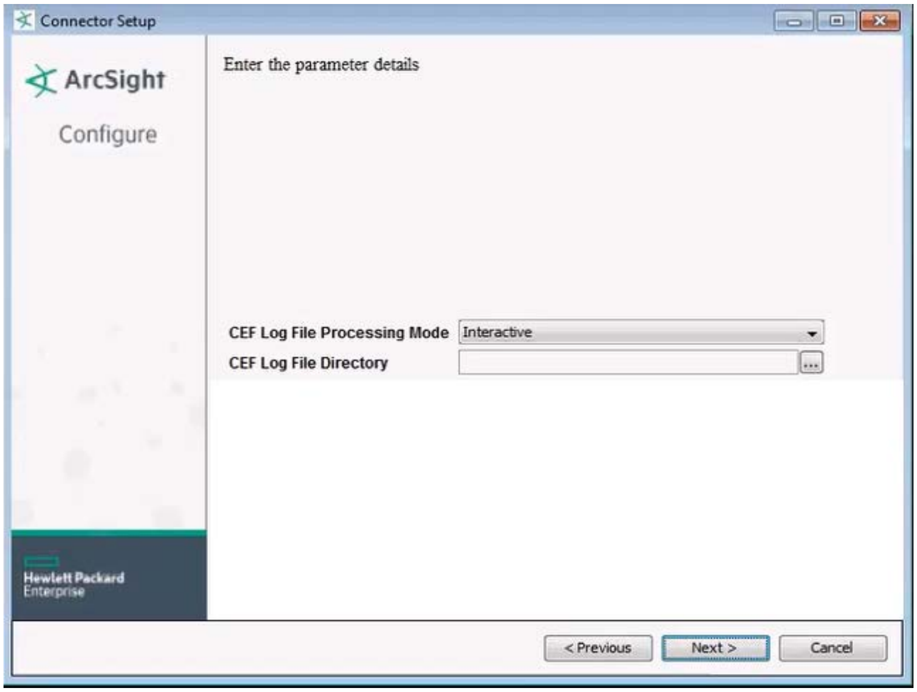
Parameter	Setting
Format Preserving Encryption	Data leaving the connector machine to a specified destination can be encrypted by selecting ‘Enabled’ to encrypt the fields identified in ‘Event Fields to Encrypt' before forwarding events. If encryption is enabled, it cannot be disabled. Changing any of 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.

Parameter	Setting
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 CEF Folder Follower Scanner** and click **Next**.
3. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



Enter the parameter details

CEF Log File Processing Mode: Interactive

CEF Log File Directory:

Parameter	Description
CEF Log File Processing Mode	Select 'Interactive' or 'Automatic'. When using ArcSight Management Center (ArcMC), only Automatic mode is supported.

Parameter	Description
	In Interactive mode, a graphical user interface shows the reports or log files available for import from the configured log directory. Choose reports to send to the connector by checking the box for 'Send' for individual log files and clicking 'Send to ArcSight.' Automatic mode is designed to be used in conjunction with an automated procedure to periodically run scans. A procedure, or shell script, should execute the scanner periodically and save a report in .cef format. At the end of the scan, after the report is saved, an empty file called '<reportname>.cef_ready' should be created, which indicates to the connector that the .cef report is ready for importing. The connector continues to search for .cef_ready files and process the corresponding .cef reports. The processed reports are renamed to '<original report file>.cef_processed'.
CEF Log File Directory	Enter the name of the directory containing the CEF log files. The log files containing the CEF events must be UTF-8 encoded.

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.

Device Event Mapping to ArcSight Data Fields

Information from vendors is formatted according to the CEF standard and sent to the ArcSight SmartConnector, which translates the data into an ArcSight event. Refer to vendor CEF documentation for device mappings for that vendor's product.