



ArcSight SmartConnectors

Software Version: 8.4.3

Configuration Guide for ArcSight CEF Folder Follower Scanner SmartConnector

Document Release Date: October 2023

Software Release Date: October 2023

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2017-2023 Open Text.

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Trademark Notices

“OpenText” and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

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>

Contents

Configuration Guide for ArcSight CEF Folder Follower Scanner SmartConnector 4

Product Overview 5

Common Event Format Implementation 6

Asset and Vulnerability Extraction 7

Preparing to install the SmartConnector10

Installing and Configuring the SmartConnector 11

Device Event Mapping to ArcSight Data Fields13

Send Documentation Feedback 14

Configuration Guide for ArcSight CEF Folder Follower Scanner SmartConnector

This guide provides information to install and configure the SmartConnector for ArcSight CEF Folder Follower Scanner.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight software and its environment.

Additional Documentation

The ArcSight SmartConnector documentation library includes the following resources:

- [Technical Requirements Guide for SmartConnector](#), which provides information about operating system, appliance, browser, and other support details for SmartConnector.
- [Installation and User Guide for SmartConnectors](#), which provides detailed information about installing SmartConnectors.
- [Configuration Guides for ArcSight SmartConnectors](#), which provides information about configuring SmartConnectors to collect events from different sources.
- [Configuration Guide for SmartConnector Load Balancer](#), which provides detailed information about installing Load Balancer.

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the [documentation site for ArcSight SmartConnectors 8.4](#).

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to MFI-Documentation-Feedback@opentext.com.

For specific product issues, [contact Open Text Support for Micro Focus products](#).

Product Overview

This connector collects and processes the Common Event Format (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).

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 on 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 allows ESM to connect, 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 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.

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 ESM.

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.

The guidelines that follow allow the connector framework to extract the asset and vulnerability information from CEF events in a consistent manner. 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, which is abbreviated as **dhost** is used to identify assets. The set of unique destination hosts or addresses identified in each set of events is collected by the connector framework.

The connector framework processes the following categories of information:

- open port
- URI
- 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.

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 such as 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	–
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	<VulnerabilityNativeIdentifier=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
```

Preparing to install the SmartConnector

Before you install any SmartConnectors, make sure that the OpenText 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. Specify the relevant [Global Parameters](#), when prompted.
4. Select **ArcSight CEF Folder Follower Scanner** from **Type** drop-down, then click **Next**.
5. Specify the following information:

Parameter	Description
CEF Log File Processing Mode	<p>Select any of the following options:</p> <p>Interactive: In Interactive mode, a graphical user interface displays the reports or log files available for import from the configured log directory. To send reports to the connector, select the Send check box for individual log files and then click Send to ArcSight.</p> <p>Automatic: The Automatic mode is designed to be used in conjunction with an automated procedure to periodically run scans. A procedure, or shell script, must 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' is 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'.</p> <p>Note: When using ArcSight Management Center (ArcMC), only Automatic mode is supported.</p>
CEF Log File Directory	Specify the name of the directory containing the CEF log files. The log files containing the CEF events must be UTF-8 encoded.

1. Select a [destination and configure parameters](#).
2. Specify a name for the connector.
3. (Conditional) 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 then click **Next**. The certificate is imported and the **Add connector Summary** window is displayed.



Note: If you select Do not import the certificate to connector from destination, the connector installation will end.

4. Select whether you want to install the connector as a service or in the standalone mode.
5. Complete the installation.
6. [Run the SmartConnector](#).

For instructions about upgrading the connector or modifying parameters, see [Installation and User Guide for SmartConnector](#).

Device Event Mapping to ArcSight Data Fields

For device mappings for a product, refer to the vendor CEF documentation.

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

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 Folder Follower Scanner SmartConnector (SmartConnectors 8.4.3)

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 MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!