



ArcSight SmartConnector

Software Version: 8.4.3

Configuration Guide for ArcSight Common Event Format File 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 2007 – 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 Common Event Format File SmartConnector 4

Product Overview 5

Common Event Format Implementation 6

Preparing to install the SmartConnector 7

8

Installing and Configuring the SmartConnector 9

Configuring Log Rotation 10

Device Event Mapping to ArcSight Data Fields11

Send Documentation Feedback 12

Configuration Guide for ArcSight Common Event Format File SmartConnector

This guide provides information to install the SmartConnector for ArcSight Common Event Format (CEF) File.

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

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 connector enables ArcSight ESM to connect, 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 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.

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 Common Event Format File** from **Type** drop-down, then click **Next**.
 5. Browse and select the CEF log filename in the **CEF Log File** field, to configure the SmartConnector, then click **Next**.
 6. Select a [destination and configure parameters](#).
 7. Specify a name for the connector.
 8. (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.
9. Select whether you want to install the connector as a service or in the standalone mode.
 10. Complete the installation.
 11. [Run the SmartConnector](#).

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

Configuring Log Rotation

To configure [Log Rotation](#), you can edit the agent.properties file after the installation of SmartConnector

1. Open the agent.properties file located at \$ARCSIGHT_HOME\current\user\agent.
2. To enable Daily log rotation, set rotationscheme to Daily, and set rotationschemeparams, as shown in the following example:

```
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
```

3. To enable Index 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,Optional true  
or false"
```

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

4. To enable Name Following log rotation, set followexternalrotation to true.
5. Save the file and restart the connector for your changes to take effect.

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.



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

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 Common Event Format File SmartConnector (SmartConnector 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!