Micro Focus Security ArcSight SmartConnectors

Software Version: 8.3.0

SmartConnector for ArcSight Common Event Format Multiple File

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.

Document Revision History

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.

To check for recent updates or to verify that you are using the most recent edition of a document, go to ArcSight Product Documentation Community on the Micro Focus Security Community.

Document Changes

Date	Product Version	Description
MM/DD/YYYY	X.X.X.X	Description of change

Contents

SmartConnector for ArcSight Common Event Format Multiple File

SmartConnector for ArcSight Common Event Format Multiple File

This guide provides information to the SmartConnector for ArcSight Common Event Format Multiple File and to configure the device for event collection. This SmartConnector is supported on the Microsoft Windows and Linux platform.

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.

SmartConnector for ArcSight Common Event Format Multiple File

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. Specify the relevant Global Parameters, when prompted.
4. Select **ArcSight Common Event Format Multiple File** from **Type** drop-down, then click **Next**.
5. Specify the following information:

Parameter	Description
Folder	The absolute path to the location of the log files. For example: • **On Windows:** c:\Program Files\CEF_Multi_File\logs\ • **On Linux: /var/log/cefmultifile/**
Wildcard	The log file name ('*.cef') has two parts: Part 1: ('*') is the file name Part 2: ('.cef') is the file type. For example: 'cefmulti.cef' See the section "Log Rotation - File Name Pattern" for details on log file rotation.

SmartConnector for ArcSight Common Event Format Multiple File

Parameter	Description
Log File Type	Select the appropriate option from the drop-down list: 'cef'. **NOTE:** To add additional log files, click **Add** again. You can change folder paths if required.

6. To export the host name data you have entered into the table into a CSV file click **Export**.
7. To select a CSV file to import into the table rather than add the data manually click **Import**..
8. Click **Next**. .
9. Select a destination and configure parameters.
10. Specify a name for the connector.
11. 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.
12. Select whether you want to run the connector as a service or in the standalone mode.
13. Complete the installation.
14. Run the SmartConnector.

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

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
```

SmartConnector for ArcSight Common Event Format Multiple File

3. To enable Index log rotation, set `rotationscheme` to Index, and set `rotationschemeparams`, as shown in the example below:

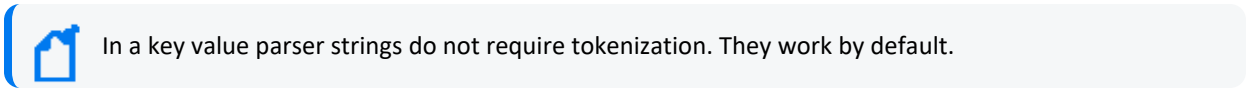
   ```
   agents[x].rotationscheme="Index"
     agents
   [x].rotationschemeparams="FilePrefix,FileSuffix,Digits,Count,Optional true
   or false"
   ```

   Where for a data file name of `foo.log.%03d,001,999,false`
4. 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.



SmartConnector for ArcSight Common Event Format Multiple File

SmartConnector for ArcSight Common Event Format Multiple File

This guide provides information to the SmartConnector for ArcSight Common Event Format Multiple File and to configure the device for event collection. This SmartConnector is supported on the Microsoft Windows and Linux platform.

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.

SmartConnector for ArcSight Common Event Format Multiple File

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. Specify the relevant Global Parameters, when prompted.
4. Select **ArcSight Common Event Format Multiple File** from **Type** drop-down, then click **Next**.
5. Specify the following information:

Parameter	Description
Folder	The absolute path to the location of the log files. For example: • **On Windows:** c:\Program Files\CEF_Multi_File\logs\ • **On Linux: /var/log/cefmultifile/**
Wildcard	The log file name ('*.cef') has two parts: Part 1: ('*') is the file name Part 2: ('.cef') is the file type. For example: 'cefmulti.cef' See the section "Log Rotation - File Name Pattern" for details on log file rotation.

SmartConnector for ArcSight Common Event Format Multiple File

Parameter	Description
Log File Type	Select the appropriate option from the drop-down list: 'cef'. **NOTE:** To add additional log files, click **Add** again. You can change folder paths if required.

6. To export the host name data you have entered into the table into a CSV file click **Export**.
7. To select a CSV file to import into the table rather than add the data manually click **Import**..
8. Click **Next**. .
9. Select a destination and configure parameters.
10. Specify a name for the connector.
11. 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.
12. Select whether you want to run the connector as a service or in the standalone mode.
13. Complete the installation.
14. Run the SmartConnector.

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

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
```

SmartConnector for ArcSight Common Event Format Multiple File

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"
```

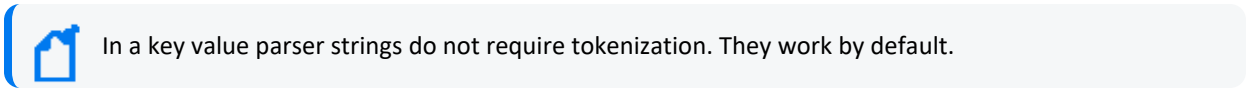
   Where for a data file name of `foo.log.%03d,001,999,false`

4. 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.



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 SmartConnector for ArcSight Common Event Format Multiple File (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!