



ArcSight SmartConnectors

Software Version: 8.4.3

Configuration Guide for ArcSight Common Event Format REST 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 2015 – 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 REST SmartConnector 4
- Product Overview 5
- Common Event Format Implementation 6
 - ArcSight Cloud CEF Implementation Standard 6
- Creating an OAuth2 Client Properties File 7
- Preparing to Install the SmartConnector 8
- Installing and Configuring the SmartConnector 9
- Device Event Mapping to ArcSight Data Fields11
- Troubleshooting12
- Send Documentation Feedback 13

Configuration Guide for ArcSight Common Event Format REST SmartConnector

This guide provides information to install and configure the SmartConnector for ArcSight Common Event Format (CEF) REST for event collection.

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 SmartConnector for ArcSight CEF REST provides a configurable method to collect security events when you use cloud-based applications such as Salesforce or Google Apps. SmartConnector allows 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.

ArcSight Cloud CEF Implementation Standard

The ArcSight Cloud CEF Implementation Standard specifies the additional requirements needed for event retrieval, transport, and security of cloud-based logs, thereby providing a means by which cloud-based service providers can integrate with ArcSight's industry-leading log collection technology. For more information, see [Implementing ArcSight Cloud CEF Implementation Standard](#).

Creating an OAuth2 Client Properties File

To register your connector application and to create authentication properties files, refer to the vendor CEF documentation.

When using OAuth2 authentication, create an OAuth2 Client Properties file for each vendor from which you want to collect events. The properties file that are stored in the local drive can contain the vendors' names to help you identify the properties files.

For example, an OAuth2 Client Properties file for Google can be named `googleclient.properties`. The file can reside on your local drive. Make a note of the configuration file name as you will need to specify during the SmartConnector installation.

Use the following template to create the OAuth2 Client properties file:

```
client_id=<your client id>
client_secret=<your client secret>
redirect_uri=https://localhost:<port-number>/<path>
auth_url=<available from cloud service provider>
token_url=<available from cloud service provider>
scope=<scope>
```

The following table describes the parameters and expected values in the OAuth2 Client properties file.

Parameter	Description
client_id	The value provided by the vendor when you register an application.
client_secret	The value provided by the vendor when you register an application. This value is obfuscated.
redirect_uri	<p>Specify this URL when you register the application with the vendor. Connector supports both http and https schemes and it must be redirected to the unused port of the localhost so that the authorization code can be captured automatically after you authenticate your identity with the vendor. For an HTTPS connection, it shares the connector's default self-signed certificate, <code>remote-management.p12</code>, located in the <code>user/agent</code> directory.</p> <p>The <code>redirect_uri</code> must be in the following format: <code>https://localhost:<port>/<path></code>. <code><port></code> can be configured to any free port.</p> <p>For example, <code>https://localhost:8081/oauth2callback</code></p>
auth_url	The URL of the vendor to which the initial request needs to be made to get an authorization code. Refer to the vendor documentation to get this URL.
token_url	The URL of the vendor to which the request to get an Access Token needs to be made. Refer to the vendor documentation to get this URL.
scope	Scope indicates the type of information to be retrieved from the vendor on behalf of the user. If there is more than one scope, you can specify these as a space-separated list of values. Although this parameter is optional, it is recommended to specify a value for scope.



Notes:

- The SmartConnector cannot be run as a service when using OAuth2 as the authentication method.
- The access token is initially obtained during the configuration phase and will be used when retrieving the events while the connector is running. Because OAuth2 gives an application temporary access permission, the access token will expire after a period of time and must be refreshed.
- After successful authentication, the OAuth2 Client Properties access tokens and refresh tokens are persisted in the `agent.properties` file. Tokens and secrets are obfuscated.

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, be sure 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 a syslog connector from **Type** drop-down, then click **Next**.

Because all syslog SmartConnectors are sub-connectors of the main syslog SmartConnector, the name of the specific syslog SmartConnector you are installing is not required during installation.

5. Specify the following information:

Parameter	Description
Proxy Host	Enter the proxy host IP address or name. This value is required for proxy configuration for access.
Proxy Port	Enter the proxy port. This value is required for proxy configuration.
Proxy User Name	Enter the proxy user name. This value is optional for additional proxy authentication. If you specify a proxy user name, you must also specify a proxy password.
Proxy Password	Enter the password for the proxy user specified in the Proxy User Name field. This value is optional for additional proxy authentication. This field is required only if you have specified a proxy user name.
Events URL	Enter the events URL. This is the REST API endpoint which is used by the connector to get the events.
Authentication Type	The type of authentication required by the service at Events URL. The options are: Basic and OAuth2
User Name	For Basic authentication, enter the User Name.
Password	For Basic authentication, enter the Password.
OAuth2 Client Properties File	For OAuth2 authentication browse for the OAuth2 Client Properties File. You should have created this file from values you obtained when you registered your connector application, and acquired a redirect_uri. Create a unique OAuth2 Client Properties File for each vendor from which you want to collect events. (See "Create an OAuth2 Client Properties File" in the Configuration section of this guide for more information.)
Refresh Token	Enter the refresh token; applies only to users running the SmartConnector in the Connector Appliance environment. If you are installing the connector in a Connector Appliance environment, see the ArcSight Connector Appliance Administrator's Guide. Other users, leave this field blank.

If you do not need a proxy to access the Internet, then leave the proxy fields blank and 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](#).

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.

Troubleshooting

SmartConnector Throws An Out Of Memory Error

The SmartConnector throws an out of memory error if the `startTime` mentioned in the Events URL (such as `https://api.seculert.com/1.1/alerts/cef-events?startTime=2016-01-07T15:22:16.000`) is very old.

To rectify this, do the following:

When the SmartConnector is running in standalone mode:

- **For Windows:** Create the batch file `$ARCSIGHT_HOME\current\user\agent\setmem.bat` with the following content:
`SET ARCSIGHT_MEM_OPTIONS= -Xms1024m -Xmx2048m`
- **For Linux:** Create the executable shell script `~/ARCSIGHT_HOME/current/user/agent/setmem.sh` with the following content:

```
ARCSIGHT_MEMORY_OPTIONS="-Xms1024m -Xmx2048m"
```

When the SmartConnector is running as a service:

- Set `wrapper.java.initmemory` and `wrapper.java.maxmemory` values in the file `$ARCSIGHT_HOME\current\user\agent\agent.wrapper.conf`

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 REST 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!