



Micro Focus Security ArcSight Connectors

SmartConnector for ArcSight Common Event Format REST

Configuration Guide

June, 2018

Configuration Guide

SmartConnector for ArcSight Common Event Format REST

June, 2018

Copyright © 2015 – 2017; 2020 Micro Focus or one of its affiliates.

Legal Notices

Micro Focus

The Lawn

22-30 Old Bath Road

Newbury, Berkshire RG14 1QN

UK

<https://www.microfocus.com>.

Confidential computer software. Valid license from Micro Focus required for possession, use or copying. The information contained herein is subject to change without notice.

The only warranties for Micro Focus products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein.

No portion of this product's documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's internal use, without the express written permission of Micro Focus.

Notwithstanding anything to the contrary in your license agreement for Micro Focus ArcSight software, you may reverse engineer and modify certain open source components of the software in accordance with the license terms for those particular components. See below for the applicable terms.

U.S. Governmental Rights. For purposes of your license to Micro Focus ArcSight software, “commercial computer software” is defined at FAR 2.101. If acquired by or on behalf of a civilian agency, the U.S. Government acquires this commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of the Agreement as specified in 48 C.F.R. 12.212 (Computer Software) and 12.211 (Technical Data) of the Federal Acquisition Regulation (“FAR”) and its successors. If acquired by or on behalf of any agency within the Department of Defense (“DOD”), the U.S. Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of the Agreement as specified in 48 C.F.R. 227.7202- 3 of the DOD FAR Supplement (“DFARS”) and its successors. This U.S. Government Rights Section 18.11 is in lieu of, and supersedes, any other FAR, DFARS, or other clause or provision that addresses government rights in computer software or technical data.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

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://community.microfocus.com/t5/ArcSight-Product-Documentation/ct-p/productdocs>

Revision History

Date	Description
10/17/2017	Added encryption parameters to Global Parameters.
08/15/2017	Updated link to CEF Implementation Standard.
04/15/2017	Updated troubleshooting information for out of memory error.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
05/16/2016	General availability of this connector. Added overview information about Common Event Format standards.
02/15/2016	Added troubleshooting information regarding out of memory error.
08/14/2015	Added configuration information for creating OAuth2 Client Properties File.
06/30/2015	First edition for beta release of this connector.

SmartConnector for ArcSight Common Event Format REST

This guide provides information for configuring the SmartConnector for ArcSight Common Event Format REST for event collection.

Product Overview

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 SmartConnector for ArcSight Common Event Format REST provides a configurable method to collect security events when you use cloud-based applications such as Salesforce or Google Apps. The connector lets ArcSight ESM connect to, 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.

ArcSight Common Event Format Standards

Implementing ArcSight Common Event Format (CEF)

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 as well as supported date formats.

To access this standard, go to <https://community.microfocus.com/t5/ArcSight-Connectors/ArcSight-Common-Event-Format-CEF-Implementation-Standard/ta-p/1645557>.

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. To access this standard, go to

<https://community.microfocus.com/t5/ArcSight-Connectors/Cloud-CEF-Implementation-Standard/ta-p/1589220>

Configuration

See the vendor CEF documentation for registering your connector application and creating authentication properties files.

Create an OAuth2 Client Properties File

When using OAuth2 authentication, create an OAuth2 Client Properties file for each vendor from which you want to collect events. You can name the file to contain the vendor's name to help you keep track of your properties files. For example, an OAuth2 Client Properties file for the vendor Google could be named `googleclient.properties`. The file can reside on your local drive. You later browse for this file to add it to the `OAuth2 Client Properties File` parameter during connector configuration.

This is a template for 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
<code>client_id</code>	This value is provided by the vendor when you register an application.
<code>client_secret</code>	This value is also provided by the vendor when you register an application. This value is obfuscated.
<code>redirect_uri</code>	<p>This is the URL to which the vendor sends the authorization code, which you configure when you register an application. The <code>redirect_uri</code> must be on the local host. Both http and https schemes are supported. This URL should be of the form <code>https://localhost:<port>/<path></code>.</p> <p>The <code><port></code> in this URL can be configured to any free port.</p> <p>For example <code>https://localhost:8081/oauth2callback</code></p> <p>Specify this URL when you register the application with the vendor. The connector will allow two schemes, http or https, 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>
<code>auth_url</code>	This is the URL of the vendor to which the initial request needs to be made to get an authorization code. Consult vendor documentation to get this URL.
<code>token_url</code>	This is the URL of the vendor to which the request to get an Access Token needs to be made. Consult vendor documentation to get this URL.

Parameter	Description
scope	Scope lets applications inform you and the vendor what type of information is 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 specifying a value for this parameter is optional, the scope parameter must be specified.

Notes

- When using OAuth2 as the authentication method, the connector cannot be run as a service.
- 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.

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 Micro Focus SSO and Protect 724 sites.

- 1 Download the SmartConnector executable for your operating system from the Micro Focus 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

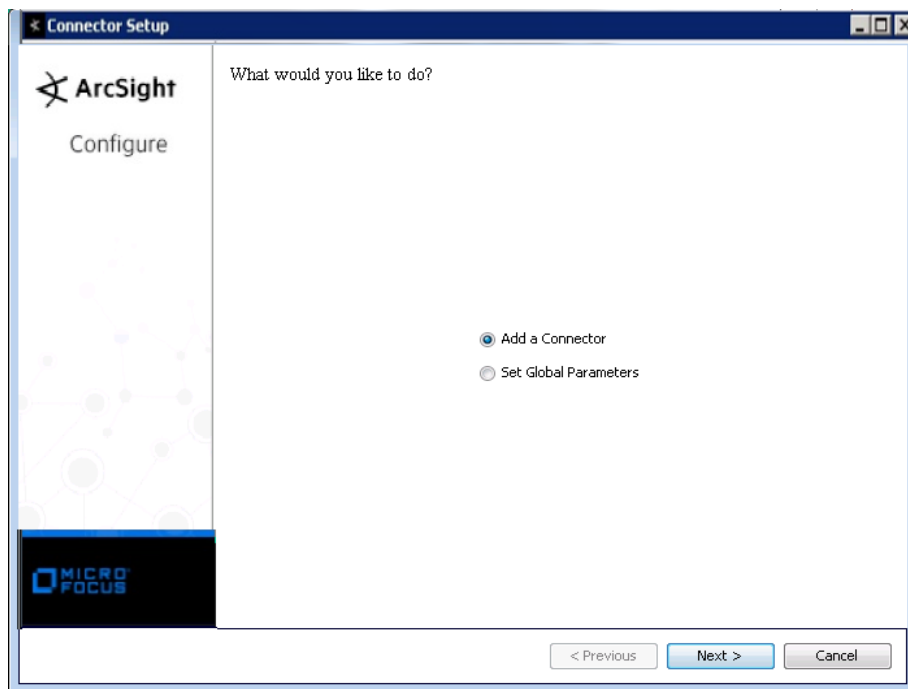
Choose Install Folder

Choose Shortcut Folder

Pre-Installation Summary

Installing...

- 3 When the installation of SmartConnector core component software is finished, the following window is displayed:



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'.

Parameter	Setting
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 Micro Focus SecureData solutions to provide encryption. See the *Micro Focus 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 Micro Focus 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.
Format Preserving Identity	The Micro Focus 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 Micro Focus SecureData.
Format Preserving Secret	Enter the secret configured for Micro Focus 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 Common Event Format REST and click Next.
- 3 Enter the required SmartConnector parameters to configure the SmartConnector, then click Next.

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, leave the proxy fields blank and click Next.

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.



When using OAuth2 authentication, the connector cannot be run as a service.

- 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

See the vendor CEF documentation for device mappings for that vendor's product. 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

Why does the connector throw 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 too old, a very large set of events is collected. The connector throws an out of memory error in this case.

To correct this problem when running as standalone:

■ For Windows:

Create the following batch file:

`$ARCSIGHT_HOME\current\user\agent\setmem.bat` with the following content: `SET ARCSIGHT_MEM_OPTIONS= -Xms1024m -Xmx2048m`

■ For Linux:

Create the following shell script and be sure it is executable

`~/ARCSIGHT_HOME/current/user/agent/setmem.sh` with the following content: `ARCSIGHT_MEMORY_OPTIONS="-Xms1024m -Xmx2048m"`

To correct this problem when running as a service:

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