



Micro Focus Security ArcSight Connectors

SmartConnector for ArcSight CEF Encrypted Syslog (UDP)

Configuration Guide

December 3, 2020

Configuration Guide

SmartConnector for ArcSight CEF Encrypted Syslog (UDP)

December 3, 2020

Copyright © 2011 – 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 |
|------------|---------------------------------------------------------------------------------------------|
| 12/03/2020 | Added a new section "Upgrading to the new AES-GCM Data Encryption Scheme". |
| 12/03/2020 | Added encryption parameters to Global Parameters. |
| 10/17/2017 | Added encryption parameters to Global Parameters. |
| 08/15/2017 | Updated link to CEF Implementation Standard. |
| 11/30/2016 | Updated installation procedure for setting preferred IP address mode. |
| 05/16/2016 | Added overview information about the CEF Implementation Standard. |
| 11/17/2015 | Added algorithm used for encryption. |
| 08/15/2014 | Removed device event mappings to ArcSight fields with referral to vendor CEF documentation. |
| 02/14/2014 | Updated parameter screen image. |

SmartConnector for ArcSight CEF Encrypted Syslog (UDP)

This guide provides information for installing and running the SmartConnector for ArcSight CEF Encrypted Syslog (UDP). This connector allows for connector-to-connector communication through an encrypted channel by decrypting events previously encrypted through the CEF Encrypted Syslog (UDP) destination. The encryption method is AES with a 128-bit key. See the *SmartConnector User's Guide*, "CEF Encrypted Syslog (UDP)," for more information about encrypting events.

Product Overview

CEF is an extensible, text-based, high-performance format designed to support multiple device types from both security and non-security devices and applications in the most simple manner possible, unlike other standards that target a single component of the security infrastructure, are tied to a specific transport protocol, or are designed specifically for applications and cannot support today's high-performance, real-time security requirements.

Each security infrastructure component tends to have its own event format, making it difficult to derive and understand the impact of certain events or combinations of events. ArcSight's Common Event Format (CEF) defines a very simple event format that can be adopted by vendors of both security and non-security devices. This format contains the most relevant event information.

The CEF SmartConnectors let ArcSight ESM connect to, aggregate, filter, correlate, and analyze events from applications and devices that deliver their logs in the CEF standard, using the syslog transport protocol.

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 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>.

Configuration

The SmartConnector is a syslogd-compatible daemon that implements a UDP receiver on the port you identify during connector installation to receive syslog events. Simply start the connector, either as a service or as a process, to start receiving events; no further configuration is needed.

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.

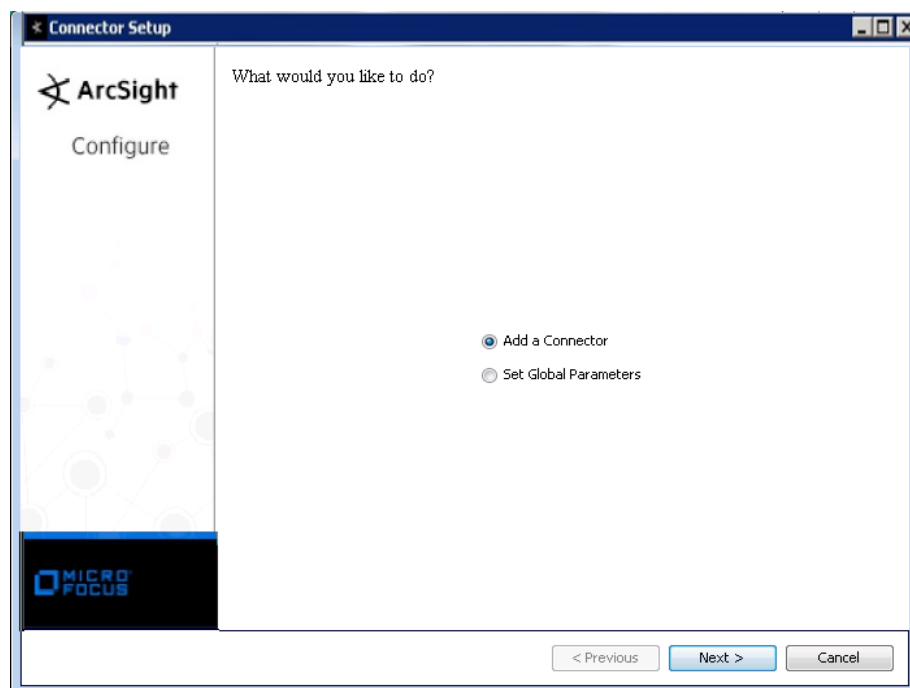
Follow the wizard through the following folder selection tasks and installation of the core connector software:

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'. |
| 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 |
|-----------|---------|
|-----------|---------|

| 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 CEF Encrypted Syslog (UDP)** and click **Next**.
- 3 Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.

Connector Setup

ArcSight
Configure

Enter the parameter details

Network Port: 514

IP Address: (ALL)

Shared Key (16 Characters):

< Previous Next > Cancel

| Parameter | Description |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Network Port | Enter the port on which the SmartConnector will listen for syslog events. Enter the same port you configured for the CEF Encrypted Syslog (UDP) destination when you configured the source connector. |
| IP Address | Enter the IP address to which the SmartConnector will listen for syslog events. |
| Shared Key (16 Characters) | The Shared Key is used to decrypt the data previously encrypted through the CEF Encrypted Syslog (UDP) destination. Enter the same 16-character shared key you entered when configuring the CEF Encrypted Syslog (UDP) destination. See the SmartConnector User's Guide, "CEF Encrypted Syslog (UDP)," for more information. |

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**.
- 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*.

Upgrading to the new AES-GCM Data Encryption Scheme

From 8.1.0 and on, connectors use a new AES-GCM data encryption scheme which replaces AES-CBC. If you cannot use a newer connector as the source, follow the steps below to change the encryption scheme back to AES-CBC:

- 1 Go to `$ARCSIGHT_HOME$\current\user\agent\agent.properties`
- 2 Change `agents[x].encryptionScheme=AES-GCM` to `agents[x].encryptionScheme=AES-CBC`
- 3 Save the `agent.properties` file.

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

Refer to 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.
