Micro Focus Security ArcSight SmartConnectors

Software Version: 8.3.0

Configuration Guide for ArcSight CEF Encrypted Syslog (UDP) SmartConnector

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://www.microfocus.com/documentation/arcsight/

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.

Contents

Configuration Guide for SmartConnector for ArcSight CEF Encrypted Syslog (UDP)

This guide provides information to install and run 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. For more information about encrypting events, see CEF Encrypted Syslog (UDP).

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. It is unlike other standards that target a single component of the security infrastructure and 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 to connect, 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 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.

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. The connector starts receiving events when you start the connector either as a service or as a process. No other configuration is needed.

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

The installation steps described in this section are specific to the SmartConnector for ArcSight CEF Encrypted Syslog (UDP). For detailed installation steps or for manual installation steps, see SmartConnector Installation and User Guide.

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. From the **Type** drop-down list, select **ArcSight CEF Encrypted Syslog (UDP)** as the type of connector, then click **Next**.
5. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.

Parameter	Description
Network Port	Enter the port on which the SmartConnector must 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 must 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. For more information, see CEF Encrypted Syslog (UDP).

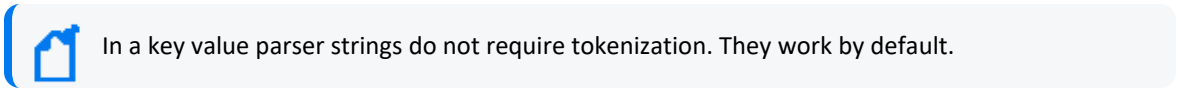
6. Select a destination and configure parameters.
7. Specify a name for the connector.
8. If you have selected ArcSight Manager as the destination, the certificate import window for the ArcSight Manager is displayed. Select **Import the certificate to the connector from destination** and click **Next**. (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.
9. Select whether you want to run 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 SmartConnector Installation and User Guide.

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.

Installing the SmartConnector

The following sections provide instructions for installing and configuring the ArcSight CEF Encrypted Syslog (UDP) SmartConnector.

Preparing to Install Connector

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* guide, available on ArcSight Documentation.

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 from step 3.

Before installing the SmartConnector, ensure that you have the following:

- Local access to the machine where the SmartConnector is to be installed
- Administrator passwords

Installing and Configuring the SmartConnector by Using the Wizard

The installation steps described in this section are specific to the ArcSight CEF Encrypted Syslog (UDP) Connector. For detailed installation steps or for manual installation steps, see SmartConnector Installation and User Guide.

To install and configure the ArcSight CEF Encrypted Syslog (UDP) Connector:

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. From the **Type** drop-down list, select **ArcSight CEF Encrypted Syslog (UDP)** as the type of connector, then click **Next**.

5. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.

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.

6. Select a destination and configure parameters.
7. Specify a name for the connector.
8. Select whether you want to run the connector as a service or in the standalone mode.
9. Complete the installation.
10. Run the SmartConnector.

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

When using Windows authentication, after completing the connector installation, if running on a Windows Server, change the service account to use the Windows account that should log in to the database. The connector will use the account used to start the service, regardless of the account value setting entered in the connector setup process.

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 CEF Encrypted Syslog (UDP) SmartConnector (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!