Micro Focus Security ArcSight SmartConnector

Software Version: 8.3.0

Configuration Guide for SmartConnector for Raw Syslog

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.

Configuration Guide for ArcSight SmartConnector for Raw Syslog

This guide provides information to install the SmartConnector for Raw Syslog Daemon and configure the device for event collection.

Product Overview

Although normalized data is faster and easier to parse and access, many IT professionals prefer having the raw data available for review, forensics, and litigation. In conjunction with the Raw Syslog connector destination, the SmartConnector for Raw Syslog Daemon lets you extract and collect raw syslog events from syslog servers using the TLS, Raw TCP, or UDP protocols.

Because this connector neither parses nor processes the raw syslog data, there are no mappings to ArcSight fields.

If you are transporting data to ArcSight Logger, you can use specific configuration parameters to provide minimal normalization of the syslog data (for source and timestamp).

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 **Raw Syslog Daemon** and click **Next**.
5. Specify the required SmartConnector parameters to configure the SmartConnector, then click **Next**.

Parameter	Description
Network Port	Specify the port on which the connector must listen for syslog events. The default port is 514.
IP Address	Specify the IP address of the device to which the connector is to listen exclusively, or accept the default value of (ALL) to bind to all available IP addresses.
Protocol	Select UDP, Raw TCP, or TLS as the protocol to be used by the connector to receive incoming messages. The default value is UDP.
Metadata Capture Level	Use if metadata (for source and timestamp) will be included in the outgoing messages to ArcSight Logger. The default value is None. Leave the default, if you do not require metadata be sent to ArcSight Logger. Else, select one of these options: **Simple:** Uses the current machine timestamp and the IP address of the source of the event. No parsing occurs. **Header:** Uses the timestamp and source information from the event message header. If that data cannot be derived, then the connector uses the Simple option. **Custom:** Uses the regular expressions provided in the Custom Regex to Capture Source and the Custom Regex to Capture Timestamp fields. If you specify a Metadata Capture Level of Custom, you must use at least one of these fields.
Custom Regex to Capture Source	Custom regular expression to capture source; the capturing group indicates the location of the source IP or host name. This regular expression needs to match the entire raw syslog event, and have at least one capturing group, which tells the connector how to find the source address. For example, this regular expression would find everything between the words “before” and “after:” .*?before(.*)after.* For the following event, that regular expression would capture the IP address 192.168.1.2: Hello there before192.168.1.2after and goodbye
Custom Regex to Capture Timestamp	Custom regular expression to capture timestamp; the capturing group indicates the location of the timestamp. Uses the parsing for the __parseMutableTimeStampSilently token operation. See the ArcSight FlexConnector Developer’s Guide for details on token operations.

6. Select **Raw Syslog** as destination and click **Next**.
7. Specify the following destination values, then click **Next**.

Parameter	Description
IP/Host	Enter the IP address or host name to which the connector is to send events.
Port	Specify the port to which the connector is to send events.
Protocol	Select either UDP, Raw TCP, or TLS as the protocol to be used by the connector to send events. The default value is UDP
Enable Metadata For Logger	If you select true, metadata about the source and timestamp is included in the outgoing message for ArcSight Logger. Select this option if you previously selected a level other than **None** for the **Metadata Capture Level** parameter.

8. Specify a name for the SmartConnector, then click **Next**.
9. Review the Add Connector Summary and click **Next**.
10. Specify whether you want to run the SmartConnector as a stand-alone process or as a service.
11. To complete the installation, choose **Exit** and click **Next**.
12. Run the smartconnector.

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 SmartConnector for Raw Syslog (SmartConnector 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!