Micro Focus Security ArcSight Micro Focus Security ArcSight Connectors

Software Version: 8.3.0

SmartConnector for Syslog NG Daemon

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

Contents

Configuration Guide for Syslog NG Daemon SmartConnector

This guide provides information for installing the SmartConnector for Syslog NG Daemon and configuring the device for event collection.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight SmartConnectors.

Additional Documentation

The ArcSight SmartConnectors documentation library includes the following resources:

- *Installation Guide for ArcSight 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.
- *Release Notes for ArcSight SmartConnectors*, which provides information about the latest release

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the documentation site for ArcSight SmartConnectors.

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 Documentation-Feedback@microfocus.com.

For specific product issues, contact Micro Focus Customer Care.

Product Overview

The Syslog NG application is an open source implementation of the syslog protocol for UNIX and UNIX-like systems, extending the original syslogd model and adding important features to syslog, such as using Transport Layer Security (TLS) to encrypt communication and support for IETF Standard (RFC 5424) syslog header.

TLS uses certificates to authenticate and encrypt the communication. The client authenticates the server by requesting its certificate. Optionally, the server can also request a certificate from the client. See "Add TLS Function to the Syslog NG Setup" for more information.

This SmartConnector is capable of receiving events over a secure TLS channel from another SmartConnector (whose destination is configured as CEF Syslog over TLS).

For a list of all mappings supported for all syslog SmartConnectors, see the *SmartConnector Configuration Guide for UNIX OS Syslog*.

Configuration

For information on how to configure Syslog NG, see the *syslog-ng Open Source Administrator Guide*.

Installing the SmartConnector

The following sections provide instructions for installing and configuring your selected SmartConnector.

When installing the syslog daemon connector in a UNIX environment, run the executable as 'root' user.

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 **Syslog NG Daemon** from the **Type** drop-down list and click **Next**.
5. Enter the following SmartConnector parameters to configure the SmartConnector, then click **Next**.

Parameter	Description
Network Port	Specify the port to which the connector is to listen for Syslog NG events. This is generally port 1999 for Syslog NG.
IP Address	Enter the IP address for the device that is receiving the events and to which the connector is to listen exclusively. Accept the default value of (ALL) to bind to all available IP addresses.
Protocol	Select either UDP, TLS or Raw TCP. The default value is TLS. The SmartConnector for Syslog NG Daemon uses the selected protocol to receive incoming messages.
Forwarder	Change this parameter to 'true' only if the events being processed are coming from another SmartConnector sending to a CEF Syslog destination, and that destination also has CEF forwarder mode enabled. That allows attributes of the original connector to be retained in the original agent fields.
IETF Standard (RFC 5424) Enabled	Select 'true' to enable IETF Standard (RFC 5424); otherwise, leave the default value of 'false'. The Syslog NG connector by default expects the events to be in BSD format, which the syslog connector supports. If the parameter is set to 'true', the connector expects the events to have the IETF Standard (RFC 5424) syslog header.

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.

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 SmartConnector for Syslog NG Daemon (Micro Focus Security ArcSight Connectors 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!