
Micro Focus Security

ArcSight Micro Focus Security

Software Version: 8.2.2

SmartConnector for Symantec Endpoint Protection Syslog

Document Release Date: October 2021

Software Release Date: October 2021



Legal Notices

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

<https://www.microfocus.com>

Copyright Notice

© Copyright 2010 – 2021 Micro Focus or one of its affiliates

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://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

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

- SmartConnector for Symantec Endpoint Protection 5
 - Product Overview 5
- Configuration 6
 - Configuring the Syslog SmartConnectors 6
 - The Syslog Daemon SmartConnector 6
 - The Syslog Pipe and File SmartConnectors 7
 - Configuring the Syslog Pipe or File SmartConnector 7
- Installing the SmartConnector 9
 - Installing Syslog 9
 - Preparing to Install Connector 9
 - Installing and Configuring the SmartConnector by Using the Wizard10
- Device Event Mapping to ArcSight Fields14
 - Symantec Endpoint Protection Syslog Mappings to ArcSight ESM Fields14
- Send Documentation Feedback 16

SmartConnector for Symantec Endpoint Protection

This guide provides information about installing the SmartConnector for Symantec Endpoint Protection DB and configuring the device for event collection. Symantec Endpoint Protection version 12.1 (for Anti-Virus, Anti-Spyware, Network Threat Protection (including firewall events), Network Access Control, and Behavior events) and 14.0 (for Scan, Server Admin Log, Network Threat Protection, Behavior, System Anti-Virus and Anti-Spyware Protection, Virus, and Server Policy events) are supported. The Symantec Endpoint Protection Small Business Edition v12.1 is also supported.

Product Overview

Symantec Endpoint Protection combines Symantec AntiVirus with advanced threat prevention for defense against malware for laptops, desktops, and servers. It integrates its security technologies in a single agent and management console. The ArcSight SmartConnector lets you import events generated by the device into the ArcSight System.

Configuration

For minimum and default system logging configuration, including configuration statements and examples, visit <https://support.symantec.com/us/en/article.HOWTO81169.html> and see "Exporting data to a Syslog server" in the *Symantec Endpoint ProtectionSystem Log Messages Reference* manual for your installed version.



Note: When the device is set up with CFEB (a router forwarding events to the connector from all devices), the hostname in syslog events is always the router name **cfeb**. This makes it impossible to identify the original device from the parsed event.

Configuring the Syslog SmartConnectors

The types of ArcSight Syslog SmartConnectors are:

- Syslog Daemon
- Syslog Pipe
- Syslog File

The Syslog Daemon SmartConnector

The Syslog Daemon SmartConnector is a syslogd-compatible daemon designed to work in operating systems that have no syslog daemon in their default configuration, such as Microsoft Windows. The SmartConnector for Syslog Daemon implements a UDP receiver on port 514 (configurable) by default that can be used to receive syslog events. Use of the TCP protocol or a different port can be configured manually.

If you are using SmartConnector for Syslog Daemon, add the following statement in the `rsyslog.conf` file to forward device events so that Syslog Daemon will start receiving events: `*.* @@(remote/local-host-IP):514`

Sample example: `local1.warning @@10.0.0.1:514`



Note: You can either use `*.*` to read all Syslog events or you can filter specific events by replacing regex with the specific event name. For example: `*.* @@(remote/local-host-IP):514` and `local1.warning @@10.0.0.1:514`



Note: Use @@ to send events over a TCP connection and use @ to send events over an UDP connection.

If you are running SmartConnector for Syslog Daemon on the same machine, you must provide the IP address of the local host. If you want to forward events to other machines, you must provide the IP address of the same.



Note: Messages longer than 1024 bytes may be split into multiple messages on syslog daemon; no such restriction exists on syslog file or pipe.

The Syslog Pipe and File SmartConnectors

When a syslog daemon is already in place and configured to receive syslog messages, an extra line in the syslog configuration file (`rsyslog.conf`) can be added to write the events to either a *file* or a system *pipe* and the ArcSight SmartConnector can be configured to read the events from it. **In this scenario, the ArcSight SmartConnector runs on the same machine as the syslog daemon. Therefore, you must do additional configurations for the ArcSight syslog file or syslog pipe SmartConnectors in the system where all Syslog Daemon SmartConnector configurations are done.**

The **Syslog Pipe** SmartConnector is designed to work with an existing syslog daemon. This SmartConnector is especially useful when storage is a factor. In this case, `syslogd` is configured to write to a named pipe, and the Syslog Pipe SmartConnector reads from it to receive events.

The **Syslog File** SmartConnector is similar to the Pipe SmartConnector; however, this SmartConnector monitors events written to a syslog file (such as `messages.log`) rather than to a system pipe.

Configuring the Syslog Pipe or File SmartConnector

This section provides information about how to set up your existing syslog infrastructure to send events to the ArcSight Syslog Pipe or File SmartConnector.

The standard UNIX implementation of a syslog daemon reads the configuration parameters from the `/etc/rsyslog.conf` file, which contains specific details about which events to write to files, write to pipes, or send to another host. First, create a pipe or a file; then modify the `/etc/rsyslog.conf` file to send events to it.

For syslog pipe:

1. Create a pipe by executing the following command: `mkfifo /var/tmp/syspipe`
2. Add any of the following line to your **/etc/rsyslog.conf** file based on the operating system:
 - `*.debug /var/tmp/syspipe`
 - `*.debug |/var/tmp/syspipe`
3. After modifying the file, restart Syslog Daemon either by executing the scripts **/etc/init.d/syslogd stop** and **/etc/init.d/syslogd start**, or by sending a `configuration restart` signal.
 - On RedHat Linux, execute: `service syslog restart`
 - On Solaris, execute: `kill -HUP `cat /var/run/syslog.pid``

This command forces Syslog Daemon to reload the configuration and start writing to the pipe you just created.

For syslog file:

1. Create a file or use the default for the file into which log messages are to be written.
2. After editing the `/etc/rsyslog.conf` file, ensure to restart the syslog daemon as described above.
3. When you follow the SmartConnector Installation Wizard, you will be prompted for the absolute path to the syslog file or pipe you created.

Installing the SmartConnector

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

Installing Syslog

Install this SmartConnector (on the syslog server or servers identified in the Configuration section) using the SmartConnector Installation Wizard appropriate for your operating system. The wizard will guide you through the installation process. When prompted, select one of the following Syslog connectors (see Configure the Syslog SmartConnectors in this guide for more information):

- Syslog Daemon
- Syslog Pipe
- Syslog File

Because all Syslog SmartConnectors are sub-connectors of the main syslog SmartConnector, the name of the specific Syslog SmartConnector you are installing is not required during installation.

The Syslog Daemon connector listens on port 514 (configurable) for UDP syslog events by default. You can configure the port number or use the TCP protocol manually. The Syslog Pipe and Syslog File connectors read events from a system pipe and file, respectively. You can select the appropriate connector as per the Syslog infrastructure setup.

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.

Start the installation procedure from step 3.

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 by Using the Wizard

The installation steps described in this section are specific to the Symantec Endpoint Protection Syslog Connector. For detailed installation steps or for manual installation steps, see SmartConnector Installation and User Guide.

To install and configure the Symantec Endpoint Protection Syslog Connector:



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

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 a Syslog Deamon or Syslog File connector from the **Type** drop-down, then click **Next**.

Because all syslog SmartConnectors are sub-connectors of the main syslog SmartConnector, a specific name is not required during installation.

5. Specify the following information depending on the type SmartConnector that you are installing:

For Syslog Deamon, specify the following parameters:

Syslog Daemon Parameters	Network port	The SmartConnector for Syslog Daemon listens for syslog events from this port.
	IP Address	The SmartConnector for Syslog Daemon listens for syslog events only from this IP address, apart from the default (ALL) to bind to all available IP addresses.

	Reading Events Real Time or Batch	Specify whether to read files in batch mode or real-time mode. In batch mode, all files are read from the beginning.
	Action Upon Reaching EOF	This option applies to Batch Mode only. Specify None , Rename , or Delete as the action to be performed to the file when the connector finishes reading and reaches end of file . For the real-time mode, retain the default value None .
	File Extension If Rename Action	This option applies to Batch Mode only. Specify the extension to be added to the file name if the action on reaching the end of file is specified as Rename . The default value is Processed , which adds a <code>.processed</code> extension.

For Syslog File Type, specify the following parameters:

Syslog Pipe Parameter	Pipe Absolute Path Name	Specify an absolute path to the pipe, or accept the default value: <code>/var/tmp/syspipe</code> .
Syslog File Parameters	File Absolute Path Name	<p>Specify the full path name for the file from which this connector will read events. The following are default values:</p> <ul style="list-style-type: none"> • Solaris: <code>\var\adm\messages</code> • Linux: <code>\var\log\messages</code> <p>You can use a wildcard pattern in the file name.</p> <p>In the real-time mode, rotation can occur only if the file is over-written or removed from the folder. The real-time processing mode assumes the following external rotation:</p> <ul style="list-style-type: none"> • Date format log rotation: The device creates a new log at a specified time in the with the naming convention <code>filename.timestamp.log</code>. The connector detects the new log and terminates the reader thread to the previous log after the processing is complete. The connector then creates a new reader thread to the new <code>filename.timestamp.log</code> and begins processing that file. To enable this log rotation, specify timestamp in <code>yyyy-MM-dd</code> date format. For example, <code>filename.yyyy-MM-dd.log</code> • Index log rotation: The device writes to indexed files in the following format: <code>filename.log.001</code>, <code>filename.log.002</code>, <code>filename.log.003</code>, and so on. At startup, the connector processes the log with highest index. When the device creates a log with a greater index, the connector terminates the reader thread to the previous log after processing completes, creates a thread to the new log, and begins processing that log. To enable this log rotation, use an index format, as shown in the following example: <code>filename'%d,1,99,true'.log</code>; Specifying <code>true</code> indicates that the index can be skipped. For example, if 5 appears before 4, processing proceeds with 5 and will not read 4. Use of <code>true</code> is optional.
	Reading Events Real Time or Batch	Specify whether to read files in batch mode or real-time mode. In batch mode, all files are read from the beginning.
	Action Upon Reaching EOF	This option applies to Batch Mode only. Specify None , Rename , or Delete as the action to be performed to the file when the connector finishes reading and reaches end of file. For the real-time mode, retain the default value None .
	File Extension If Rename Action	This option applies to Batch Mode only. Specify the extension to be added to the file name if the action on reaching the end of file is specified as Rename . The default value is Processed , which adds a <code>.processed</code> extension.

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. The connector cannot detect the network drive when running as a service on a Windows platform. This problem does not occur when the connector and IIS Server are installed on the same host.
11. Complete the installation.
12. [Run the SmartConnector](#).

For instructions about upgrading the connector or modifying parameters, see [SmartConnector Installation and User Guide](#).

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See the *ArcSight Console User's Guide* for more information about the ArcSight data fields.

Symantec Endpoint Protection Syslog Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Destination DNS Domain	Domain Name
Destination Host Name	Server Name
Destination User Name	Client User
Device Action	Action
Device Custom Date 1	Event time
Device Custom Number 1	Occurrences
Device Custom Number 2	SID
Device Custom String 1	Rule
Device Custom String 2	Policy Name
Device Custom String 4	Site Name
Device Custom String 5	Location
Device Custom String 6	Version
Device Host Name	SymantecServer
Device Product	Endpoint Protection
Device Vendor	Symantec
External Id	Scan ID
File Path	file
File Size	Size (bytes)
Name	Event Description
Source Dns Domain	Domain

ArcSight ESM Field	Device-Specific Field
Source Process Id	PID
Source Process Name	Application
Source User Name	User

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 Symantec Endpoint Protection Syslog (Micro Focus Security ArcSight Connectors 8.2.2)

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!