



ArcSight SmartConnectors

Software Version: 8.4.3

Configuration Guide for Symantec Messaging Gateway Syslog SmartConnector

Document Release Date: October 2023

Software Release Date: October 2023

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2023 Open Text.

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Trademark Notices

“OpenText” and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

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>

Contents

- Configuration Guide for Symantec Messaging Gateway Syslog SmartConnector 4
- Product Overview 5
- Configuration 6
 - Configuring Log Settings 6
 - Configure Event Merging 7
 - Configure the Syslog SmartConnectors 7
 - The Syslog Daemon SmartConnector 7
 - The Syslog Pipe and File SmartConnectors 8
 - Configure the Syslog Pipe or File SmartConnector 9
- Installing the SmartConnector 11
 - Preparing to Install the SmartConnector 11
 - Installing and Configuring the SmartConnector 11
- Device Event Mapping to ArcSight Fields 15
 - Symantec Messaging Gateway Event Mappings to ArcSight ESM Fields 15
- Send Documentation Feedback 16

Configuration Guide for Symantec Messaging Gateway Syslog SmartConnector

This guide provides information for installing the SmartConnector for Symantec Messaging Gateway Syslog and configuring the appliance for event collection.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight software and its environment.

Additional Documentation

The ArcSight SmartConnector documentation library includes the following resources:

- [Technical Requirements Guide for SmartConnector](#), which provides information about operating system, appliance, browser, and other support details for SmartConnector.
- [Installation and User Guide for 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.
- [Configuration Guide for SmartConnector Load Balancer](#), which provides detailed information about installing Load Balancer.

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the [documentation site for ArcSight SmartConnectors 8.4](#).

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 MFI-Documentation-Feedback@opentext.com.

For specific product issues, [contact Open Text Support for Micro Focus products](#).

Product Overview

Symantec Messaging Gateway offers enterprises a comprehensive gateway-based message-security solution. It delivers inbound and outbound messaging security, real-time antispam and antivirus protection, advanced content filtering, and data loss prevention in a single platform.

Configuration

Configuring Log Settings

The operating system provides a local logging facility, via syslog, that is configured to store logs accessed through the Control Center. You can configure log settings for Symantec Messaging Gateway components on each Scanner in your system. The severity of errors you want written to the log files can be chosen for the following components:

- Conduit
- Filter Engine
- Mail Transfer Agent

Five logging levels are provided. Each successive level includes all errors from previous levels. Your choices, from the least to the greatest amount of error reporting, and from the highest to the lowest severity, are as follows:

- Errors (least logged data)
- Warnings
- Notices
- Information
- Debug (most logged data)

To configure log settings:

- 1 In the Control Center, click **Settings -> Log Settings**.
- 2 On the **Log Settings** page, under **Logging**, choose a Scanner from the Host drop-down list.
- 3 Use the component drop-down lists to select the logging level for each component.
- 4 Complete the items under **Syslog Settings**.
- 5 For changes to apply to all scanners, check **Apply to all hosts**.
- 6 To reduce the size of the log table under **Log Storage Limits**, check **Maximum log size**. As the table exceeds the size specified, the oldest entries are removed.

If you check Maximum log size, indicate an upper limit for log size in KB, MB, or GB. The default is 50 MB.
- 7 Enter a numeric value in **Maximum number of days to retain**. The default is 7.

8 Under **Log Expunger**, choose a frequency and a start time when the Control Center runs the Log Expunger to delete log data. The default is once per day.

9 Click **Save** to store your information.

Configure Event Merging

The Symantec Messaging Gateway system provides a way to track security-relevant information on the system. Based on pre-configured rules, Symantec Messaging Gateway generates log entries to record as much information as possible about the events happening on your system. These events often contains multiple sub-events that can span multiple lines. The event merging feature aggregates the related sub-events into one large event with a concatenated long message.

To enable event merging:

1 Set up the Syslog Daemon connector according to the instructions in "Configure the Syslog SmartConnectors".

2 Edit the `syslog.subagent.parsers` parameter in the `agent.properties` file (located in the `$ARCSIGHT_HOME/current/user/agent` folder) as follows:agents
`[0].syslog.subagent.parsers=sms7x_syslog\:merge`

3 Start the connector as described in "Run the SmartConnector".

Configure the Syslog SmartConnectors

The three 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 Oracle Audit events so that Syslog Daemon will start receiving events: `*.* @@(remote/local-host-IP):514`

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



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`



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 as the Oracle server, 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.



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.

Configure 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 the following line to your **/etc/rsyslog.conf** file:

```
*.debug /var/tmp/syspipe
```

or

```
*.debug | /var/tmp/syspipe
```

depending on your operating system.

- 3 After you have modified the file, restart the 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, you would execute:

```
service syslog restart
```

On Solaris, you would execute:

```
kill -HUP `cat /var/run/syslog.pid`
```

This command forces the syslog daemon to reload the configuration and start writing to the pipe you just created.

For syslog file:

Create a file or use the default for the file into which log messages are to be written.

After editing the `/etc/rsyslog.conf` file, be sure to restart the syslog daemon as described above.

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.

Preparing to Install the SmartConnector

Before you install any SmartConnectors, make sure that the OpenText 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. Exit the installation wizard.
4. Do one of the following depending on your requirement:

- Select **Syslog Daemon** from the **Type** drop-down:
 - a. Click **Next**, then specify the following parameters:

| Parameters | Description |
|--------------|---|
| 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. |
| Protocol | Specify whether to read files in batch mode or real-time mode. In batch mode, all files are read from the beginning. |
| Forwarder | 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 . |

- b. Click **Next**.
- Select **Syslog File** from the **Type** drop-down:

a. Click **Next**, then specify the following parameters:

| Parameters | Description |
|-------------------------|--|
| Pipe Absolute Path Name | Specify an absolute path to the pipe, or accept the default value: <code>/var/tmp/syspipe</code> . |
| 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. |

| Parameters | Description |
|---|---|
| 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. |

b. Click **Next**.

5. Select a [destination and configure parameters](#).
6. Specify a name for the connector.
7. (Conditional) 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 then click **Next**. The certificate is imported and the **Add connector Summary** window is displayed.



Note: If you select Do not import the certificate to connector from destination, the connector installation will end.

8. Select whether you want to install 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 [Installation and User Guide for SmartConnector](#).

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 Messaging Gateway Event Mappings to ArcSight ESM Fields

| ArcSight ESM Field | Device-Specific Field |
|----------------------------|---|
| Agent (Connector) Severity | Very High when Device Severity = emerg or alert; High when Device Severity = crit or err; Medium when Device Severity = warning or notice; Low when Device Severity = info; Very Low when Device Severity = debug |
| Device Custom String 2 | pid (Process ID) |
| Device Custom String 3 | Externalid (Full External ID) |
| Device Direction | direction |
| Device Event Class ID | info |
| Device Facility | _SYSLOG_FACILITY |
| Device Process Name | procname |
| Device Product | 'Messaging Gateway' |
| Device Severity | _SYSLOG_PRIORITY |
| Device Vendor | 'Symantec' |
| External ID | externalId (40 characters) |
| Message | One of (Msg,(mergedevent.message," ",msg)) |
| Name | _ifThenElse(msg,,info,) |

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 Symantec Messaging Gateway Syslog SmartConnector (SmartConnectors 8.4.3)

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 MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!