



ArcSight SmartConnector

Software Version: 8.4.3

Configuration Guide for UNIX OS 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>

Configuration Guide for Syslog for UNIX OS SmartConnector

This guide provides information about installing the Syslog SmartConnectors for UNIX OS and configuring the device for syslog 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

The syslog SmartConnectors use a sub-connector architecture that lets them receive and process syslog events from multiple devices. There is a unique regular expression that identifies the device. For example, the same SmartConnector can process events from a Cisco Router and a NetScreen Firewall simultaneously. The SmartConnector inspects all incoming messages and automatically detects the type of device that originated the message.

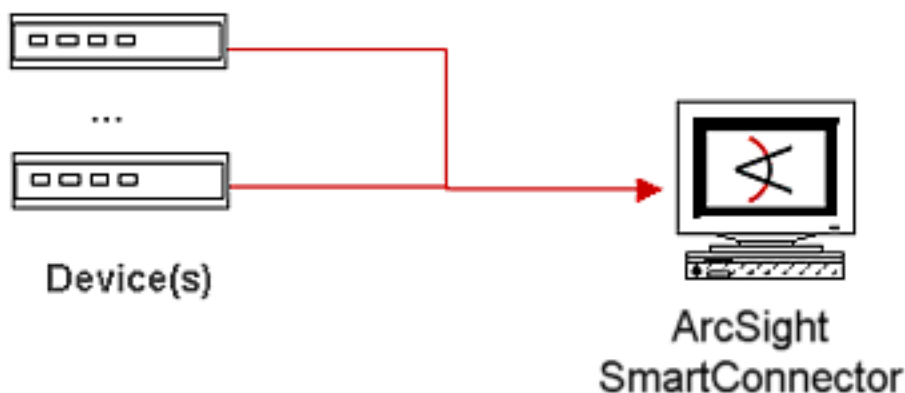
You can install the syslog SmartConnector as a syslog daemon, pipe, or file connector. You can use the Syslog Daemon, Syslog Daemon NG, or Syslog File connector types depending on your requirement. The Syslog File type SmartConnectors also support Syslog Pipe.

For information specific to configuration of devices to send syslog events to ArcSight SmartConnectors for Syslog (for example, Cisco Routers and Netscreen Firewall), see the relevant [SmartConnector Configuration Guides](#) specific to those devices.

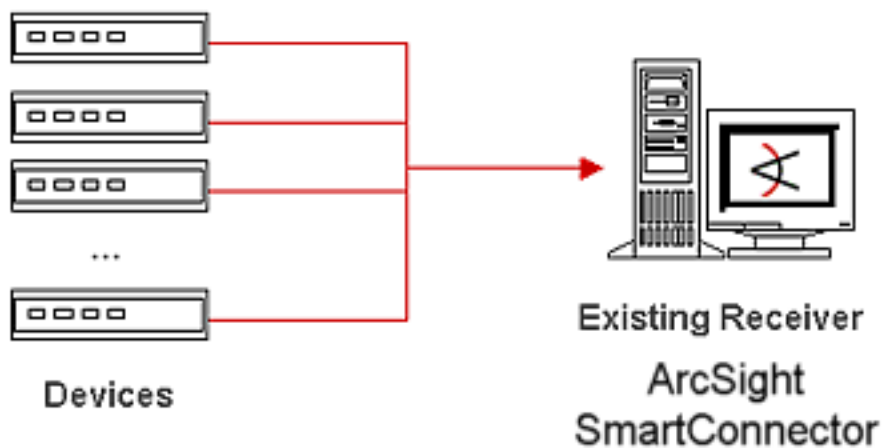
Using the SmartConnector for UNIX OS Deployment

SmartConnectors for Syslog can be used to receive information from any of the supported devices through syslog. Several deployment configurations can be implemented to leverage existing syslog infrastructures or to create a new one.

- In the simplest scenario, one or more devices can be configured to send syslog messages to a host running a SmartConnector for Syslog Daemon (typically a Windows-based host).



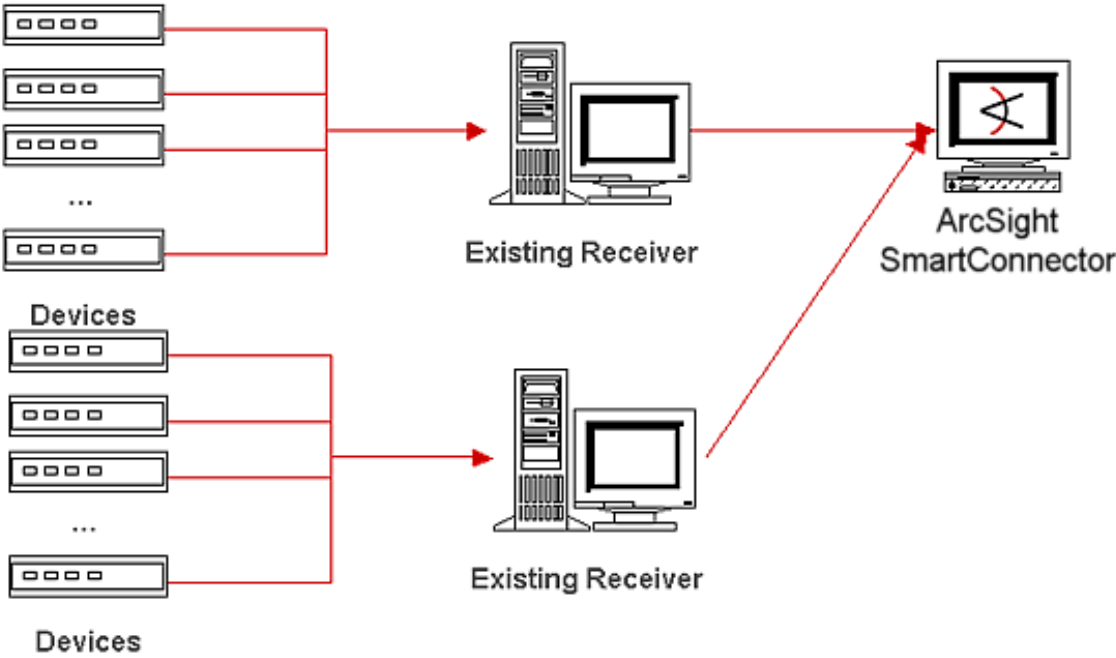
- When a UNIX Syslog Daemon is already in place and configured to receive syslog messages, an extra line in the syslog configuration file can be added to write the events to either a file or a system pipe. The ArcSight SmartConnector will run on the same machine as the Syslog Daemon.



- ArcSight SmartConnectors also can receive message input forwarded from an existing syslog infrastructure. A configuration line can be added on the concentrator to forward events to the ArcSight SmartConnector.



- Multiple concentrators also can forward events to a single ArcSight SmartConnector. However, depending on the rate of events sent by the concentrators, you might require more than one ArcSight SmartConnector to handle the event volume.



Configuration

Syslog Daemon SmartConnector

If you are using SmartConnector for Syslog Daemon, then add the following statement in the `rsyslog.conf` file to forward Oracle Audit events to Syslog Daemon:

```
<eventname> @@(remote/local-host-IP):514
```

Use `*.*` to read all Syslog events. For example, For example: `*.* @@(remote/local-host-IP):514`.

Replace regex with the specific event name, to filter specific events. For example, `local1.warning @@10.0.0.1:514`.

Use `@@` to send events over a TCP connection.

Use `@` to send events over an UDP connection.

If you run SmartConnector for Syslog Daemon on the same machine as the Oracle server, then you must provide the IP address of the local host. If you want to forward events to other machines, then you must provide the IP address of the same.



Note: Messages longer than 1024 bytes might be split into multiple messages on syslog daemon. There are no such restriction for syslog file or pipe.

Syslog Pipe and File SmartConnectors

When a syslog daemon is already in place and configured to receive syslog messages, you can add a line in the syslog configuration file (`rsyslog.conf`) 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.

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.

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.

For Syslog Pipe:

Create a pipe, then modify the **/etc/rsyslog.conf** file to send events to it.

1. Create a pipe by executing the following command:
`mkfifo /var/tmp/syspipe`
2. Add one of the following lines to **/etc/rsyslog.conf** file, depending on your operating system:
 - `*.debug /var/tmp/syspipe`
 - `*.debug | /var/tmp/syspipe`
3. To restart the syslog daemon, do one of the following:
 - Execute the following scripts:
 - a. **/etc/init.d/syslogd stop**
 - b. **/etc/init.d/syslogd start,**
 - Execute the following command to send a configuration restart signal:
 - **RedHat Linux:** `service syslog restart`
 - **Solaris:** `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:

1. Create a file or use the default file into which log messages are to be written.
2. After editing the **/etc/rsyslog.conf** file.
3. To restart the syslog daemon, do one of the following:
 - Execute the following scripts:
 - a. **/etc/init.d/syslogd stop**
 - b. **/etc/init.d/syslogd start,**
 - Execute the following command to send a configuration restart signal:
 - **RedHat Linux:** `service syslog restart`
 - **Solaris:** `kill -HUP `cat /var/run/syslog.pid``



Important: Make a note of the absolute path to the syslog file or pipe you created as you would need to specify the details during the installation of the SmartConnector.

Installing the 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. Specify the relevant [Global Parameters](#), when prompted.
4. Do one of the following depending on your requirement:

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

Parameter	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**, and specify the following parameters:

Parameter	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.

Parameter	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.

See the Configuration Guide for each individual syslog connector device for their mappings to ArcSight ESM fields. The following table shows the general UNIX OS Mappings to ArcSight ESM Fields:

ArcSight ESM Field	Device-Specific Field
Connector Severity	Very High when Device Severity = emerg, crit, ALERT, alert, fatal, Critical, CRITICAL, or VeryHigh; High when Device Severity = err, Error, error, High, or err error; Medium when Device Severity = warn, Warning, warning, WARNING, Medium, or warn warning; Low when Device Severity = info, notice, debug, NOTIFICATION, success, NOTICE, Low
Device Custom IPv6 Address 2	Source IPv6 Address
Device Custom IPv6 Address 3	Destination IPv6 Address
Device Custom IPv6 Address 3 Label	Destination IPv6 Address
Device Custom Number 1	File Descriptor
Device Custom String 1 Label	Module
Device Custom String 1	File Beat, Crond, Falcon-Sensor, Postfix/ Smtps/ Smtpd, Postfix/ Smtpd, Ansible-Slurp, Ipstat, Nscd, Sudo, Nscd, Cmlb, Root, Nfs Rpcbind, and Cmlb
Device Custom String 2 Label	Facility
Device Custom String 2	Mail, User, Deamon, and Local6
Device Custom String 4 Label	PID, Label, Command
Device Custom String 4	PID
Device Custom String 6 Label	eid
Device Custom String 6	login sshd httpd, 0, unknown
Device Facility	One of (Facility1, Facility2, _SYSLOG_FACILITY)
Device Host Name	Host Name
Device Process Name	ProcessHeader
Device Product	'Unix'
Device Severity	Info, Err, Crit, Warning, Low, Medium, Notice, Debug, Alert, and ERROR

ArcSight ESM Field	Device-Specific Field
Device Time Zone	DetectTime
Device Vendor	'Unix'
Destination Service Name	CROND, Activating service name
Event Outcome	Failed, Successfully, Failing
External ID	ID
Name	One of (Message, WholeMessage)
Source Service Name	lldpad, cachefilesd, gdm
Source User Name	root, gdm, lldpad

Troubleshooting

Depending on the deployment configuration that you choose, messages could pass through any number of intermediate layers before reaching the SmartConnector. For the process to work, each of these layers must be function accurately.

Following are some of the potential issues and the procedure to diagnose and troubleshoot these issues:**There is no route from the sender to the receiver, or a firewall could be blocking traffic on the selected port (usually UDP 514).**

To diagnose, run a packet sniffer on the receiver and make sure that the syslog packets arrive.

Solution: If there is any issue in receiving packets, modify firewall rules to allow syslog traffic through.

A local firewall is blocking incoming access to that port

To diagnose, check the current firewall rules. On Linux, run 'iptables-L' to list the current firewall rules.

Solution: Modify firewall rules to allow syslog traffic through.

The receiver is not listening on the specified port

To diagnose, issue the 'netstat-a' command and look for a line with "udp" and ":syslog".

Solution: If the receiving process is the Unix syslogd, the '-r' option might need to be passed to it before it starts listening for remote messages. Check /etc/sysconfig/syslog on RedHat.

Another process is listening on the named pipe (only applicable for the Pipe connector)

To diagnose, use 'fuser -v/path/to/pipe' to see which process is listening on the pipel.

Solution: Kill offending process.

Events are not being picked up and processed

To diagnose, open Raw Events and make sure a line is inserted.

Solution: The Line Feed (LF) character (0x0A, \n) is used as a new line character in UNIX based systems (Linux, Mac OSX, etc).

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 UNIX OS Syslog SmartConnector (SmartConnector 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!