



ArcSight SmartConnectors

Software Version: CE 24.2

Configuration Guide for Cisco IOS Syslog SmartConnector

Document Release Date: April 2024

Software Release Date: April 2024

Legal Notices

Open Text Corporation

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

Copyright Notice

Copyright 2003 – 2024 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 Cisco IOS Syslog SmartConnector 4
- Product Overview 5
- Configurations 6
 - Configuring the Device for Event Collection 6
 - Enabling Time-Stamps on Log Messages 6
 - Enabling System Message Logging 6
 - Setting the Syslog Destination 6
 - Limiting the Error Message Severity Level 7
 - Defining the UNIX System Logging Facility 7
 - Configuring for the Syslog SmartConnectors 7
- Installing the SmartConnector 11
 - Preparing to Install the SmartConnector 11
 - Installing and Configuring the SmartConnector by Using the Wizard 11
- Device Event Mapping to ArcSight Fields 15
 - Cisco Router IOS Event Mappings to ArcSight ESM Events 15
- Send Documentation Feedback 17

Configuration Guide for Cisco IOS Syslog SmartConnector

This guide provides information for installing the SmartConnector for Cisco IOS Syslog and configuring the IOS 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

Cisco IOS Software is the world's leading network infrastructure software, delivering a seamless integration of technology innovation, business-critical services, and hardware support. Dozens of hardware platforms are supported, and more than 700 industry-leading features that span multiple technology areas, including Security, Voice, High Availability, IP Routing, Quality of Service, IP Multicast, IP Addressing, IP Mobility, Multiprotocol Label Switching, and VPNs.



Note: IOS debug logs are not supported.

Configurations

Configuring the Device for Event Collection

To configure a Cisco IOS device to send syslog events to a syslog server:

1. Telnet to your IOS device.
2. Within the console, specify **enable** or **en** to enable mode.
3. Specify configuration mode as **configure terminal** or **conf t**.

Follow the instructions provided in the following sections to enable timestamps and system message logging, and to set the syslog destination, severity level, and syslog facility.

Enabling Time-Stamps on Log Messages

By default, log messages are not time-stamped. To enable time-stamping of log messages and debug messages, use the following commands in global configuration mode respectively:

- Router(Config)#service timestamps log datetime localtime
- Router(Config)#service timestamps debug datetime localtime

Enabling System Message Logging

System message logging is enabled by default. It must be enabled to send messages to any destination other than the console. To re-enable message logging after it has been disabled, use the following command in global configuration mode:

```
Router(config)#logging on
```

Setting the Syslog Destination

To identify the syslog server that is to receive logging messages, use the following command in global configuration mode:

```
Router(config)#logging host
```

The *host* argument is the name or IP address of the host. By issuing this command more than once, you build a list of syslog servers that receive logging messages. The `no logging` command deletes the syslog server with the specified address from the list of syslogs.

Limiting the Error Message Severity Level

You can limit the number of messages by specifying the severity level of the error message. To do so, use the following command in global configuration mode:

Router(config)#logging trap *Level*

Keyword	Level	Description	Syslog Def
emergencies	0	System unusable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

Defining the UNIX System Logging Facility

You can log messages produced by UNIX system utilities. To do this, enable this type of logging and define the UNIX system facility from which you want to log messages. Consult the operator manual for your UNIX operating system for more information about these UNIX system facilities.

To define UNIX system facility message logging, use the following command in global configuration mode: Router(config)#logging facility *facility-type*

Configuring for the Syslog SmartConnectors

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.

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 by default, or can be configured on another port to receive syslog events. You can also configure to use the TCP protocol.

To use the SmartConnector for Syslog Daemon, add the following statement in the *rsyslog.conf* file:

```
*.* @@(remote/local-host-IP):514
```

Example: local1.warning @@10.0.0.1:514

- To read all Syslog events, use *.*
- To filter specific events, replace regex with the specific event name.
- For example: *.* @@(remote/local-host-IP):514 and local1.warning @@10.0.0.1:514.
- To send events over a TCP connection, use @@ and to send events over an UDP connection, use @.

If you are running SmartConnector for Syslog Daemon on the same machine as the 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 might be split into multiple messages on syslog daemon. No such restriction exists on syslog file or pipe.

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. The 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.

Using the SmartConnector for Syslog Pipe or File

This section provides information 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.

For Syslog Pipe:

1. Execute the following command to create a pipe:

```
mkfifo /var/tmp/syspipe
```

2. Add one of the following lines depending on your OS to the `/etc/rsyslog.conf` file:

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

or

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

3. Restart the syslog daemon in one of the following methods:

Enter the following commands:

```
/etc/init.d/syslogd stop  
/etc/init.d/syslogd start
```

or

Execute the following command to send a configuration restart signal:

On RedHat Linux:

```
service syslog restart
```

On Solaris:

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

For Syslog File:

1. Create a file or use the default file into which log messages must be written.
2. Modify the /etc/rsyslog.conf file
The syslog daemon is forced to reload the configuration and start writing to the pipe.
3. Restart the syslog daemon in one of the following methods:
 - a. Restart the syslog daemon in one of the following methods:
Enter the following commands:

```
/etc/init.d/syslogd stop  
/etc/init.d/syslogd start
```

or

Execute the following command to send a configuration restart signal:

On RedHat Linux:

```
service syslog restart
```

On Solaris:

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

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.

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 Cisco IOS Syslog Connector. For detailed installation steps or for manual installation steps, see SmartConnector Installation and User Guide.

To install and configure the Cisco IOS Syslog Connector:

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.

Cisco Router IOS Event Mappings to ArcSight ESM Events

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Very High = 0 or 1; High = 2 or 3; Medium = 4 or 5; Low = 6 or 7.
Destination Address	dest_addr
Device Custom Floating Point 1	Operating value
Device Custom Floating Point 2	Threshold value
Device Custom IPv6 Address 2	Source IPv6 Address
Device Custom IPv6 Address 3	Destination IPv6 Address
Device Custom Number 2	Packets
Device Custom String 1	Slot/Card
Device Custom String 2	CiscoFacility
Device Custom String 3	CiscoCode
Device Custom String 4	ICMP Type
Device Custom String 5	CiscoAlertCode
Device Custom String 6	ACL Number
Device Event Category	Category
Device Event Class ID	CiscoFacility plus CiscoCode
Device Facility	_SYSLOG_FACILITY
Device Inbound Interface	R0/0
Device Process Name	kernel
Device Product	'CiscoRouter'
Device Receipt Time	DetectTime

ArcSight ESM Field	Device-Specific Field
Device Severity	CiscoSeverity
Device Vendor	'CISCO'
External ID	CiscoAlertID
File	btrace_rotate_sh_pmanlog_R0-0.24184_15571.20210507122646.bin.gz
File Location	/harddisk/tracelogs/.btrace_rotate_sh_pmanlog_R0-0.24184_15571.20210507122646.bin.gz.tmp
File Size	size
Message	Message Detail
Name	Message Detail
Old File Name	Object Name
Old File Path	Object Location
Old File Permission	Warning
Reason	Status
Source Address	src_addr
Source Translated Address	remote IP Address
Source User Name	Client User



Note: The **event.name** field is supported by the common mapping, and then parsed by another mapping file again.

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 Cisco IOS Syslog SmartConnector (SmartConnectors CE 24.2)

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 MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!