Hewlett Packard Enterprise

HPE Security ArcSight Connectors

SmartConnector for Cisco Catalyst OS Syslog

Configuration Guide

October 17, 2017

Configuration Guide

SmartConnector for Cisco Catalyst OS Syslog

October 17, 2017

Revision History

Date	Description
10/17/2017	Added encryption parameters to Global Parameters.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
05/15/2015	Added new parameters for Syslog File.
02/16/2015	Added parameter for Syslog Daemon connector configuration.
05/15/2012	Added new installation procedure.
11/15/2010	Added support for CatOS v8.0.
02/11/2010	Added support for FIPS Suite B and CEF File transport.
06/30/2009	Added global update to installation procedure.
02/11/2009	Clarified platforms supported for connector installation.

SmartConnector for Cisco Catalyst OS Syslog

This guide provides information for installing the SmartConnector for Cisco Catalyst OS Syslog and configuring the device for event collection. Cisco Catalyst Switch devices using CatOS versions 5.0 and 8.0 are supported.

Product Overview

The Cisco Catalyst Switches are fixed-configuration, stackable standalone switches that provide wire-speed Fast Ethernet and Gigabit Ethernet connectivity. Differing models of the Catalyst switches offer distinct sets of software features and a range of configurations.

Configuration

Configure the System Message Log

The system message logging facility provides you with logging information for monitoring and troubleshooting, and lets you select the types of logging informaiton captured and the destination of the captured information.

By default, Cisco Catalyst logs normal but significant system messages to its internal buffer and sends these messages to the system console. You can specify which system messages should be saved based on the type of facility and the severity level. Messages can be time-stamped to enhance real-time debugging and management.

The Cisco Catalyst switches ship with the following default configuration:

System message logging to the console is enabled.
System message logging to Telnet sessions is enabled.
Logging server is disabled.
Syslog server IP address is not configured.
Server facility is LOCAL7.
Server severity is Warnings (4).
Logging buffer size is 500.
Logging history size is 1
Timestamp option is disabled

When you first log on to the switch console, enter the `show logging` command to display the default configuration.

Change Logging Defaults

To change the default system message logging facility and severity levels, perform one of these tasks in privileged mode:

■ Set the default facility and severity level for system messages.

```
set logging level facility severity [default]
```

■ Disable system message logging to the console.

```
set logging console disable
```

Examples:

To change the default system message logging facility and severity levels for the Cisco Discovery Protocol (CDP) to severity level 3:

```
Console> (enable) set logging level cdp 3
```

To disable system message logging to the console:

```
Console> (enable) set logging console disable
```

Configure the Syslog Daemon

Before you can send system log messages to a UNIX syslog server, you must configure the syslog daemon on the UNIX server. To configure the syslog daemon, log in as root and perform these steps:

1   Add a line such as the following in the file /etc/syslog.conf:

```
user.debug      /var/log/myfile.log
```

> There must be five tab characters between user.debug and /var/log/myfile.log. Refer to entries in the /etc/syslog.conf file for further examples.

The switch sends messages according to specified facility types and severity levels. The user keyword specifies the UNIX logging facility. The messages from the switch are generated by user processes. The debug keyword specifies the severity level of the condition being logged. You can set UNIX systems to receive all messages from the switch.

2   Create the log file by entering these commands at the UNIX shell prompt:

```
$ touch /var/log/myfile.log
$ chmod 666 /var/log/myfile.log
```

3   Make sure the syslog daemon reads the new changes by entering this command:

```
$ kill -HUP \Qcat /etc/syslog.pid
```

Configure Syslog Servers

To configure the switch to log messages to a syslog server, perform this task in privileged mode:

1   Add a syslog server to the configuration.

```
set logging server ip_addr
```

2   Enable system message logging to configured syslog servers.

```
set logging server enable
```

3   Set the facility and severity level for syslog server messages.

```
set logging server facility server_facility_parameter
set logging server severity server_severity_level
```

You can configure a maximum of three syslog servers at any time.

Examples

To add a new syslog server with an IP address of 171.69.192.205 to the system logging server table:

```
Console> (enable) set logging server 171.69.192.205
```

To enable system message logging to a configured syslog server:

```
Console> (enable) set logging server enable
```

To set the syslog server facility to local0:

```
Console> (enable) set logging server facility local0
```

To set the syslog server severity level to 4:

```
Console> (enable) set logging server severity 4
```

To remove a syslog server from the configuration, perform this task in privileged mode:

```
clear logging server ip_addr
```

To remove a syslog server from the configuration, perform this task in privileged mode:

```
clear logging server ip_addr
```

To delete the syslog server 171.69.192.207 from the configuration:

```
Console> (enable) clear logging server 171.69.192.207
```

To disable logging to the syslog server, perform this task in privileged mode:

```
set logging server disable
```

To disable system message logging to a configured syslog server:

```
Console> (enable) set logging server disable
```

To limit the number of messages buffered, perform this task in privileged mode:

```
set logging buffer buffer_size
```

To limit to 200 the number of messages stored in the buffer:

```
Console> (enable) set logging buffer 200
```

To enable or disable the system logging messages timestamp, perform this task in privileged mode:

```
set logging timestamp {enable | disable}
```

To enable the timestamp display on system logging messages:

```
Console> (enable) set logging timestamp enable
```

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 the SmartConnector for Syslog Daemon, simply start the connector, either as a service or as a process, to start receiving events; no further configuration is needed.

> 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.**

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.

Install the SmartConnector

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

Syslog Installation

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 by default listens on port 514 (configurable) for UDP syslog events; you can configure the port number or use of the TCP protocol manually. The syslog pipe and syslog file connectors read events from a system pipe or file, respectively. Select the one that best fits your syslog infrastructure setup.

Prepare to Install Connector

Before you install any SmartConnectors, make sure that the ArcSight products with which the connectors will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger).

For complete product information, read the *Administrator's Guide* as well as the *Installation and Configuration* guide for your ArcSight product before installing a new SmartConnector. If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* for instructions, and start the installation procedure at "Set Global Parameters (optional)" or "Select Connector and Add Parameter Information."

Before installing the SmartConnector, be sure the following are available:

■   Local access to the machine where the SmartConnector is to be installed

■   Administrator passwords

Install Core Software

Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms; for the complete list, see the *SmartConnector Product and Platform Support* document, available from the HPE SSO and Protect 724 sites.

1   Download the SmartConnector executable for your operating system from the HPE SSO site.

2   Start the SmartConnector installation and configuration wizard by running the executable.

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

Follow the wizard through the following folder selection tasks and installation of the core connector software:

Introduction
Choose Install Folder
Choose Shortcut Folder
Pre-Installation Summary
Installing...

3 When the installation of SmartConnector core component software is finished, the following window is displayed:
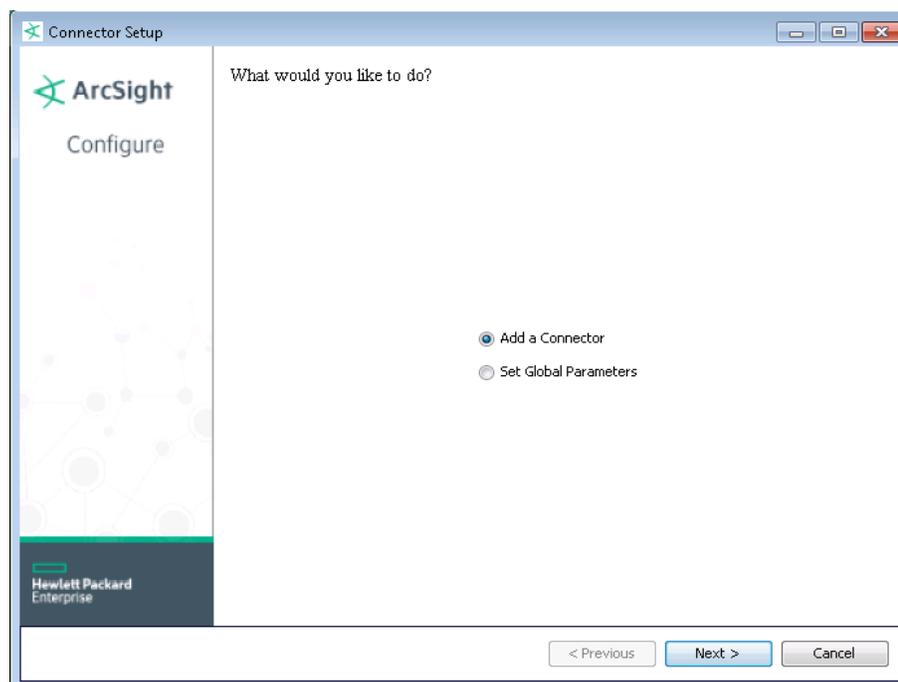
Set Global Parameters (optional)

If you choose to perform any of the operations shown in the following table, do so before adding your connector. You can set the following parameters:

Parameter	Setting
FIPS mode	Select 'Enabled' to enable FIPS compliant mode. To enable FIPS Suite B Mode, see the SmartConnector User Guide under "Modifying Connector Parameters" for instructions. Initially, this value is set to 'Disabled'.
Remote Management	Select 'Enabled' to enable remote management from ArcSight Management Center. When queried by the remote management device, the values you specify here for enabling remote management and the port number will be used. Initially, this value is set to 'Disabled'.
Remote Management Listener Port	The remote management device will listen to the port specified in this field. The default port number is 9001.
Preferred IP Version	When both IPv4 and IPv6 IP addresses are available for the local host (the machine on which the connector is installed), you can choose which version is preferred. Otherwise, you will see only one selection. The initial setting is IPv4.

The following parameters should be configured only if you are using HPE SecureData solutions to provide encryption. See the *HPE SecureData Architecture Guide* for more information.

Parameter	Setting
Format Preserving Encryption	Data leaving the connector machine to a specified destination can be encrypted by selecting 'Enabled' to encrypt the fields identified in 'Event Fields to Encrypt' before forwarding events. If encryption is enabled, it cannot be disabled. Changing any of the encryption parameters again will require a fresh installation of the connector.
Format Preserving Policy URL	Enter the URL where the HPE SecureData Server is installed.
Proxy Server (https)	Enter the proxy host for https connection if any proxy is enabled for this machine.
Proxy Port	Enter the proxy port for https connection if any proxy is enabled for this machine.
Format Preserving Identity	The HPE SecureData client software allows client applications to protect and access data based on key names. This key name is referred to as the identity. Enter the user identity configured for HPE SecureData.
Format Preserving Secret	Enter the secret configured for HPE SecureData to use for encryption.
Event Fields to Encrypt	Recommended fields for encryption are listed; delete any fields you do not want encrypted and add any string or numeric fields you want encrypted. Encrypting more fields can affect performance, with 20 fields being the maximum recommended. Also, because encryption changes the value, rules or categorization could also be affected. Once encryption is enabled, the list of event fields cannot be edited.

After making your selections, click **Next**. A summary screen is displayed. Review the summary of your selections and click **Next**. Click **Continue** to return to proceed with "Add a Connector" window. Continue the installation procedure with "Select Connector and Add Parameter Information."

Select Connector and Add Parameter Information

1   Select **Add a Connector** and click **Next**. If applicable, you can enable FIPS mode and enable remote management later in the wizard after SmartConnector configuration.

2   Select **Unix Syslog Daemon, Pipe, or File** and click **Next**.

3   Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.

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 (accept the default (ALL) to bind to all available IP addresses).
	Protocol	The SmartConnector for Syslog Daemon uses the selected protocol (UDP or Raw TCP) 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.
Syslog Pipe Parameter	*Pipe Absolute Path Name*	Absolute path to the pipe, or accept the default: /var/tmp/syspipe
Syslog File Parameters	*File Absolute Path Name*	Enter the full path name for the file from which this connector will read events or accept the default: \var\adm\messages (Solaris) or \var\log\messages (Linux).
		A wildcard pattern can be used in the file name; however, in realtime mode, rotation can occur only if the file is over-written or removed from the folder. Realtime processing mode assumes following external rotation.

	For date format log rotation, the device writes to 'filename.timestamp.log' on a daily basis. At a specified time, the device creates a new daily log and begins to write to it. The connector detects the new log and terminates the reader thread to the previous log after processing is complete. The connector then creates a new reader thread to the new 'filename.timestamp.log' and begins processing that file. To enable this log rotation, use a date format in the file name as shown in the following example:
	`filename'yyyy-MM-dd'.log;`
	For index log rotation, the device writes to indexed files - 'filename.log.001', 'filename.log.002', 'filename.log.003', 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:
	`filename'%d,1,99,true'.log;`
	Specifying 'true' indicates that it is allowed for the index to be skipped; for example, if 5 appears before 4, processing proceeds with 5 and will not read 4, even if 4 appears later. Use of 'true' is optional.
Reading Events Real Time or Batch	Specify whether file is to be read in batch or realtime mode. For batch mode, all files are read from the beginning. The 'Action Upon Reaching EOF' and 'File Extension if Rename Action' parameters apply for batch mode only.
Action Upon Reaching EOF	For batch mode, specify 'None', 'Rename', or 'Delete' as the action to be performed to the file when the connector has finished reading and reaches end of file (EOF). For realtime mode, leave the default value of 'None' for this parameter.
File Extension If Rename Action	For batch mode, specify the extension to be added to the file name if the action upon EOF is 'Rename' or accept the default value of '.processed'.

Select a Destination

1   The next window asks for the destination type; select a destination and click **Next**. For information about the destinations listed, see the *ArcSight SmartConnector User Guide*.

2   Enter values for the destination. For the ArcSight Manager destination, the values you enter for **User** and **Password** should be the same ArcSight user name and password you created during the ArcSight Manager installation. Click **Next**.

3   Enter a name for the SmartConnector and provide other information identifying the connector's use in your environment. Click **Next**. The connector starts the registration process.

4   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.

Complete Installation and Configuration

1   Review the **Add Connector Summary** and click **Next**. If the summary is incorrect, click **Previous** to make changes.

2   The wizard now prompts you to choose whether you want to run the SmartConnector as a stand-alone process or as a service. If you choose to run the connector as a stand-alone process, select **Leave as a standalone application**, click **Next**, and continue with step 5.

3   If you chose to run the connector as a service, with **Install as a service** selected, click **Next**. The wizard prompts you to define service parameters. Enter values for **Service Internal Name** and **Service Display Name** and select **Yes** or **No** for **Start the service automatically**. The **Install Service Summary** window is displayed when you click **Next**.

4   Click **Next** on the summary window.

5   To complete the installation, choose **Exit** and Click **Next**.

For instructions about upgrading the connector or modifying parameters, see the *SmartConnector User Guide*.

Run the SmartConnector

SmartConnectors can be installed and run in stand-alone mode, on Windows platforms as a Windows service, or on UNIX platforms as a UNIX daemon, depending upon the platform supported. On Windows platforms, SmartConnectors also can be run using shortcuts and optional Start menu entries.

If the connector is installed in stand-alone mode, it must be started manually and is not automatically active when a host is restarted. If installed as a service or daemon, the connector runs automatically when the host is restarted. For information about connectors running as services or daemons, see the *ArcSight SmartConnector User Guide*.

To run all SmartConnectors installed in stand-alone mode on a particular host, open a command window, go to `$ARCSIGHT_HOME\current\bin` and run: `arcsight connectors`

To view the SmartConnector log, read the file `$ARCSIGHT_HOME\current\logs\agent.log`; to stop all SmartConnectors, enter `Ctrl+C` in the command window.

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 Catalyst OS Field Mappings

ArcSight ESM Field	Device-Specific Field
Additional Data	asic
Additional Data	BusIFRegister
Additional Data	ConfigurationBlock
Additional Data	ConfigurationSize
Additional Data	MacAddressRange
Additional Data	NvramAvailable
Additional Data	NvramSize
Additional Data	Port rxTotalDrops
Additional Data	ReInitCount

ArcSight ESM Field	Device-Specific Field
Additional Data	RxTotoalDrops
Additional Data	seq
Additional Data	SourceMemoryLocation
Additional Data	srcidx
Additional Data	TargetMemoryLocation
Application Protocol	'UDP'
ArcSight Severity (High)	2 or 3
ArcSight Severity (Low)	6 or 7
ArcSight Severity (Medium)	4 or 5
ArcSight Severity (Very High)	0 or 1
Destination Address	Destination IP
Destination Mac Address	Destination Mac
Destination Port	Destination port
Destination Process Name	ProcessId
Device Action	Action taken by the device
Device Custom String 1	Source Module
Device Custom String 2	Destination Module
Device Custom String 3	Socket
Device Custom String 4	VLAN
Device Custom String 5	Port State
Device Event Class ID	MessageId
Device Inbound Interface	Source Interface
Device Outbound Interface	Destination Interface
Device Product	'CatOS'
Device Receipt Time	DetectTime
Device Severity	CiscoSeverity
Device Time Zone	TimeZone
Device Vendor	'CISCO'
Name	Text of message
Source Address	Source IP
Source Port	Source port
Transport Protocol	protocol