Hewlett Packard Enterprise

HPE Security ArcSight Connectors

SmartConnector for Cisco ASA Syslog

Configuration Guide

February 15, 2017

Configuration Guide

SmartConnector for Cisco ASA Syslog

February 15, 2017

Revision History

Date	Description
02/15/2017	End of support for versions 6.2, 6.3, 7.0, 7.1, 7.2, 8.0, and 8.1 due to end of support by vendor. Removed 'PIX' from connector name as PIX is no longer supported by vendor.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
10/28/2016	Added support for ASA 9.6 events.
02/15/2016	Added support for ASA 9.5 events.
05/15/2015	Added new parameters for Syslog File.
02/16/2015	Added parameter for Syslog Daemon connector configuration. Added support for ASA 9.3 events.
08/15/2014	Added support for ASA 9.2 events.
05/15/2013	Added support for ASA 9.0 and 9.1 events.
08/15/2012	Added support for ASA 8.5 and 8.6 events.
05/15/2012	Added IPv6 address event support; added new installation procedure.

SmartConnector for Cisco ASA Syslog

This guide provides information for installing the SmartConnector for Cisco ASA Syslog and configuring the device for syslog event collection. Cisco ASA versions 8.2, 8.3, 8.4, 8.5, 8.6, 9.0, 9.1, 9.2, 9.3, 9.5, and 9.6 are supported.

Product Overview

The Cisco Adaptive Security Appliance (ASA) Series is a modular platform that provides firewall security monitoring and intrusion protection services for the complete security solution. These security appliances provide the next generation of security and VPN services.

> If your appliance has Cisco IDS or Cisco IPS installed, those events are not collected as syslog events. Use the SmartConnector for Cisco Secure IPS SDEE for IPS event collection.
>
> Cisco default syslog format is the only format supported by this SmartConnector.

Configuration

Configuring the Cisco Device to Send Events

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

1 Telnet to your Cisco machine.

2 Within the console, enter enable mode by entering `hostname(config)# enable` or `hostname(config)# en`.

3 Enter configuration mode by entering `hostname(config)# configure terminal` or `hostname(config)# conf t`.

4 Enter the following lines:

```
hostname(config)# logging on
hostname(config)# logging timestamp
hostname(config)# no logging standby
hostname(config)# no logging console
hostname(config)# no logging monitor
hostname(config)# no logging buffered debugging
hostname(config)# logging trap debug
hostname(config)# no logging history
hostname(config)# logging facility <syslog server logging directory>
hostname(config)# logging queue 512
hostname(config)# logging host inside <syslog server ip address>
```

The **logging facility** can be one of the following:

16	local0
17	local1
18	local2
19	local3
20	local4
21	local5
22	local6
23	local7

For example, to log to syslog facility local6, create the following entry on the device:

```
logging facility 22
```

For the **logging host**, replace `syslog server ip address` with the syslog server's IP address. You can use multiple logging host commands to specify additional servers.

For the **logging trap** severity level, the `debug` level is specified, which logs the following message types:

    0–emergencies–System unusable messages
    1–alert–Take immediate action
    2–critical–Critical condition
    3–error–Error message
    4–warning–Warning message
    5–notification–Normal but significant condition
    6–informational–Information message
    7–debugging–Debug messages and log FTP commands and WWW URLs

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:
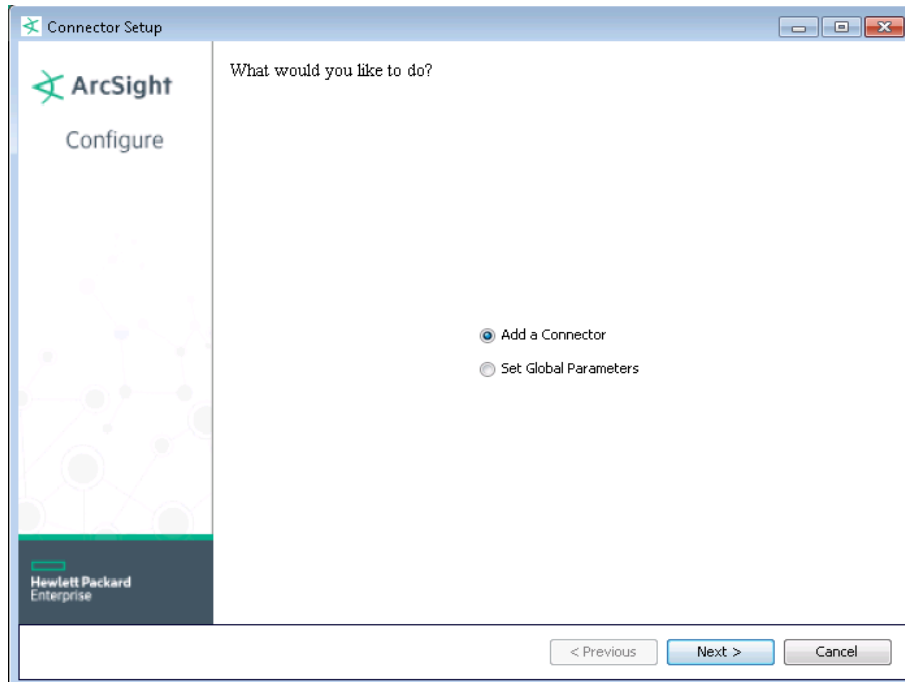
Set Global Parameters (optional)

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:

Global Parameter	Setting
Set FIPS mode	Set to 'Enable' 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 'Disable'.
Set Remote Management	Set to 'Enable' 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 'Disable'.
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	If 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. When both values are present, the initial setting is IPv4.

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 the "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 **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 ASA Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Very High = 0, 1; High = 2, 3; Medium = 4, 5; Low = 6,7
Application Protocol	Protocol
Destination Address	Destination IP
Destination Host Name	IP
Destination Port	Destination Port
Destination Translated Address	NATted Destination Address
Destination Translated Port	NATted Destination Port
Destination User Id	Destination User
Destination User Name	User
Destination User Privileges	Destination user privileges
Device Action	Action taken by the device
Device Custom IPv6 Address 1	Device IPv6 Address
Device Custom IPv6 Address 2	Source IPv6 Address
Device Custom IPv6 Address 3	Destination IPv6 Address
Device Custom Number 1	ICMP Type
Device Custom Number 2	ICMP Code
Device Custom Number 3	DurationInSeconds

ArcSight ESM Field	Device-Specific Field
Device Custom String 1	ACL
Device Custom String 2	Unit
Device Custom String 3	TCP Flags
Device Custom String 4	Order
Device Custom String 5	Connection Type
Device Custom String 6	Duration
Device Direction	Inbound or Outbound
Device Event Category	MessageClass
Device Event Class Id	PixMessageId
Device Host Name	One of (DeviceHostName, _SYSLOG_SENDER)
Device Inbound Interface	Source interface
Device Outbound Interface	Destination interface
Device Product	Product
Device Receipt Time	PixDate
Device Severity	PixSeverity (7 - 0)
Device Vendor	'CISCO'
External Id	Connection Id/Tunnel Id/event_ID
File Name	Command, Filename
Message	Reason, Message
Name	PixMessage
Request URL	Accessed URL
Source Address	Source IP address
Source Host Name	Source host name
Source Mac Address	Source mac address
Source Port	Source port
Source Translated Address	Source NATted address
Source Translated Port	Source NATted port
Source User Name	Source user
Transport Protocol	TCP/UDP/ICMP/IGMP/ARP/PPTP/PPP/PPPoE/TACACS+/ESMTP

Troubleshooting

What is the expected behavior from the connector for a typical teardown message from ASA?

For teardown messages, because the direction of the flow is not known from the syslog message, we do not know for certain what is the source and what is the destination. Based on the format of the syslog message (shown below) we map the **for/from** part to `source` and the **to** part to `destination`.

```
Apr 20 17:54:51 151.174.6.33 Apr 20 2010 13:54:51: %ASA-6-302014:
Teardown TCP connection 227777586 for outside:98.136.152.54/80 to
inside:172.27.191.13/2710 duration 0:00:00 bytes 4699 TCP FINs
```