Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for Juniper Pulse Secure Access Syslog (Legacy)

Configuration Guide

February 15, 2016

Configuration Guide

SmartConnector for Juniper Pulse Secure Access Syslog (Legacy)

February 15, 2016

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Package Enterprise Development LP shall not be liable for technical or editorial omissions contained herein. The information contained herein is subject to change without notice. The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only. Hewlett Package Enterprise Development LP products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices. This document is confidential.

Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise Development LP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Follow this link to see a complete statement of Hewlett Package Enterprise Development LP copyrights, trademarks and acknowledgements:
https://www.protect724.hpe.com/docs/DOC-13026.

Revision History

Date	Description
02/15/2016	Marked this connector as legacy. For future version support, use the SmartConnector for PulseSecure Pulse Connect Secure Syslog.
06/30/2015	Renamed connector from Juniper Secure Access SSL VPN Syslog to Juniper Pulse Secure Access Syslog. Added support for version 8.1 and removed support for versions prior to 8.0 due to end of support by vendor.
05/15/2015	Added new parameters for Syslog File.
02/16/2015	Updated Device Receipt Time mappings in SSL VPN Syslog and SSL VPN Key Value Version 6.3/6.5/7.0/7.1/8.0 Event Mappings. Added parameter for Syslog Daemon connector configuration.
08/15/2014	Corrected parser errors in "Secure Access SSL VPN Syslog Version 6.3/6.5/7.0/7.1/8.0 Event Mappings".
05/15/2014	Added support for version 8.0.
05/15/2012	Added new installation procedure.
11/15/2011	Added support for versions 7.0 and 7.1.
08/12/2011	Added configuration information.

SmartConnector for Juniper Pulse Secure Access Syslog (Legacy)

This guide provides information for installing the SmartConnector for Juniper Pulse Secure Access Syslog (Legacy) and configuring the device for event collection. Juniper Pulse Secure Access versions 8.0 and 8.1 are supported. For future version support, use the SmartConnector for PulseSecure Pulse Connect Secure Syslog.

Product Overview

Juniper JUNOS Pulse Secure Access Service is a remote access solution that enables enterprises and service providers to provide secure, location and device-independent network connectivity to remote and mobile users from any web-enabled device through a JUNOS Pulse client interface.

Configuration

Specify Events to Log

See the Juniper Pulse Secure Access documentation for complete logging and monitoring information.

The logging feature lets you create custom filters to view and save only those log messages you select in the format of your choice. You can access the logging feature from the **System -> Log/Monitoring** page of the admin console.

Use options in the **Settings** tab to specify what is written to the log file, which syslog servers are used to store the log files, and the maximum file size.

To specify events log settings:

1 In the admin console, select **System -> Log/Monitoring**.

2 Select the **Events**, **User Access**, **Admin Access**, or **Sensors** tab, and then select **Settings**.

3 In the **Maximum Log Size** field, specify the maximum file size for the local log file (the limit is 500 MB). The system log displays data up to the amount specified.

4 Under **Select Events to Log**, select the checkbox for each type of event that you want to capture in the local log file.

5 Under **Syslog Servers**, enter information about the syslog servers where you want to store your log files:

- **a** Enter the name or IP address of the syslog server.
- **b** Enter a facility for the server (LOCAL0-LOCAL7 can be mapped to facilities on your syslog server).
- **d** Click **Add**.
- **e** Repeat for different servers and facilities as required.

Make sure your syslog server accepts messages with the following settings: facility = LOG_USER and level = LOG_INFO.

6 Click **Save Changes**.

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 are 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). This configuration guide takes you through the installation process with **ArcSight Manager (encrypted)** as the destination.

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 Connector Appliance/ArcSight Management Center, see the *ArcSight Connector Appliance or ArcSight Management Center Administrator's Guide* for instructions, and start the installation procedure at "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 HP SSO and Protect 724 sites.

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

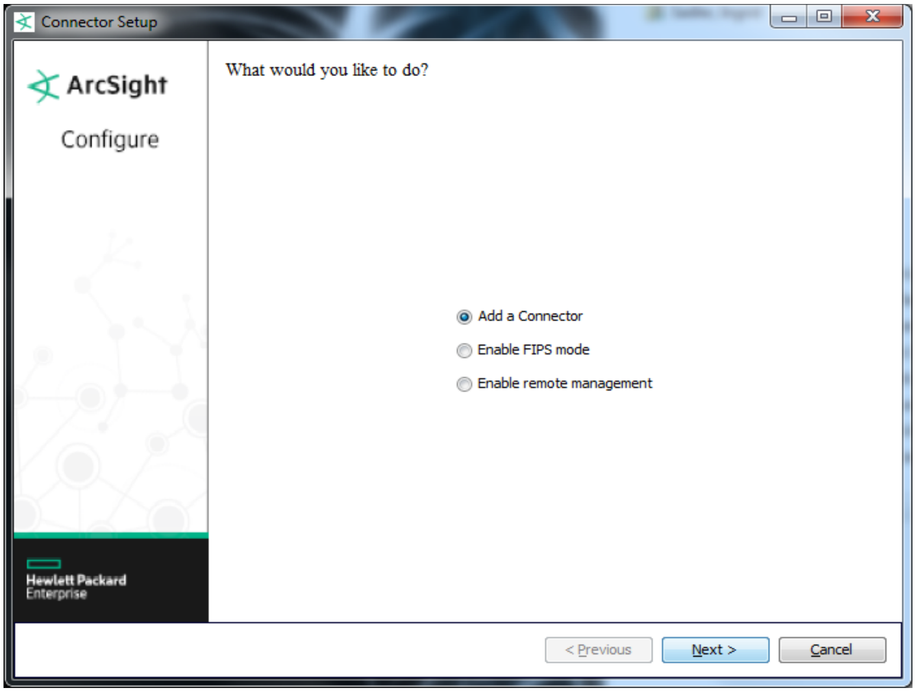
2 Start the SmartConnector Installer by running the executable.

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

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

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

3 When the installation of SmartConnector core component software is finished, the following window is displayed:



What would you like to do?

● Add a Connector

○ Enable FIPS mode

○ Enable remote management

Select Connector and Add Parameter Information

1 Select **Add a Connector** and click **Next**. Enabling FIPS mode and enabling remote management can be configured later in the process after SmartConnector configuration.

2 Select **Syslog Daemon, File, or Pipe** 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; make sure **ArcSight Manager (encrypted)** is selected and click **Next**. (For information about this destination or any of the other destinations listed, see the *ArcSight SmartConnector User Guide*.)

2. Enter values for the **Manager Host Name**, **Manager Port**, **User** and **Password** required parameters. This is 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. 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**.

   To enable remote management, choose **Continue**, click **Next** and select **Enable remote management**. Select Yes for **Enable remote management?** Specify a Remote Management Listener Port or accept the default value of 9001. When queried by the remote management device, the values you specify here for enabling remote management and the port number will be used. Follow the wizard prompts to complete the configuration process.

   If the connector you are installing supports FIPS-compliant mode and you want to enable that mode, select **Continue** rather than **Exit** and click **Next**. Then follow the instructions in "Enable FIPS Mode (optional)". If that section does not appear in this configuration guide, FIPS-compliant mode is not supported for this connector.

For some SmartConnectors, a system restart is required before the configuration settings you made take effect. If a **System Restart** window is displayed, read the information and initiate the system restart operation.

> Save any work on your computer or desktop and shut down any other running applications (including the ArcSight Console, if it is running), then shut down the system.

Complete any **Additional Configuration** required, then continue with "Run the SmartConnector".

For connector upgrade or install instructions, see the *SmartConnector User Guide*.

Enable FIPS Mode

1. To enable FIPS-compliant mode, choose **Continue** rather than **Exit** and click **Next**.

2. After choosing **Continue** and clicking **Next** after connector installation, choose **Enable FIPS Mode** and click **Next**. A confirmation window is displayed when FIPS mode is enabled.

3. Click **Next**. To complete installation of FIPS support, click **Exit**. To enable FIPS Suite B mode, click **Continue**.

4. On the window displayed, select **Modify Connector**.

5. Select **Add, Modify, or remove destinations** and click **Next**.

6. Select the destination for which you want to enable FIPS Suite B mode and click **Next**.

7. Select **Modify destination parameters** and click **Next**.

8 When the parameter window is displayed, select **FIPS with Suite B 128 bits** or **FIPS with Suite B 192 bits** for the **FIPS Cipher Suites** parameter. Click **Next**.

9 The window displayed shows the editing changes to be made. Confirm and click **Next** to continue. (To adjust changes before confirming, click **Previous**.)

10 A summary of the configuration changes made is displayed. Click **Next** to continue.

11 Click **Exit** to exit the configuration wizard.

Troubleshooting Raw TCP Connection

When selecting Syslog Daemon, with Raw TCP, connections remain idle in a CLOSE_WAIT state until closed explicitly by the application. Idle connections can grow over a period of time and can exceed the connector limit or the OS limit. By default the `agents[0].tcppeerclosedchecktimeout=-1` property in `agent.properties` keeps all TCP sessions open, which causes the connectors to crash after too many sessions or files are open.

This can be corrected in the default configuration by allowing adequate time for closing TCP sockets by changing `tcppeerclosedchecktimeout=-1` to `tcppeerclosedchecktimeout=30000` (msec) or greater. Once the parameter is set to 30000 msec, the sessions start to close after the client has closed its connection. In addition, the `agents[0].tcpmaxsockets=1000` parameter can be increased as required to accommodate simultaneous connections from a large number of devices.

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.

Pulse Secure Access Syslog Event Mappings

ArcSight ESM Field	Device-Specific Field
Destination Address	CapturedIP
Device Custom IPv6 Address 2	Source IPv6 Address

ArcSight ESM Field	Device-Specific Field
Device Custom IPv6 Address 3	Destination IPv6 Address
Device Custom String 1	Rule
Device Custom String 2	Duration
Device Custom String 3	Role
Device Custom String 4	Policy
Device Custom String 5	Realm
Device Custom String 6	Group Name
Device Event Class ID	Signature
Device Product	'Pulse Secure Access'
Device Receipt Time	One of (FullTimeStamp, PartialTimeStamp)
Device Severity	SubMessageID
Device Vendor	'Juniper'
Device Version	'IVE 6.X'
Message	Message
Name	Message
Source Address	CapturedIP
Source Host	User
Source Process Name	Process
Source User Name	User
Source User Privileges	Access

Pulse Secure Access Key Value Event Mappings

ArcSight ESM Field	Device-Specific Field
Additional data	duration
Application Protocol	proto
Bytes In	rcvd
Bytes Out	sent
Destination Address	dst
Destination Host Name	dstname
Device Action	op
Device Address	fw
Device Custom String 1	VPN (User Group)
Device Custom String 5	Realm
Device Custom String 6	ID
Device Event Category	type
Device Event Class ID	result
Device Product	'Pulse Secure Access'
Device Receipt Time	One of (DateTimeStamp, time)
Device Severity	pri
Device Vendor	'Juniper'
Device Version	'IVE 6.x'
File Path	arg
Message	Message

ArcSight ESM Field	Device-Specific Field
Name	Message
Request Client Application	agent
Request Protocol	proto
Source Address	src
Source Host	User
Source User Name	user
Source User Privileges	roles