Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for UNIX OS Syslog

Configuration Guide

September 15, 2017

Configuration Guide

SmartConnector for UNIX OS Syslog

September 15, 2017

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 Packard 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 Packard 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

Revision History

Date	Description
09/15/2017	Added support for event collection from RHEL versions 6.7 and 7.3.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
05/16/2016	Added support for RHEL 7.2 and Solaris 11 x86 64-bit platforms.
02/15/2016	Added support for RHEL 7.1 platform. Removed support for the following platforms: AIX 6.1, RHEL 6.0 and 6.1, Oracle Solaris 7, 8, and 9 SPARC, and Oracle Solaris 11 32-bit.
05/15/2015	Added support for Red Hat Linux Enterprise 7.0. Added new Syslog File configuration parameters. Updated field mappings.
02/16/2015	Added parameter for Syslog Daemon connector configuration.
08/15/2014	Added support for Oracle Solaris 11 x86 and Oracle Solaris 11 SPARC.
11/15/2012	Supported ended for AIX versions 4 and 5.

Contents

SmartConnector for UNIX OS Syslog

This guide provides information about installing the SmartConnector for UNIX OS Syslog and configuring the device for syslog event collection.

Collection of data from the following UNIX operating systems is supported:

Oracle Solaris 10 and 11 64-bit (SPARC)
Oracle Solaris 11 64-bit (x86_64)
HP-UX 10 and 11 64-bit
Red Hat Linux Enterprise 6.7, 7.0, 7.1, 7.2, and 7.3 64-bit
IBM AIX 7.1 64-bit

Product Overview

There are three different UNIX OS Syslog SmartConnectors–Daemon, Pipe, and File. These SmartConnectors are described in the "Configuration" section of this guide.

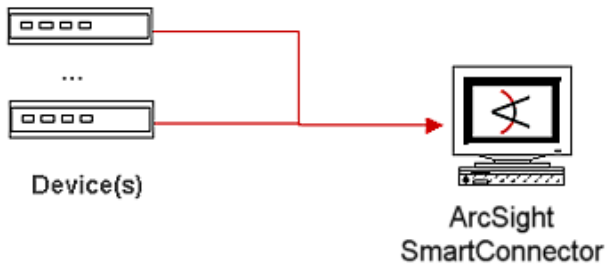
The SmartConnectors for UNIX OS Syslog use a sub-connector architecture that lets them receive events from different types of devices all sending syslog events. For example, the same SmartConnector can process events from a Cisco Router and a NetScreen Firewall simultaneously. The SmartConnector inspects all incoming messages and automatically detects the type of device that originated the message.

For more specific information regarding configuration of specific devices sending syslog events to ArcSight SmartConnectors for Syslog (for example, Cisco Routers and Netscreen Firewall), consult the relevant SmartConnector Configuration Guide particular to those devices. See the *SmartConnectorReadMe.htm* or *index.html* file downloaded with your SmartConnector documentation to locate the individual SmartConnector Configuration Guides.

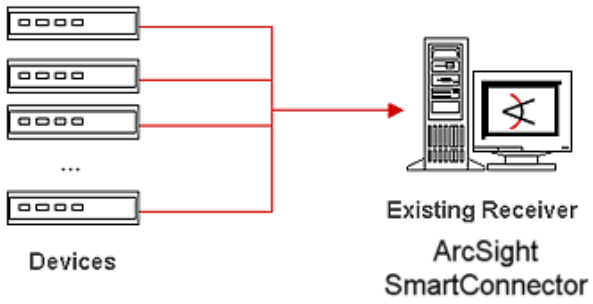
SmartConnector for UNIX OS Deployment

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).

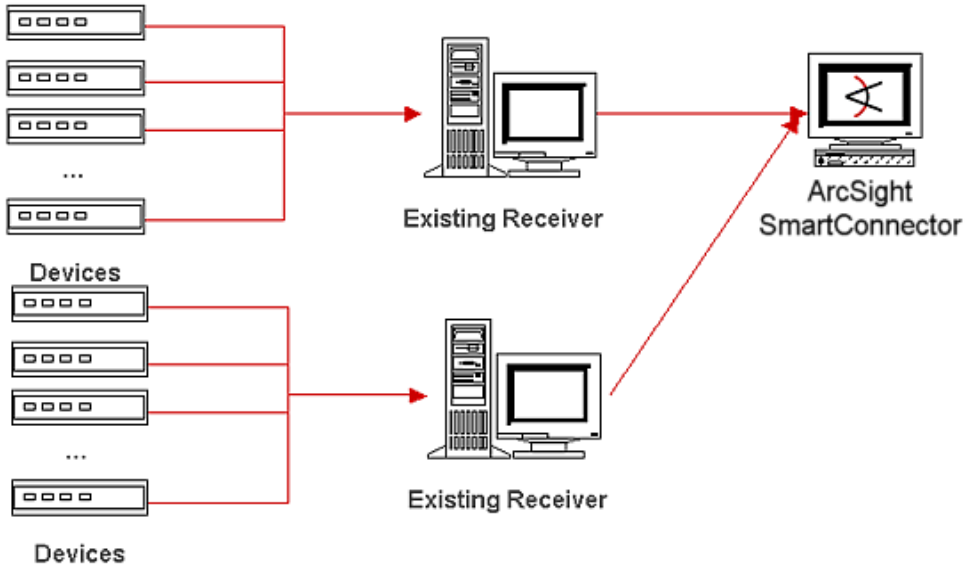


- When a UNIX Syslog Daemon is already in place and configured to receive syslog messages, an extra line in the syslog configuration file can be added to write the events to either a file or a system pipe; the ArcSight SmartConnector would run on the same machine as the Syslog Daemon.



- 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 upon the rate of events sent by the concentrators, you could require more than one ArcSight SmartConnector to handle the event volume.



Configuration

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.

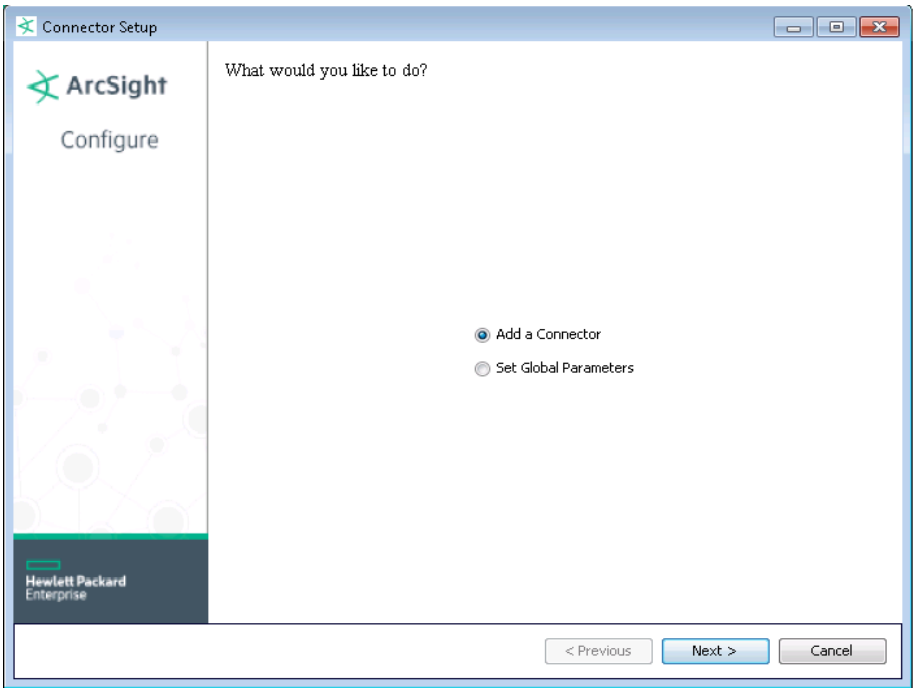
1. Download the SmartConnector executable for your operating system from the HPE SSO site.
2. Start the SmartConnector installation and configuration wizard by running the executable.

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, Syslog Pipe, or Syslog 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.

See the Configuration Guide for each individual syslog connector device for their mappings to ArcSight ESM fields.

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, or High; Medium when Device Severity = warn, Warning, warning, WARNING, or Medium; 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 Number 1	File Descriptor
Device Custom String 1	Module
Device Custom String 2	One of (Facility1, Facility2, _SYSLOG_FACILITY)
Device Custom String 4	PID
Device Custom String 6	login|sshd|httpd
Device Event Class ID	ID portion of message
Device Facility	One of (Facility1,Facility2,_SYSLOG_FACILITY)
Device Host Name	HostName
Device Process Name	ProcessHeader
Device Product	'Unix'
Device Receipt Time	DetectTime
Device Severity	One of (Priority, severity, _SYSLOG_PRIORITY)
Device Vendor	'Unix'
External ID	ID
Message	One of (Message, WholeMessage)
Name	One of (Message, WholeMessage)

IpTables Firewall Logs Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Additional Data	Comment
Additional Data	DatagramID
Additional Data	datagramType
Additional Data	Length
Additional Data	res
Additional Data	TOSPrecedence
Additional Data	TOSType
Additional Data	TTL
Additional Data	urgp

ArcSight ESM Field	Device-Specific Field
Additional Data	window
Destination Address	Destination Address
Destination MAC Address	Destination Mac Address
Destination Port	Destination Port
Device Inbound Interface	Device Inbound Interface
Device Outbound Interface	Device Outbound Interface
Device Process Name	'iptables'
Name	'IPTables Event'
Protocol	name of the protocol
Source Address	Source address
Source MAC Address	Source Mac address
Source Port	Source port
Transport Protocol	TCP | UDP | ICMP | IGMP | ARP

Ipchains Logs Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Additional Data	IPTOS
Application Protocol	protocol
Bytes In	Bytes in transaction
Destination Address	Destination address
Destination Port	Destination port
Destination Translated Port	Destination Translated Port
Device Action	action taken by the device
Device Custom Number 1	TTL
Device Custom Number 2	IP ID
Device Custom String 1	Rule Number
Device Custom String 2	IPChain Name
Device Custom String 4	Pool name
Device Custom String 6	IP Flags
Device Inbound Interface	Device Inbound Interface
Name	'Ipchains Event'
Request URL	URL from which request originated
Source Address	Source address
Source Port	Source port
Source Process Name	Source Process Name
Source User ID	Source User ID
Transport Protocol	TCP | UDP | ICMP | IGMP | ARP

sshd Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Additional Data	channel
Additional Data	duration
Additional Data	euid
Additional Data	exception
Additional Data	NoOfOpenChannels
Additional Data	SourcePid
Additional Data	sshVersion
Additional Data	transferedBytes
Additional Data	tty
Additional Data	version
Application Protocol	'ssh'
Bytes In	bytes transferred in
Bytes Out	bytes transferred out
Destination Host Name	_SYSLOG_SENDER
Destination Process Name	'sshd'
Destination Service Name	Destination service name
Destination User ID	Destination user ID
Destination User Name	Destination User Name
Device Action	action taken by the device
Device Custom IPv6 Address 2	"Source IPv6 Address"
Device Custom IPv6 Address 3	"Destination IPv6 Address"
Device Custom String 1	Kerberos principal
Device Custom String 1	Module
Device Custom String 2	Kerberos realm
Device Custom String 3	KeyType
Device Custom String 4	client hostname
Device Custom String 5	Kerberos status
Device Process Name	One of (Module, ProcessHeader)
Device Severity	High, Medium, or Low
Event Outcome	outcome
File Name	File name
File Path	File path
Reason	reason
Source Address	Source Address
Source Host Name	Source Host Name
Source Port	Source Port
Source Process ID	Source Process ID
Source Process Name	Source Process Name
Source User ID	Source User ID
Source User Name	Source User Name
Transport Protocol	TCP | UDP | ICMP | IGMP | ARP

dhcpd Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Additional Data	additionalInfo
Additional Data	classDeclsNumberToLeasesFile
Additional Data	DUID
Additional Data	errorCode
Additional Data	interface1
Additional Data	interface2
Additional Data	leaseNumber
Additional Data	leaseNumberToDatabase
Additional Data	leaseNumberToFile
Additional Data	oldAddress
Additional Data	transactionID
Application Protocol	'DHCP'
Destination Address	Destination Address
Destination Host Name	Target or destination host name
Destination Mac Address	Destination Mac Address
Device Action	action taken by the device
Device Custom IPv6 Address 2	"Source IPv6 Address"
Device Custom IPv6 Address 3	"Destination IPv6 Address"
Device Custom Number 1	Lease-duration
Device Custom String 1	Subnet
Device Custom String 3	Relay | Relay Agent | Uid
Device Custom String 4	Circuit ID |Old HostName
Device Custom String 5	Remote ID
Device Inbound Interface	Device Inbound Interface
Device Outbound Interface	Device Outbound Interface
File Name	File name
File Size	File size
Source Address	Source address
Source Host Name	_SYSLOG_SENDER
Source MAC Address	Source Mac Address
Source Port	Source port

Connector Verification and Troubleshooting

Depending upon the deployment configuration you choose, messages could pass through any number of intermediate layers before reaching the SmartConnector. Each of these layers should be functioning for the entire system to work.

Here is a list of potential problems and ways to troubleshoot and diagnose them.

1 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: Modify firewall rules to allow syslog traffic through.

2 A local firewall is blocking incoming access to that port.

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

Solution: Modify firewall rules to allow syslog traffic through.

3 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 may need to be passed to it before it will start listening for remote messages. (Check /etc/sysconfig/syslog on RedHat).

4 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.