Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for Cisco VPN Syslog

Configuration Guide

November 30, 2016

Configuration Guide

SmartConnector for Cisco VPN Syslog

November 30, 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 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

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 Packard Enterprise Development LP copyrights, trademarks and acknowledgements:
https://www.protect724.hpe.com/docs/DOC-13026.

Revision History

Date	Description
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.
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.

Contents

SmartConnector for Cisco VPN Syslog

This guide provides information for installing the SmartConnector for Cisco VPN Syslog (both IOS and non-IOS) and for configuring the Cisco VPN device for syslog event collection. Cisco IOS Version 3.6 is supported.

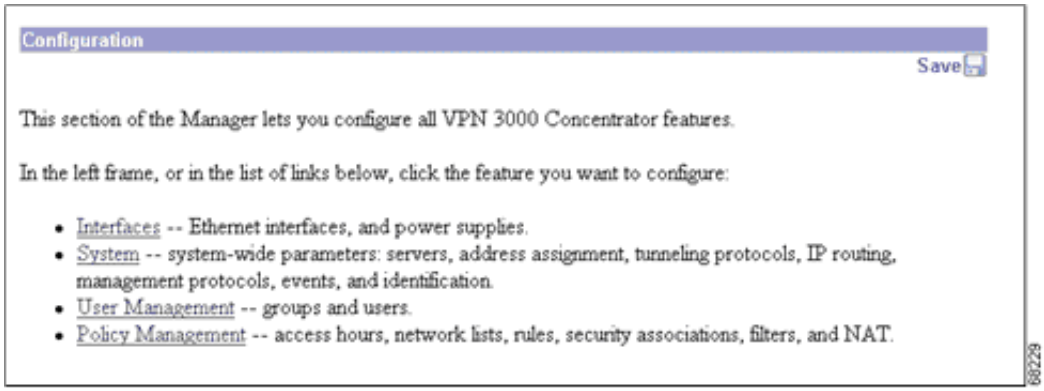
Product Overview

Simple to deploy and operate, the Cisco VPN Client lets organizations establish end-to-end, encrypted VPN tunnels for secure connectivity for mobile employees or teleworkers. This thin design, IP security (IPSec)-implementation is compatible with all Cisco virtual private network (VPN) products.

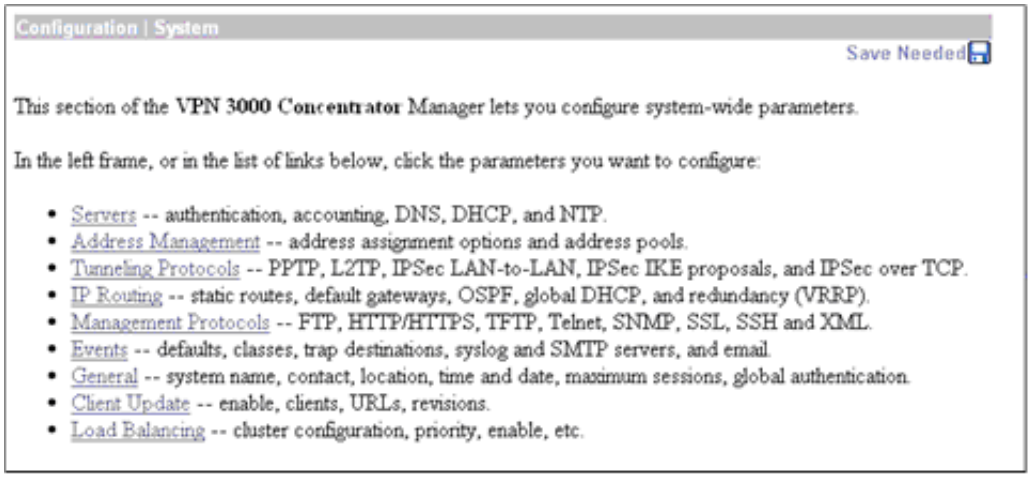
Configuration

Follow these steps to configure the device to send syslog events. For complete configuration information for your Cisco VPN Concentrator, see Cisco's *VPN 3000 Series Concentrator Reference Volume I: Configuration* for Release 3.6.

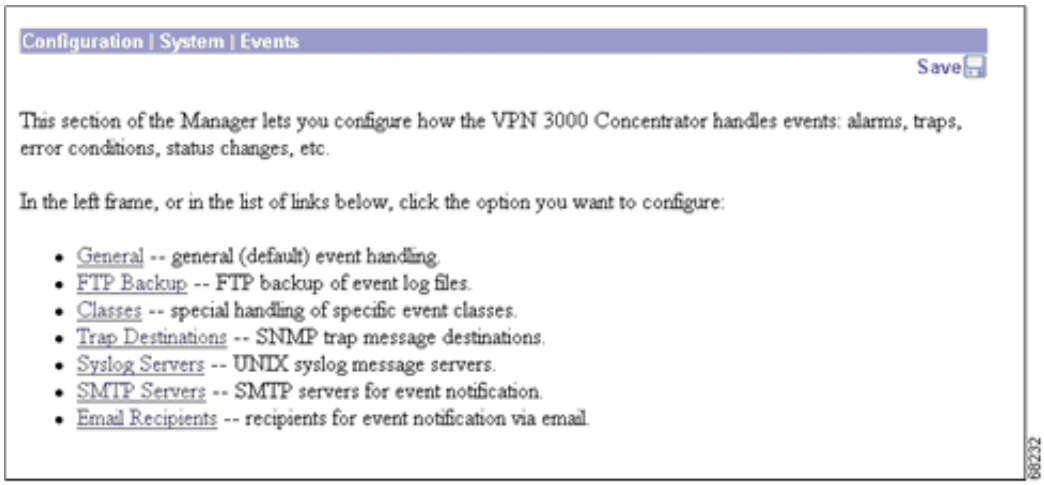
1 Login to the Cisco VPN device as an administrator using a browser interface. In the Concentrator Manager table of contents, click **Configuration**. The Configuration section of the Manager lets you configure all VPN Concentrator features and functions.



2 To configure the device to send syslog events, click the **System** link; the following System Configuration window is displayed. This window lets you set parameters for system-wide functions, such as server access, address assignment, tunneling protocols, IP routing, built-in management servers, system events, and system identification.

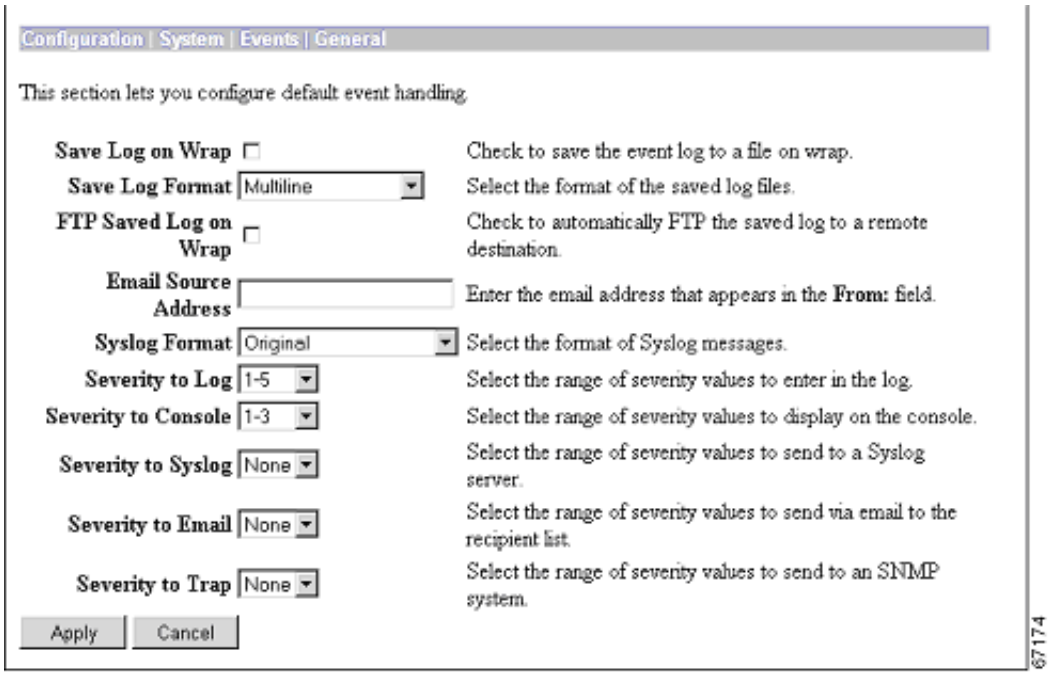


3 Click the **Events** link, from which you can configure handling system events via syslog. An *event* is any significant occurrence within or affecting the VPN 3000 Concentrator, such as an alarm, error condition, network problem, task completion, threshold breach, or status change. The VPN Concentrator records events in an event log. You also can specify that certain events trigger a UNIX syslog record.



This Manager window lets you configure the general, or default, handling of all events. These defaults apply to all event classes. You can override these default settings by configuring specific events for special handling on the **Configuration | System | Events | Classes** windows.

4 Select **General**.



5 Check the **Save Log on Wrap** check box to automatically save the event log when it is full. (The box is unchecked by default.) When the log is full, newer events overwrite older events. If you select automatic save, the system saves the log file to a file in Flash memory with the filename LOGNNNNN.TXT, where NNNNN is an increasing sequence number that starts with 00001 and restarts after 99999. The sequence numbers continue through reboots. For example, if four log files have already been saved, the next one saved after a reboot is LOG00005.TXT.

If Flash memory has less than 2.56 MB of free space, the system deletes the oldest log files to make room for the newest saved log file. It also generates an event that notes the deletion. If there are no old log files to delete, the save function fails, and the system generates an event that notes the failure.

6 Click the **Syslog Format** drop-down menu button and choose the format for all events sent to UNIX syslog servers. For non-IOS VPN Concentrators, select **Original**; for IOS VPN Concentrators, select **Cisco IOS Compatible** format.

7 Click the **Severity to Syslog** drop-down menu button and choose the range of event severity levels to send to a UNIX syslog server by default. The default is **None**. Using the default means that no events are sent to a syslog server.

When you select any severity levels to send, you must also configure the syslog servers on the **'Configuration | System | Events | Syslog Servers'** windows.

Avoid configuring Severity to Syslog with ranges greater than 1-5 for all events. Configuring the severity ranges above 5 for all events greatly impacts system performance. Instead, configure only individual event classes with higher severities. Setting a high range can disable your ability to manage the VPN Concentrator using the browser management interface.

Severity level indicates how serious or significant the event is. It indicates how likely the event is to cause unstable operation of the VPN concentrator, whether it represents a high-level or low-level operation, or whether it returns little or great detail. Level 1 is most significant. The **Original** severities and the **Cisco IOS** severities differ.

IOS Severity	Severity Meaning	Original Severity
0	Emergencies	1
1	Alerts	not used
2	Critical	2
3	Errors	not used
4	Warning	3
5	Notification	4
6	Informational	5, 6
7	Debugging	7-13

Within a severity level category, higher-numbered events provide more details than lower-numbered events, without necessarily duplicating the lower-level details. For example, within the Information category, Level 6 provides greater detail than Level 4, but does not necessarily include the same information as Level 4. Logging higher-numbered severity levels causes performance to deteriorate, since more system resources are used to log and handle these events.

The VPN Concentrator, by default, displays all events of severity level 1 through 3 on the console. It writes all events of severity level 1 through 5 to the event log. You can change these defaults on the **Configuration | System | Events | General** window, and you can configure specific events for special handling on the **Configuration | System | Events | Classes** windows.

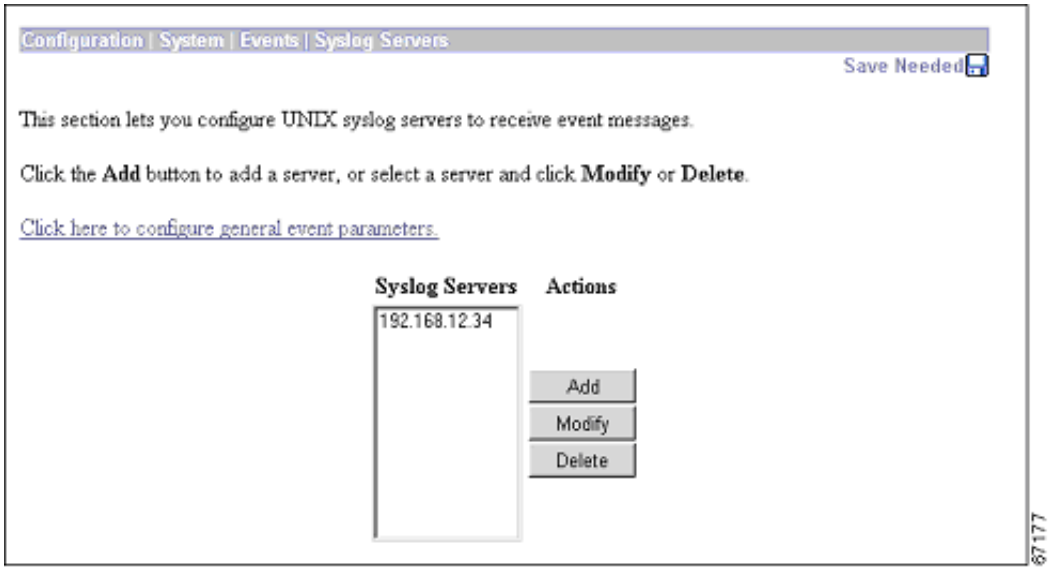
8 To include your settings for default event handling in the active configuration, click Apply. The Manager returns to the **Configuration | System | Events** window.

To save the active configuration and make it the boot configuration, click the **'Save Needed'** icon at the top of the Manager window. To discard your settings, click **'Cancel**.' The Manager returns to the **'Configuration | System | Events'** window.

Configure the Syslog Server

This section lets you configure a syslog server as the recipient of event messages. The VPN Concentrator can send event messages in two syslog formats to configured syslog systems. If you configure any event handling, either default or special, with values in **Severity to Syslog** fields, configure your syslog server in this section.

To configure default event handling and syslog formats, click the highlighted link that says **Click here to configure general event parameters.** To configure special event handling, see the **Configuration | System | Events | Classes** windows.



The Syslog Servers list shows the UNIX syslog servers that have been configured as recipients of event messages. If no syslog servers have been configured, the list shows `--Empty--`. You can add a UNIX syslog server as a recipient of event messages, or modify a configured UNIX syslog server. You can configure a maximum of five syslog servers.

To configure a new syslog server, click **Add**. To modify a syslog server that has been configured, select the server from the list and click **Modify**. To remove a syslog server that has been configured, select the server from the list and click **Delete**. *There is no confirmation or undo*. The Manager refreshes the window and shows the remaining entries in the list.

The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

For **Syslog Server**, enter the IP address or host name of the syslog server to receive event messages. If you have configured a DNS server, you can enter a host name; otherwise, enter an IP address.

For **Port**, enter the UDP port number by which you access the syslog server. Use a decimal number from 0 to 65535. The default value is 514.

For **Facility**, choose the syslog facility tag for events sent to this server. The facility tag lets the syslog server sort messages into different files or destinations. Select **Daemon** for syslog daemons when you are using syslog on a Windows platform; select one of the following, as appropriate:

- Daemon = System daemons.
- Syslog = Internal syslogd-generated messages.
- Local 0 through Local 7 (default) = User defined.

To add this server to the list of syslog servers, click **Add**. Or, to apply your changes to this syslog server, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the Configuration | System | Events | Syslog Servers window and any new server is displayed in the Syslog Servers list.

Reminder:
To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window. To discard your entries, click **Cancel**. The Manager returns to the **Configuration | System | Events | Syslog Servers** window, and the Syslog Servers list is unchanged.

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.

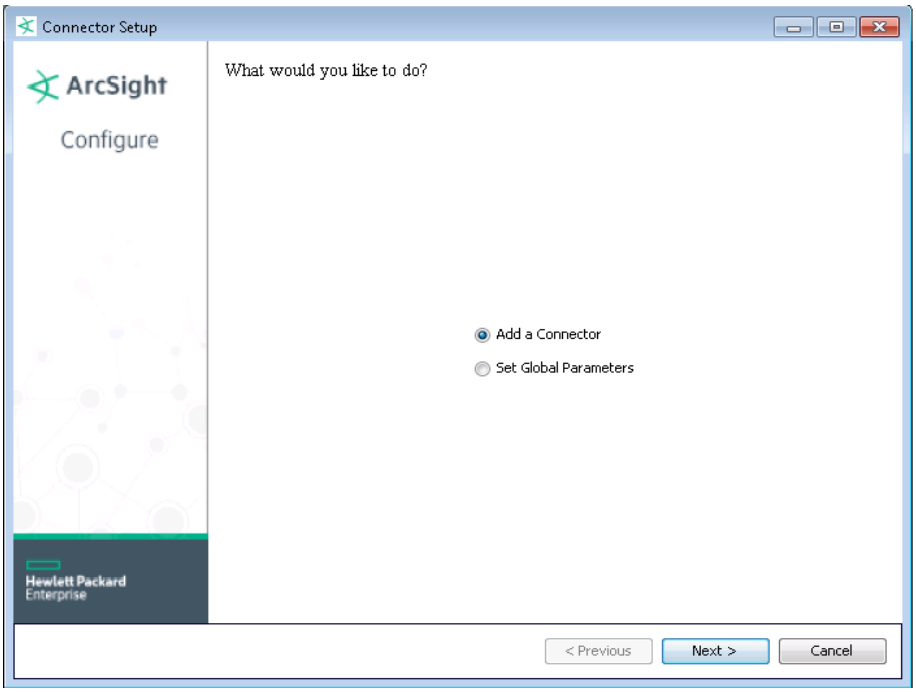
1. Download the SmartConnector executable for your operating system from the HPE SSO site.
2. Start the SmartConnector installation and configuration wizard by running the executable.

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 VPN Field Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Application Protocol	Application Protocol
ArcSight Severity (High)	2 or 3
ArcSight Severity (Low)	6 – 13
ArcSight Severity (Medium)	4 or 5
ArcSight Severity (Very High)	0 or 1
Bytes In	Bytes In
Bytes Out	Bytes Out
Destination Address	Destination IP
Destination DNS Domain	Destination DNS Domain
Destination Port	Destination Port
Destination Translated Address	Destination Translated IP
Destination User Name	User
Destination User Name	Destination User
Detect Time	Timestamp
Device Action	Action taken by the device
Device Custom Number 1	Phase
Device Custom Number 2	Message Number
Device Custom Number 3	Sequence Number
Device Custom String 1	Group
Device Custom String 2	Facility
Device Custom String 3	Mnemonic
Device Custom String 4	Duration
Device Custom String 5	Slot
Device Custom String 6	Rule
Device Event Class ID	MessageId | Module
Device Inbound Interface	Inbound Interface
Device Process Name	Process Name
Device Product	'Cisco VPN'
Device Receipt Time	DetectTime
Device Severity	Severity
Device Vendor	'CISCO'
External ID	ID
File Name	Command
Message	MessageId plus Message
Name	Message
Request URL	Accessed URL
Source Address	Source
Source User Name	User

ArcSight ESM Field	Device-Specific Field
Transport Protocol	Protocol

Cisco VPN Mappings to Additional Data Fields

ArcSight ESM Field	Device-Specific Field
Additional data	CentryAddr
Additional data	ClientType
Additional data	Expected
Additional data	Filter
Additional data	FilterSet
Additional data	Group1
Additional data	Group2
Additional data	Handle
Additional data	handle
Additional data	Header
Additional data	InboundSPI
Additional data	LocalProxy
Additional data	localProxy
Additional data	MAC Addr
Additional data	Mask
Additional data	Name2
Additional data	OutboundSPI
Additional data	pRec
Additional data	RadiusCode
Additional data	RadiusCodeHex
Additional data	RemoteProxy
Additional data	remoteProxy
Additional data	SA
Additional data	SAAddr
Additional data	SequenceNumber
Additional data	server
Additional data	SessionID
Additional data	SessionType
Additional data	SPI
Additional data	TunnelCnt
Additional data	Value
Additional data	ValueHex
Additional data	Where

Troubleshooting

How to verify if Cisco VPN Device is sending Syslog Events or not?

You can verify if the Cisco VPN device is sending syslog events by executing the following steps:

a Make sure that the ArcSight SmartConnector is not running.

b Start listening on the pipe that you configured by executing the following command: (where path/to/pipe is the absolute path to the pipe)

```
cat /path/to/pipe
```

c The command should display the events that are coming from the Cisco VPN device.