

Logger SmartConnector™ Configuration Guide for

Cisco PIX/ASA Syslog

May 15, 2011



Logger SmartConnector™ Configuration Guide for

Cisco PIX/ASA Syslog

May 15, 2011

Copyright © 2010 – 2011 ArcSight, Inc. All rights reserved. ArcSight, the ArcSight logo, ArcSight TRM, ArcSight NCM, ArcSight Enterprise Security Alliance, ArcSight Enterprise Security Alliance logo, ArcSight Interactive Discovery, ArcSight Pattern Discovery, ArcSight Logger, FlexConnector, SmartConnector, SmartStorage and CounterACT are trademarks of ArcSight, Inc. All other brands, products and company names used herein may be trademarks of their respective owners.

Follow this link to see a complete statement of ArcSight's copyrights, trademarks and acknowledgements:

<http://www.arcsight.com/company/copyright/>.

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

This document is ArcSight Confidential.

Revision History

Date	Description
05/15/2011	Update to guide for Logger v.5.1.
11/09/2010	Editorial update.
9/20/2010	First release of Logger SmartConnector documentation supporting Logger v.5.0 – Downloadable Version.

Logger SmartConnector for Cisco PIX/ASA Syslog

ArcSight Logger is a log management solution optimized for extremely high event throughput, efficient long-term storage, and rapid data analysis. This SmartConnector supports Logger 5.0 Downloadable Version.

This guide provides information for installing the SmartConnector for Cisco PIX/ASA Syslog and configuring the device for syslog event collection. Cisco PIX and ASA versions 6.2, 6.3, 7.0, 7.1, 7.2, 8.0, 8.1, 8.2, and 8.3 are supported.

Product Overview

The Cisco PIX Security Appliance Series provides firewall security monitoring and intrusion protection services for the complete security solution. Cisco PIX security appliances provide robust site-to-site and remote-access VPN services.

The Cisco ASA 5500 Series Adaptive Security Appliance is a modular platform that provides the next generation of security and VPN services.

This ArcSight SmartConnector lets you import syslog events generated by the Cisco PIX or ASA device into the ArcSight System. (See the section "Device Event Mapping to ArcSight Data Fields" later in this document for the specific events mapped to fields in the ArcSight database.)



If your appliance has Cisco IDS or Cisco IPS installed, those events are not collected as syslog events. Use the SmartConnector for Cisco Secure IDS RDEP or the SmartConnector for Cisco Secure IPS SDEE for IDS 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 PIX:

```
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—alerts—Take immediate action
- 2—critical—Critical condition
- 3—errors—Error message
- 4—warnings—Warning message
- 5—notifications—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 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 (`syslog.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/syslog.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/syslog.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/syslog.conf` file:

```
*.debug /var/tmp/syspipe
```

For syslog pipe on Linux, use:

```
*.debug | /var/tmp/syspipe
```

- 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:

```
service syslog restart
```

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. The default is `var/log/messages`

After editing the `/etc/syslog.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

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 *Configuring the Syslog SmartConnector* in this guide for more information):

- Syslog Daemon
- Syslog Pipe
- Syslog File

All three syslog connectors are supported for installation on Linux platforms. The syslog daemon connector is also supported for installation on Windows platforms.



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.

SmartConnector Installation

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

- Local access to the machine where the SmartConnector is to be installed
- Administrator passwords

Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported Linux and Windows platforms; for the complete list, see the SmartConnector Product and Platform Support document.

- 1 Download the ArcSight executable for your operating system from the ArcSight Customer Support Site per the instructions provided in the connector release notes.
- 2 Start the ArcSight SmartConnector Installer by running the executable.



When Installing a Syslog Daemon SmartConnector in a UNIX environment, run the executable as 'root' user.

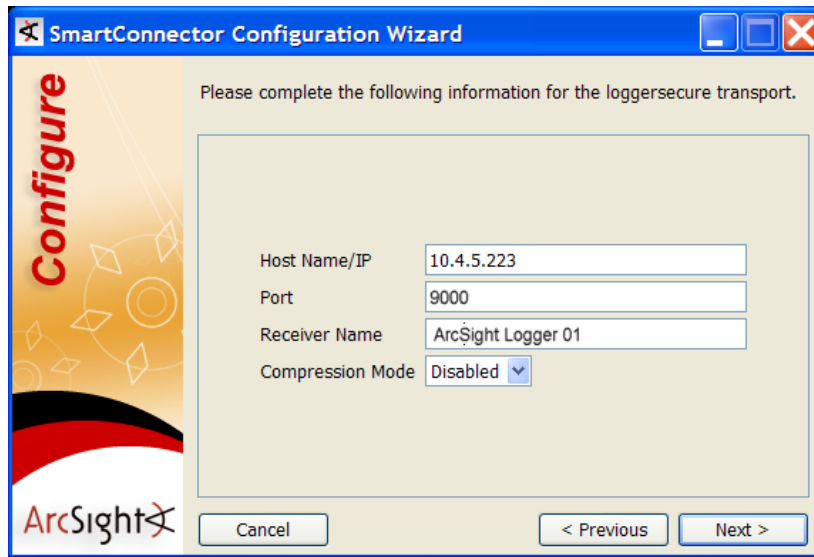
Follow the Installation Wizard through the following folder selection tasks and installation of the core connector software:

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

- 3 When the destination window is displayed, make sure **ArcSight Logger SmartMessage (encrypted)** is selected and click **Next**.



- 4 Before proceeding with step 5, set up the **SmartMessage Receiver** from the Logger appliance (see the *ArcSight Logger Administrator's Guide* for detailed instructions).
- 5 From the Configuration Wizard, enter the Logger **Host Name/IP**, make sure the **Port** number is **9000**, and enter the **Receiver Name**. This setting should match the Receiver name you created in the previous step so that Logger can listen to events from this SmartConnector. Click **Next**.



SmartConnector Configuration Wizard

Please complete the following information for the loggersecure transport.

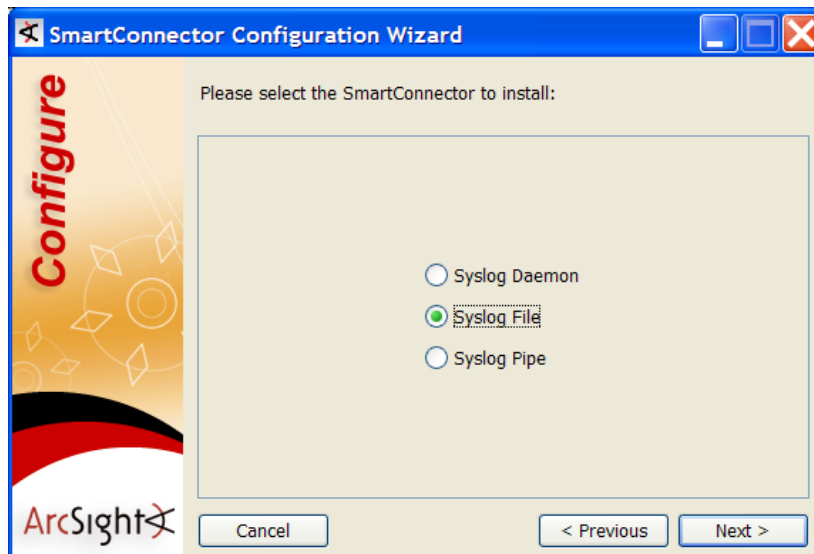
Host Name/IP	10.4.5.223
Port	9000
Receiver Name	ArcSight Logger 01
Compression Mode	Disabled

Buttons: Cancel, < Previous, Next >

- 6 Depending upon your platform, choose between the required connector types.

For **Windows** platforms, **Syslog Daemon** is the only available option.

For **Linux** platforms, select **Syslog Daemon**, **Syslog File**, or **Syslog Pipe**.



SmartConnector Configuration Wizard

Please select the SmartConnector to install:

☐ Syslog Daemon
☒ Syslog File
☐ Syslog Pipe

Buttons: Cancel, < Previous, Next >

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

For **Syslog Daemon**:



SmartConnector Configuration Wizard

Please fill in the required parameters for this SmartConnector.

Configure

Network Port: 514

Ip Address: (ALL)

Protocol: UDP

Cancel < Previous Next >

ArcSight

Syslog Daemon Parameters	<i>Network port</i>	The SmartConnector for Syslog Daemon listens for syslog events on this port.
	<i>IP Address</i>	The SmartConnector for Syslog Daemon listens for syslog events only on this IP address (accept the default (ALL) to bind to all available IP addresses).
	<i>Protocol</i>	The SmartConnector for Syslog Daemon uses the selected protocol (UDP or Raw TCP) to receive incoming messages.

For **Syslog File**:



SmartConnector Configuration Wizard

Please fill in the required parameters for this SmartConnector.

Configure

Path to file: /var/log/messages

Cancel < Previous Next >

ArcSight

Syslog File Parameter	<i>File Absolute Path Name</i>	Absolute path to the file, or accept the default: /var/log/messages
------------------------------	--------------------------------	---

For **Syslog Pipe**:



The screenshot shows the 'SmartConnector Configuration Wizard' window. On the left is a vertical banner with the word 'Configure' in red and the ArcSight logo at the bottom. The main area has a light beige background with the text 'Please fill in the required parameters for this SmartConnector.' Below this is a text input field labeled 'Pipe Absolute Pathname' containing the value '/var/tmp/syspipe'. At the bottom are three buttons: 'Cancel', '< Previous', and 'Next >'.

Syslog Pipe Parameter	<i>Pipe Absolute Path Name</i>	Absolute path to the pipe, or accept the default: /var/tmp/syspipe
----------------------------------	------------------------------------	---

- 8 Enter a name for the SmartConnector and provide other information identifying the connector's use in your environment. Click **Next**.



The screenshot shows the 'SmartConnector Configuration Wizard' window. On the left is a vertical banner with the word 'Configure' in red and the ArcSight logo at the bottom. The main area has a light beige background with the text 'Select a name for your SmartConnector and specify location parameters.' Below this are four text input fields: 'SmartConnector Name' (containing 'Logger Syslog'), 'SmartConnector Location' (containing 'HQ'), 'Device Location' (containing 'Lab1'), and 'Comment' (empty). At the bottom are three buttons: 'Cancel', '< Previous', and 'Next >'.

- 9 Read the SmartConnector summary and click **Next**. If the summary is incorrect, click **Back** to make changes.
- 10 When the SmartConnector completes its configuration, click **Next**. The Wizard prompts you to choose whether you want to run the SmartConnector as a process or as a service.

If you choose **Yes**, to run the SmartConnector **as a service**, the Wizard prompts you to define service parameters for the SmartConnector.

If you choose **No**, to run the SmartConnector as a **standalone application**, go to step 11.



11 After making your selections, click **Next**. The Wizard displays a dialog confirming the SmartConnector's setup and/or service configuration.

12 Click **Finish**.

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.

To uninstall the connector, or for connector upgrade instructions, see the *SmartConnector User's Guide*.

Run the SmartConnector

SmartConnectors can be installed and run in standalone 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 installed standalone, the SmartConnector must be started manually, and is not automatically active when a host is re-started. If installed as a service or daemon, the SmartConnector runs automatically when the host is re-started. For information about connectors running as services or daemons, see the *ArcSight SmartConnector User's Guide*.

For connectors installed standalone, to run all installed SmartConnectors 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.

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
```