

Configuration Guide

Logger SmartConnector™ for Linux Audit Syslog

June 30, 2011



Configuration Guide

Logger SmartConnector™ for Linux Audit Syslog

June 30, 2011

Copyright © 2003-2012 Hewlett-Packard Development Company, L.P. Confidential computer software. Valid license from HP 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.

The information contained herein is subject to change without notice. The only warranties for HP 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. HP shall not be liable for technical or editorial errors or omissions contained herein.

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

<http://www.arcsight.com/copyrightnotice>.

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

This document is confidential.

Revision History

Date	Description
06/30/2012	Update for Logger v5.3.
05/15/2011	First release of guide for Logger v.5.1.

Logger SmartConnector for Linux Audit Syslog

This guide provides information for installing the SmartConnector for Linux Audit Syslog and configuring the device for event collection. Version 1.7 of Linux auditd is supported for pulling events from Red Hat Linux 5, 6, and 6.1 AS and Red Hat Linux Enterprise version 5, 6, and 6.1 platforms.

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 5.3 Downloadable Version.

Product Overview

The Linux auditd daemon can help you detect violations of your security policies. It detects violations of security policy but does not enforce it. Rather, it is similar to network-based intrusion detection systems and host-based intrusion detection systems. Because the audit daemon is part of the Linux kernel, it is included in most major Linux distributions by default.

Configuration

For complete information about the Linux auditd daemon, see the man pages for `auditd`, `auditd.conf`, and `auditctl`. You can access these manual pages by running `man auditd` or `man auditctl`, for example, from the command line of your Linux system.

Linux auditd does not log to syslog by default. To enable syslog logging, edit `# /etc/audit/plugins.d/syslog.conf` and change the line `active = no` to `active = yes`.

Before you can start generating audit logs and processing them, configure the audit daemon itself. Configure how it is started in the `/etc/sysconfig/auditd` configuration file and configure how the audit system functions once the daemon has been started in `/etc/auditd.conf`.

`auditctl` is responsible for controlling the status and some basic system parameters of `auditd`. Using audit rules, `auditctl` controls which components of your system are subjected to the audit and to what extent they are audited. Audit rules can be passed to `auditd` on the `auditctl` command line as well as by composing a rule set and instructing `auditd` to process this file.

`auditd` has built-in functions to watch access attempts to files without needing to monitor the applicable system calls. Administrators can add rules by amending the provided configuration files or at run time using the command line. The default location for the audit daemon rules in `/etc/auditd/audit.rules`.

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.

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.

For Solaris, the default is `/var/adm/messages`

For Linux, 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, Solaris, and AIX 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.

Before you install any SmartConnectors, make sure that the ArcSight Logger product with which the connectors will communicate has already been installed correctly.

For complete product information, read the *ArcSight Logger Administrator's Guide* before installing a new SmartConnector. If you are adding a connector to the Connector Appliance, see the *ArcSight Connector Appliance Administrator's Guide* for instructions, and start the installation procedure at step 3.

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 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.

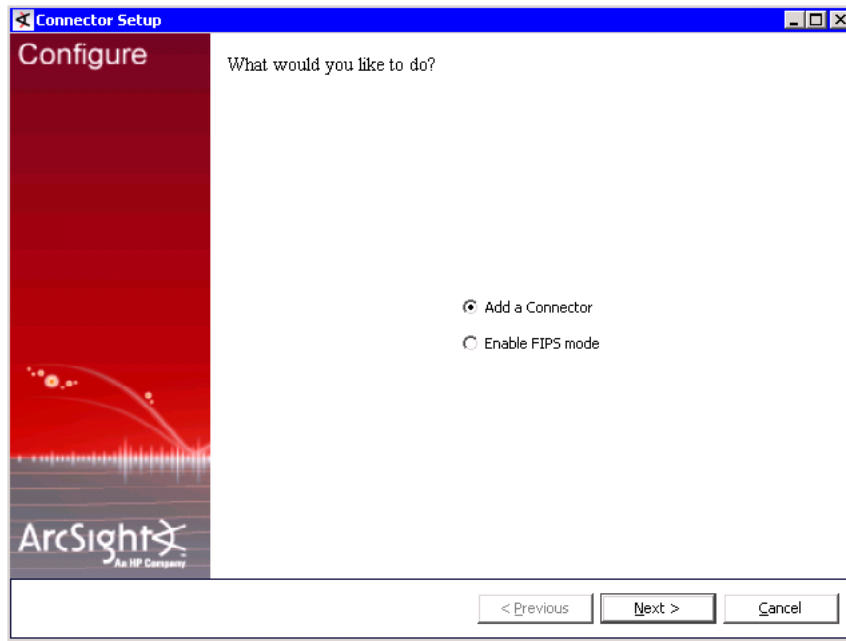


When installing a syslog daemon SmartConnector in a UNIX environment, run the executable as 'root' user.

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.



4 Select **Add a Connector** and click **Next**.

5 Select **Syslog Daemon, Syslog Pipe, or Syslog File** and click **Next**.

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

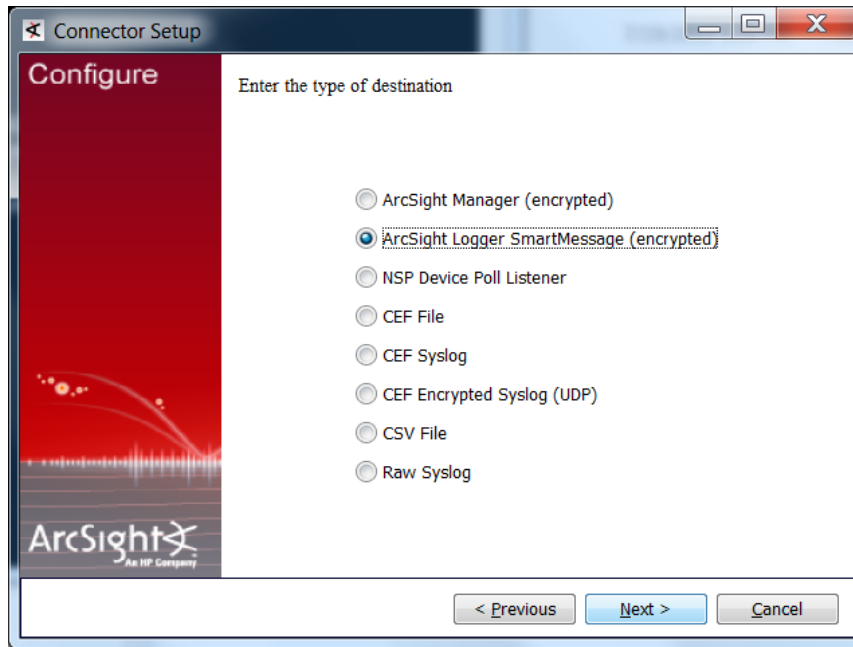
For **Windows** platforms, **Syslog Daemon** is the only available option.

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

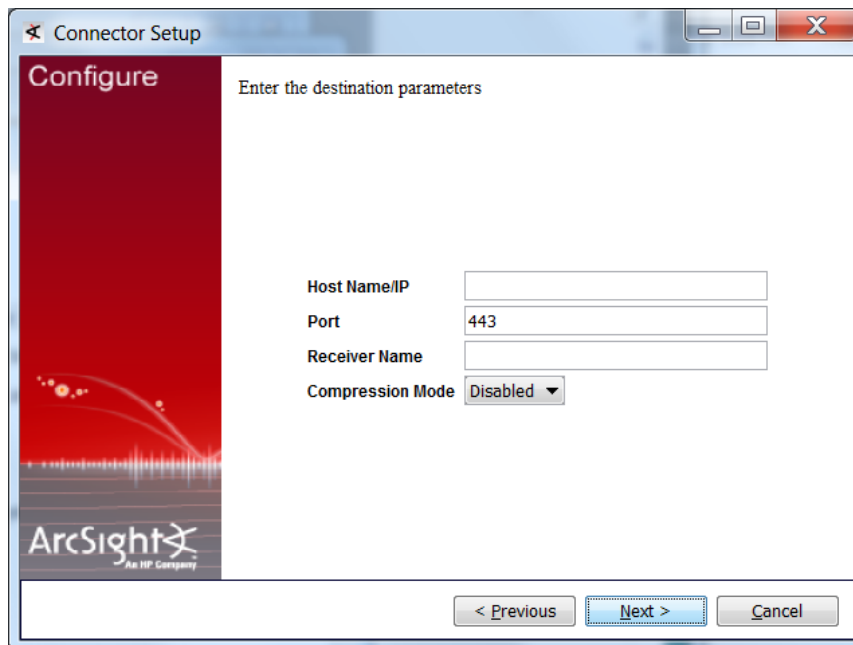
6 Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.

Syslog Daemon Parameters	<i>Network port</i>	The SmartConnector for Syslog Daemon listens for syslog events from this port.
	<i>IP Address</i>	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).
	<i>Protocol</i>	The SmartConnector for Syslog Daemon uses the selected protocol (UDP or Raw TCP) to receive incoming messages.
Syslog Pipe Parameter	<i>Pipe Absolute Path Name</i>	Absolute path to the pipe, or accept the default: /var/tmp/syspipe
Syslog File Parameter	<i>File Absolute Path Name</i>	Absolute path to the file, or accept the default: /var/adm/messages(Solaris) or /var/log/messages (Linux)

7 When the destination window is displayed, make sure **ArcSight Logger SmartMessage (encrypted)** is selected and click **Next**. For information about the other destinations listed, see the *ArcSight SmartConnector User's Guide* as well as the Administrator's Guide for your ArcSight product.

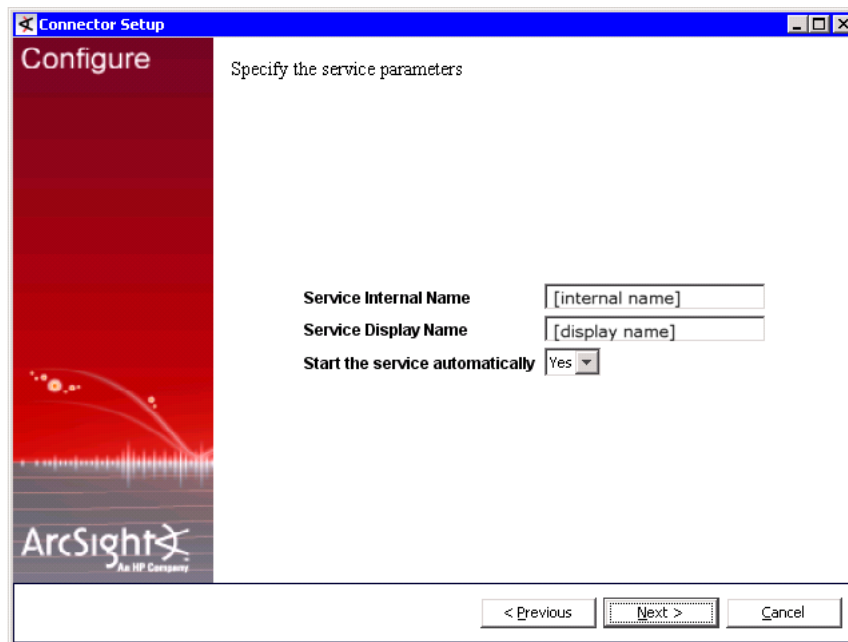


- 8 Before proceeding with step 9, set up the **SmartMessage Receiver** from Logger (see the *ArcSight Logger Administrator's Guide* for detailed instructions).
- 9 From the Configuration Wizard, enter the Logger **Host Name/IP** and **Port**. Make sure the port number is the same that you used to set up your Logger. For the **Receiver Name**, enter the Receiver name you created in the previous step so that Logger can listen to events from this SmartConnector. Click **Next**.



- 10 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.

- 11 The **Add connector Summary** is displayed; review and click **Next**. If the summary is incorrect, click **Previous** to make changes.
- 12 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, skip step 12. If you choose to run the connector as a service, the wizard prompts you to define service parameters.



- 13 Enter the service parameters and click **Next**. The **Install Service Summary** window is displayed.
- 14 Click **Next**.

To complete the installation, choose **Exit** and click **Next**.

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.

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 *HP ArcSight SmartConnector User's 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.