Logger SmartConnector™ Configuration Guide for

Juniper Network and Security Manager Syslog

May 15, 2011

ArcSight
An HP Company

Logger SmartConnector™ Configuration Guide for

Juniper Network and Security Manager Syslog

May 15, 2011

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 Juniper Network and Security Manager 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 Juniper Network and Security Manager (NSM) and configuring the device for syslog event collection. Juniper NSM versions 4.x, 2006.1, 2007.1, 2007.2, 2007.3, 2008.1, 2008.2, 2009.1, 2010.1, 2010.2, 2010.3, and 2010.4 are supported.

Product Overview

Juniper Network and Security Manager is a management system that integrates your individual devices into a single security system controlled from a central location. With NSM, you can manage your network at the system level, using policy-based central management, as well as at the device level, managing all device parameters for devices.

The ArcSight SmartConnector lets you import events generated by the Juniper Network and Security Manager Syslog 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.

Configuration

Configure the Device for Logging

For complete information about Network and Security Manager logging, see the chapter "Configuring the Device for Logging" in the Juniper *Network and Security Manager Administration Guide*. Information in this section has been extracted from that document.

Configure the device and the NSM system for logging so your device can generate log entries and log data. You can configure an individual device to generate attack, alarm, configuration, information, and self-log entries for specific destinations.

You can configure how and where the device sends its log entries. For each destination you can define the category of log entries you want the device to generate and forward to a specific destination, and the severity of log entries you want the device to forward. The severity setting applies to all log types for that destination.

To log an event for a rule, enable logging. Each time your security device matches network traffic to the rule, the device creates a traffic log entry that describes that event. You can enable logging when a session is initialized, closed or both on a security device.

Direct Logs to a Syslog Server

The managed device can generate syslog messages for system events at predefined severity levels and optionally for traffic that policies permit across a firewall. It sends these messages via UDP (port

514) to up to four designated syslog hosts running on UNIX/Linux systems. When you enable syslog reporting, you also specify which interface the devices use to send syslog packets.

To send log entries to a Syslog server, click the **Syslog** option. NSM displays the **Syslog** dialog box. Enter appropriate data into the following fields.

Field	Description
Enable Syslog Messages	Initiates the logging of system event messages to the syslog server.
Port Number	Indicates the port number from where the messages are sent to the syslog server.
Use Trust Zone Interface as Source IP for VPN	Specifies using the interface mapped to the Trust zone as the source of traffic for a VPN.
Include Traffic Log	Specifies that all traffic log events are included as part of the messages sent to the syslog server.
Config Host	Indicates the name of the host device.

Forward Logs

You can forward your log records using one of the following methods:

- Use the Action Manager, a node on the main UI, to configure the management system to forward logs generated within a specific domain or subdomain in NSM.
- Use the log2Action Utility located on the NSM Device Server.

Use the Action Manager

Use the **Action Manager** node to configure the management system to perform actions (such as syslog) on log data based on the criteria you specify. These actions occur for all the managed devices in a specific domain or subdomain.

To enable the management system to export logs, you must configure:

- Action parameters, which define the default log export settings for the management system and determine how the system handles qualified log entries (log entries that match specified log criteria).
- Device log action criteria, which specifies the category and severity of the log entries you want to export. When a log entry meets the specified criteria, it is considered qualified and NSM performs the specified actions defined in the criteria.

To configure action parameters, from the **Action Manager**, select **Action Parameters** to define the default log export settings for the management system. To enable the management system to export qualified logs to the system log, configure the export settings for syslog format.

For exporting to the system log, configure the IP address and the server facility for all of multiple syslog servers to which you want to send qualified logs. NSM uses the specified server when exporting qualified log entries to the system log. To actually export logs to a system log server, you must select **Syslog Enable** using the **Actions** tab in the **Device Log Action Criteria** node.

Use the log2Action Utility

The syslog action directs the system to send logs to a syslog server in syslog format. Specify the IP address of the syslog server that receives the exported log records and the syslog facility.

To export:

1 Login to the Device Server as root, then change to the utility directory by entering:

```
cd /usr/netscreen/DevSvr/utils
```

2 To export to a file, enter:

```
sh devSvrCli.sh --log2action --action --syslog <server> <facility>
```

The Device Server exports all log records to the specified IP address for the syslog server.

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.

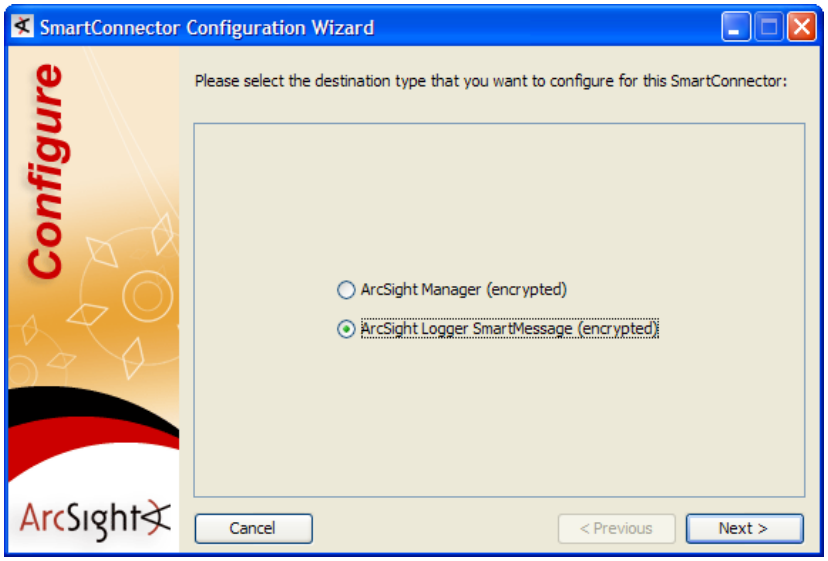
2 Start the ArcSight SmartConnector Installer by running the executable.

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:

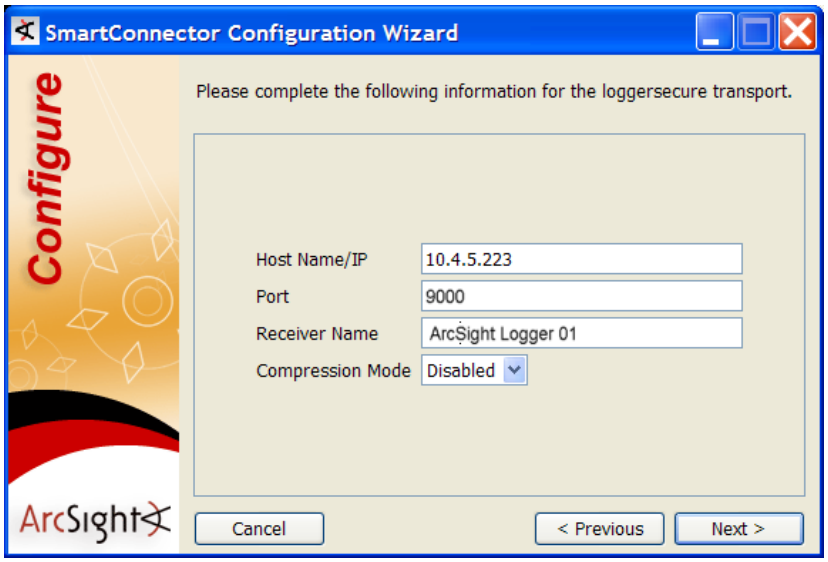
Introduction
Choose Install Folder
Choose Install Set
Pre-Installation Summary
Installing...

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).

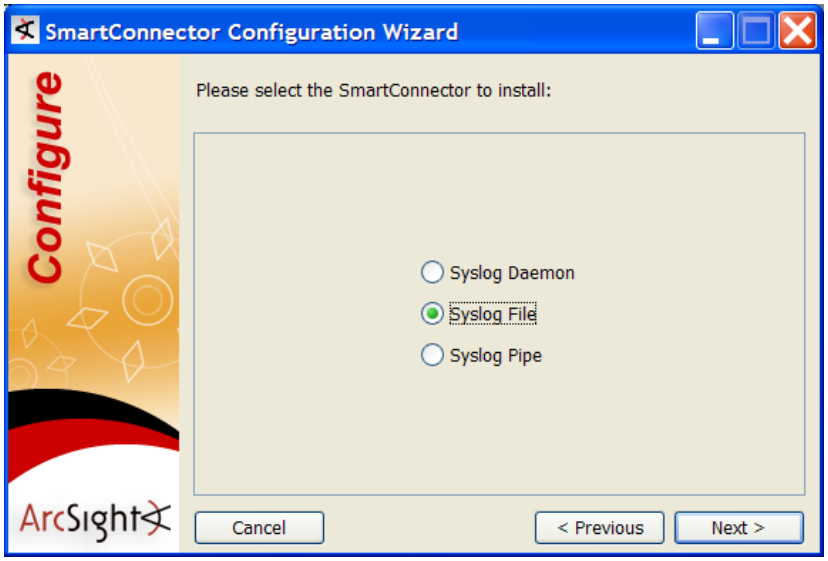
5 From the Configuration Wizard, enter the Logger **Host Name/IP**, make sure the **Port** number is **9000**, and enter the **Receiver Name**. This setting should match the Receiver name you created in the previous step so that Logger can listen to events from this SmartConnector. Click **Next**.



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

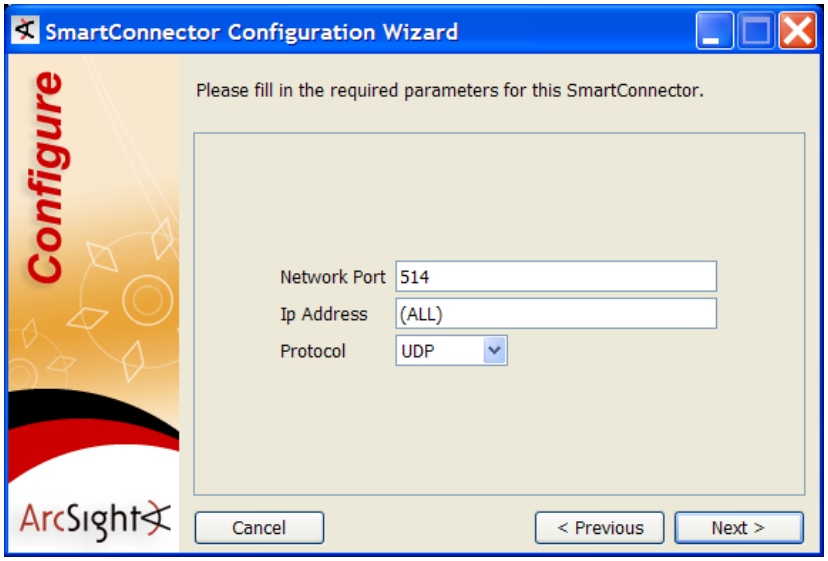
For **Windows** platforms, **Syslog Daemon** is the only available option.

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



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

For **Syslog Daemon**:



Syslog Daemon Parameters	*Network port*	The SmartConnector for Syslog Daemon listens for syslog events on this port.
	IP Address	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).
	Protocol	The SmartConnector for Syslog Daemon uses the selected protocol (UDP or Raw TCP) to receive incoming messages.

For **Syslog File**:

Syslog File Parameter	*File Absolute Path Name*	Absolute path to the file, or accept the default: /var/log/messages

For **Syslog Pipe**:

Syslog Pipe Parameter	*Pipe Absolute Path Name*	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**.

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.

Connector Verification and Troubleshooting

For basic syslog and Communication issues, see the troubleshooting section of the *SmartConnector for UNIX OS Configuration Guide*.

You may encounter the following NetScreen and NSM specific issues during installation.

Syslog Daemon on SmartConnector machine is not receiving messages from NetScreen.

Verification and Action:

- Be sure the NetScreen devices are configured for sending log information to NSM. This includes the log destination, log types, and severities.
- Be sure NSM is configured for syslog reporting as described in the section "Configuring the Juniper NSM Device." Be sure the syslog settings are configured on the correct interface to reach the SmartConnector machine.
- Be sure none of the basic syslog and communication problems as described in the troubleshooting section of the *SmartConnector for UNIX OS Configuration Guide* apply to the current issue.
- Review the policies or rules configured on the NSM and NetScreen devices and the order in which they are applied. Ensure that no rule or policy is defined that blocks the outgoing syslog messages on the interface defined for syslog reporting.

- Review the various log entry viewers on NSM and ensure that some events are being logged.