

# **Logger SmartConnector™ Configuration Guide for**

---

**Intersect Alliance SNARE Syslog**

May 15, 2011



## Logger SmartConnector™ Configuration Guide for

### Intersect Alliance SNARE 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 Intersect Alliance SNARE 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 Intersect Alliance SNARE Syslog and configuring the device for event collection. Snare for Windows version 2.5 is supported. Support for Windows 2008 and Windows Vista events generated by Snare for Windows Vista 1.1.



With Snare Vista 1.1 installed on a Windows 2008 box, the syslog messages may be truncated by Snare and the truncated portion may not be sent in another packet. The connector processes the syslog message as received from Snare, so a part of the message may be lost.

---

### Product Overview

SNARE (System iNtrusion Analysis and Reporting Environment), is an Enterprise audit event log analysis solution that is built using open source technology. SNARE is composed of a central service that provides audit event collection, event analysis, and reporting and archive capabilities, coupled with security agents that are designed for a wide range of operating systems and applications. These SNARE agents have been released as Open Source and are in use worldwide.

Snare for Windows is a Windows NT, Windows 2000, Windows XP, and Windows 2003 compatible service that interacts with the underlying Windows Event Log subsystem to facilitate remote, realtime transfer of event log information.

Snare for Windows Vista is a Windows 2008, Vista, and Windows 2007 compatible service that interacts with the underlying "Crimson" Eventlog subsystem to facilitate remote, realtime transfer of event log data.

The ArcSight SmartConnector lets you import events generated by Intersect Alliance SNARE Syslog 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

This section provides information about configuring your device for syslog event collection, including configuring the syslog server, setting filtering objectives, and syslog-specific connector configuration.

#### Configure the Syslog Server

- 1 Open the **Snare for Windows** icon in the Intersect Alliance folder on the Start menu.
- 2 Choose **Network Configuration**.
- 3 Enter the IP address of the syslog server in the **Destination Snare Server Address** box.
- 4 Change the **Destination Port** from the default 6161 to the standard syslog port 514.

5 Check the **Enable SYSLOG Header** box.

6 Click **Change Configuration**.

The following window is from Snare for Windows:

## SNARE Network Configuration

The following network configuration parameters of the SNARE unit is set to the following values:

Override detected DNS Name with:	<input type="text"/>
Destination Snare Server address(s) (Comma delimited)	<input type="text" value="127.0.0.1"/>
Destination Port (if SYSLOG Header NOT enabled)	<input type="text" value="6161"/>
Use UDP or TCP (Note that the Snare Micro Server only uses UDP at this stage)	<input checked="" type="radio"/> UDP <input type="radio"/> TCP
Perform a scan of ALL objectives, and display the maximum criticality?	<input type="checkbox"/>
Allow SNARE to automatically set audit configuration?	<input checked="" type="checkbox"/>
Allow SNARE to automatically set file audit configuration?	<input checked="" type="checkbox"/>
Export Snare Log data to a file?	<input type="checkbox"/>
Enable SYSLOG Header?	<input checked="" type="checkbox"/>
SYSLOG Facility	<input type="text" value="User"/>
SYSLOG Priority	<input type="text" value="Notice"/>

The following window is from Snare for Windows Vista:

## SNARE Network Configuration

The following network configuration parameters of the SNARE unit is set to the following values:

Override detected DNS Name with:	<input type="text"/>
Destination Snare Server address	<input type="text" value="192.168.40.180"/>
Destination Port	<input type="text" value="514"/>
Perform a scan of ALL objectives, and display the maximum criticality?	<input type="checkbox"/>
Allow SNARE to automatically set audit configuration?	<input checked="" type="checkbox"/>
Allow SNARE to automatically set file audit configuration?	<input checked="" type="checkbox"/>
Export Snare Log data to a file?	<input checked="" type="checkbox"/>
Enable SYSLOG Header?	<input type="checkbox"/>
SYSLOG Facility	<input type="text" value="Local2"/>
SYSLOG Priority	<input type="text" value="Information"/>

## Configure Objectives

Open the **Objective Configuration** window to view existing filtering objectives.

### SNARE Filtering Objectives Configuration

The following filtering objectives of the SNARE unit are active:

Action Required	Criticality	Event ID Match	User Include/Exclude	User Match	General Match	Return	Event Src
<div>Delete</div> <div>Modify</div>	Information	Logon_Logoff	Include	*	*	Success Failure Error Information Warning	Security
<div>Delete</div> <div>Modify</div>	Clear	Process_Events	Include	*	cmd.exe	Success Failure Error Information Warning	Security
<div>Delete</div> <div>Modify</div>	Warning	User_Group_Management_Events	Include	*	*	Success Failure Error Information Warning	Security
<div>Delete</div> <div>Modify</div>	Information	Reboot_Events	Include	*		Success Failure	Security
<div>Delete</div> <div>Modify</div>	Priority	Security_Policy_Events	Include	*		Success Failure Error Information Warning	Security
<div>Delete</div> <div>Modify</div>	Information	*	Include	*		Success Failure Error Information Warning	System Application

Select this button to add a new objective. Add

Click **Modify** to modify attributes for a particular objective. Click **Add** at the bottom of the window to add a new objective.

### SNARE Filtering Objective Configuration

The following parameters of the SNARE objective may be set:

Identify the high level event	<input checked="" type="radio"/> Logon or Logoff <input type="radio"/> Access a file or directory <input type="radio"/> Start or stop a process <input type="radio"/> Use of user rights <input type="radio"/> Account Administration <input type="radio"/> Change the security policy <input type="radio"/> Restart, shutdown and system <input type="radio"/> Any event(s)
Event ID Search Term <i>Optional, Comma separated: only used by the 'Any Event' setting above</i>	<input type="text"/>
General Search Term <i>Wildcards accepted</i>	<input type="text"/>
Select the User Match Type	<input checked="" type="radio"/> Include <input type="radio"/> Exclude
User Search Term <i>User Names, comma separated. Wildcards accepted</i>	<input type="text"/>
Identify the event types to be captured	<input checked="" type="checkbox"/> Success Audit <input checked="" type="checkbox"/> Failure Audit <input checked="" type="checkbox"/> Information <input checked="" type="checkbox"/> Warning <input checked="" type="checkbox"/> Error
Identify the event logs (ignored if any objective other than 'Any event(s)' is selected):	<input checked="" type="checkbox"/> Security <input type="checkbox"/> System <input type="checkbox"/> Application <input type="checkbox"/> Directory Service <input type="checkbox"/> DNS Server <input type="checkbox"/> File Replication
Select the Alert Level	<input type="radio"/> Critical <input type="radio"/> Priority <input type="radio"/> Warning <input checked="" type="radio"/> Information <input type="radio"/> Clear

Change Configuration Reset Form

(c) [Intersect Alliance](#) Pty Ltd 1999-2005. This site is powered by [SNARE for Windows](#).

Each of the objectives provides a high level of control over which events are selected and reported. Events are selected from a group of high level requirements and further refined using selected filters. These groups are provided to service the most common security objectives likely to be encountered. If other event types are required, the **Any event(s)** objective will allow fully tailored objectives to be set.

For each of these groups, a level of importance can be applied. These criticality levels are **critical**, **priority**, **warning**, **information**, and **clear**.

The following objectives should be set to enable the device for syslog event collection by the ArcSight SmartConnector.

- *SNARE Syslog Receiver Objective.* Lets you define server names for incoming syslog messages and define the log format associated with each server.
- *Syslog Reports Objective.* Lets you send syslog events directly to the syslog server on port 514. These events can be from any source and are placed in the GenericSyslog table unless they match a specific log type. The event is usually the priority afforded a syslog event by the program or application that generated it.
- *Syslog Event Summary Objective.* Displays a summary of the syslog Events.
- *Syslog Source Summary Objective.* Displays a summary of the syslog sources. The source usually describes the program or application that generated the syslog event.

For further information about configuring SNARE for Windows, see the Intersect Alliance *Guide to SNARE for Windows*.

## 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:

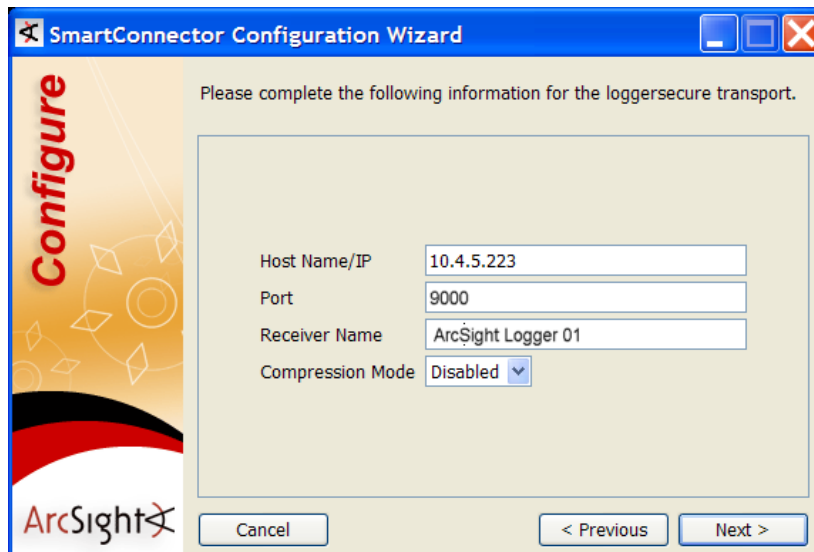
- Introduction
- Choose Install Folder
- Choose Install Set
- Pre-Installation Summary
- Installing...



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



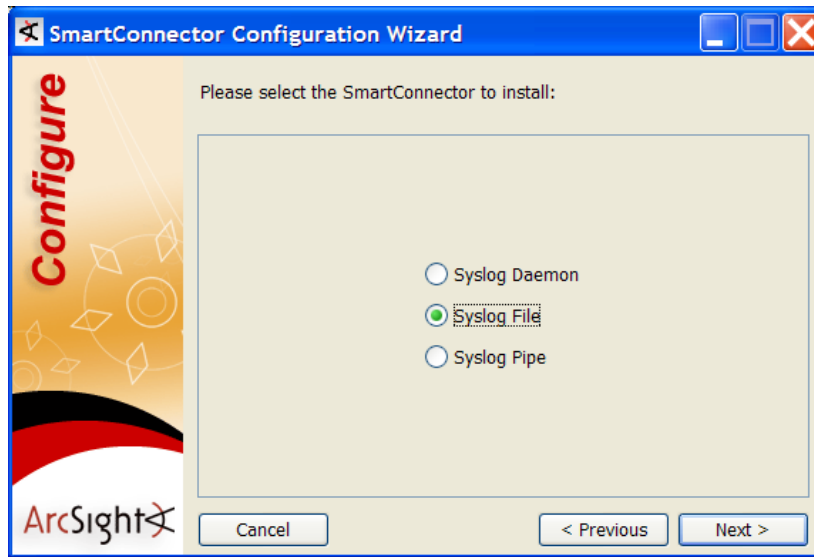
- 4 Before proceeding with step 5, set up the **SmartMessage Receiver** from the Logger appliance (see the *ArcSight Logger Administrator's Guide* for detailed instructions).
- 5 From the Configuration Wizard, enter the Logger **Host Name/IP**, make sure the **Port** number is **9000**, and enter the **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**:



<b>Syslog Daemon Parameters</b>	<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**:



---

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

---

For **Syslog Pipe**:



---

<b>Syslog Pipe Parameter</b>	<b>Pipe Absolute Path Name</b>	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 title bar and a close button. The instruction text reads: 'Select a name for your SmartConnector and specify location parameters.' Below this are four 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.



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 title bar and a close button. The instruction text reads: 'Please enter an internal name and a description for the service. The prefix "arc\_" will be added to the internal name and the prefix "ArcSight " will be added to the display name.' Below this are three input fields: 'Service Internal Name' (containing 'syslog'), 'Service display name' (containing 'Syslog Daemon'), and 'Start the service automatically?' (a dropdown menu set to 'Yes'). At the bottom are three buttons: 'Cancel', '< Previous', and 'Next >'.

- 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.