Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for Intersect Alliance SNARE Syslog

Configuration Guide

November 30, 2016

Configuration Guide

SmartConnector for Intersect Alliance SNARE 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.
06/30/2016	Added an event mapping table for Intersect Alliance SNARE Heartbeat Mappings.
05/15/2015	Added new parameters for Syslog File.
02/16/2015	Added parameter for Syslog Daemon connector configuration.
05/15/2012	Updated installation procedure.
03/30/2012	Updated SNARE versions supported.
05/15/2011	Updated SNARE versions supported.
03/31/2010	General availability of support for Windows Vista events generated by Snare for Windows Vista v1.1.

SmartConnector for Intersect Alliance SNARE Syslog

This guide provides information for installing the SmartConnector for Intersect Alliance SNARE Syslog and configuring the device for event collection. Snare for Windows versions 2.5, 3.0 and 4.0 are supported. Support for Windows 2008 and Windows Vista events generated by Snare for Windows Vista 1.1 is also provided.

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.

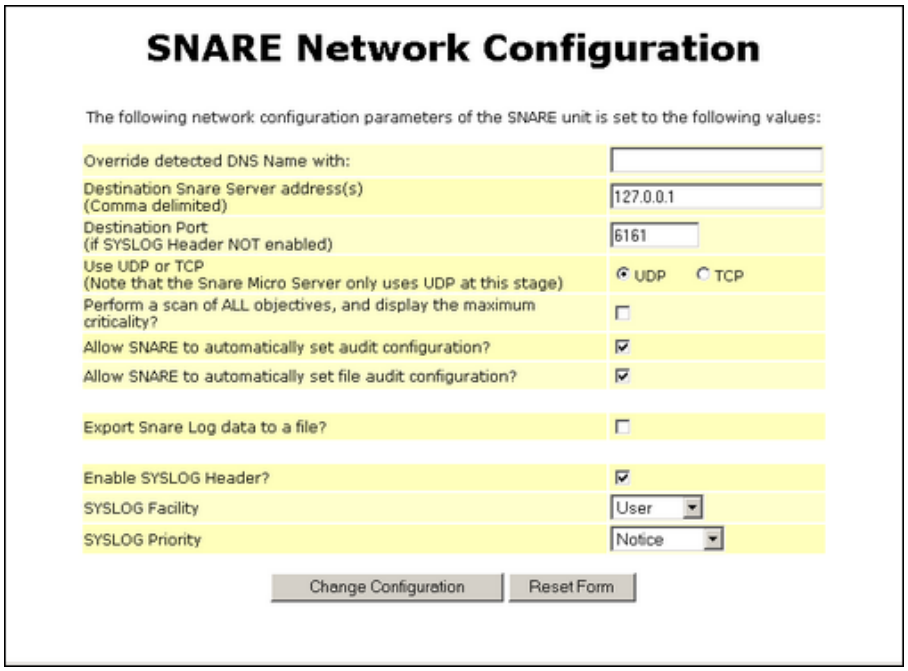
Configuration

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.

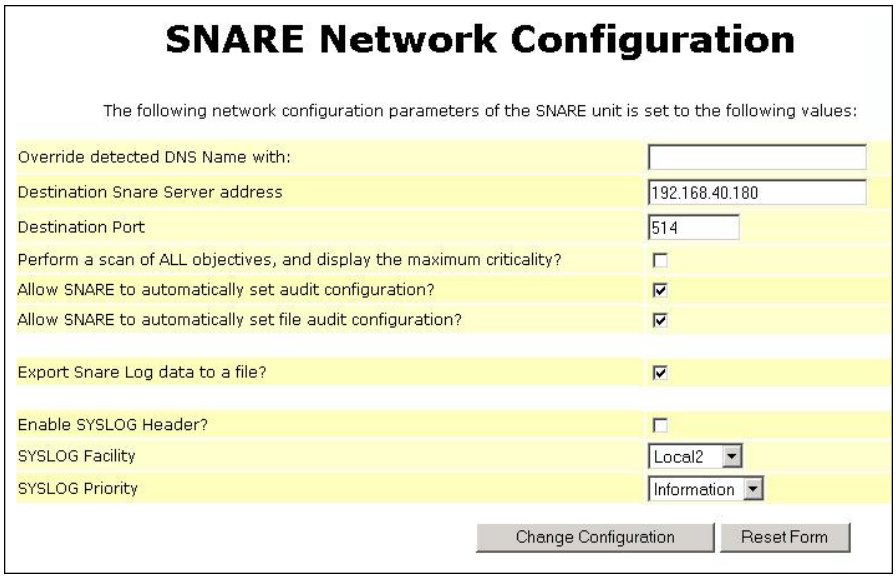
Configure the Syslog Server

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:

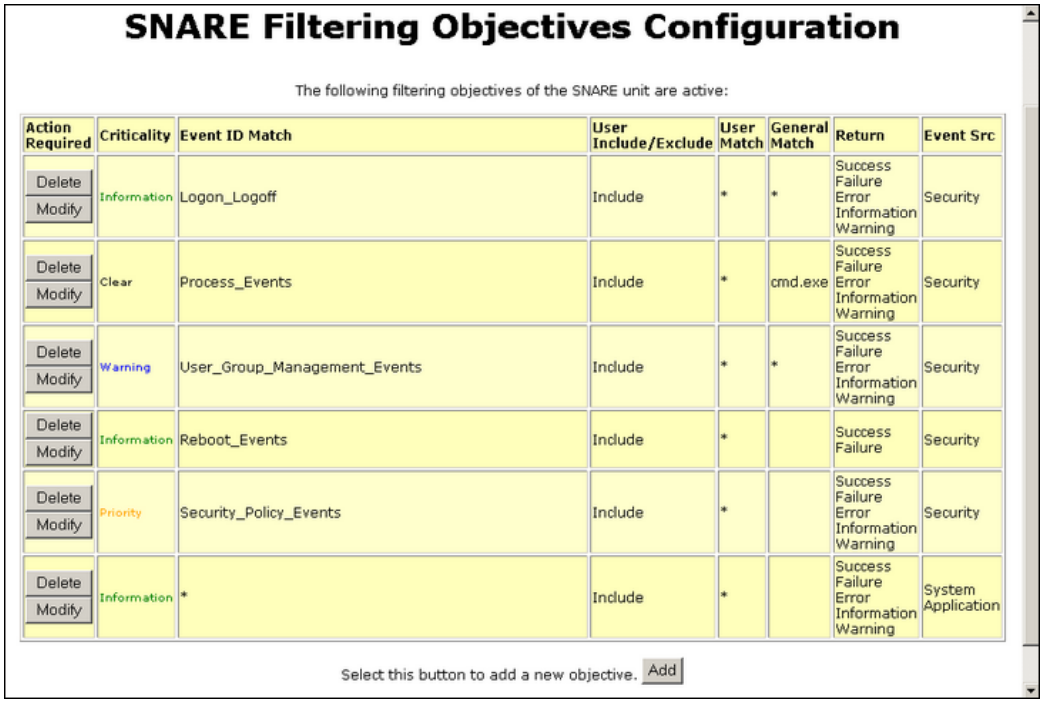


The following window is from Snare for Windows Vista:



Configure Objectives

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



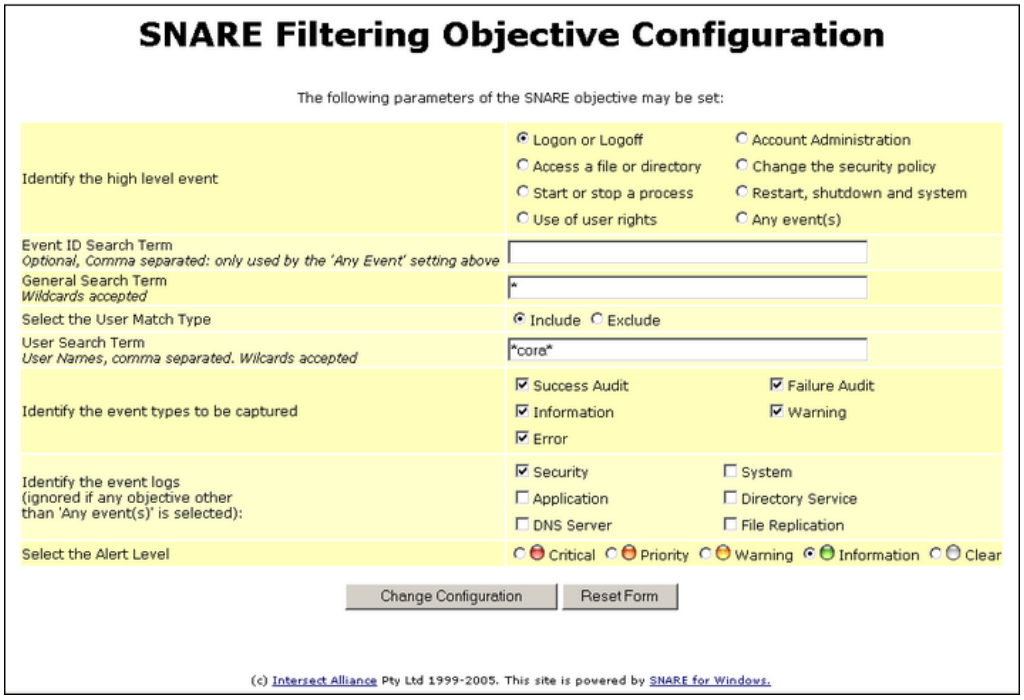
SNARE Filtering Objectives Configuration

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
Delete Modify	Information	Logon_Logoff	Include	*	*	Success Failure Error Information Warning	Security
Delete Modify	Clear	Process_Events	Include	*	cmd.exe	Success Failure Error Information Warning	Security
Delete Modify	Warning	User_Group_Management_Events	Include	*	*	Success Failure Error Information Warning	Security
Delete Modify	Information	Reboot_Events	Include	*		Success Failure	Security
Delete Modify	Priority	Security_Policy_Events	Include	*		Success Failure Error Information Warning	Security
Delete Modify	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	◉ Logon or Logoff ○ Account Administration ○ Access a file or directory ○ Change the security policy ○ Start or stop a process ○ Restart, shutdown and system ○ Use of user rights ○ Any event(s)
Event ID Search Term *Optional, Comma separated: only used by the 'Any Event' setting above*	
General Search Term *Wildcards accepted*	*
Select the User Match Type	◉ Include ○ Exclude
User Search Term *User Names, comma separated. Wilcards accepted*	*cora*
Identify the event types to be captured	☑ Success Audit ☑ Failure Audit ☑ Information ☑ Warning ☑ Error
Identify the event logs (ignored if any objective other than 'Any event(s)' is selected):	☑ Security ☐ System ☐ Application ☐ Directory Service ☐ DNS Server ☐ File Replication
Select the Alert Level	○ Critical ○ Priority ○ Warning ◉ Information ○ 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 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.

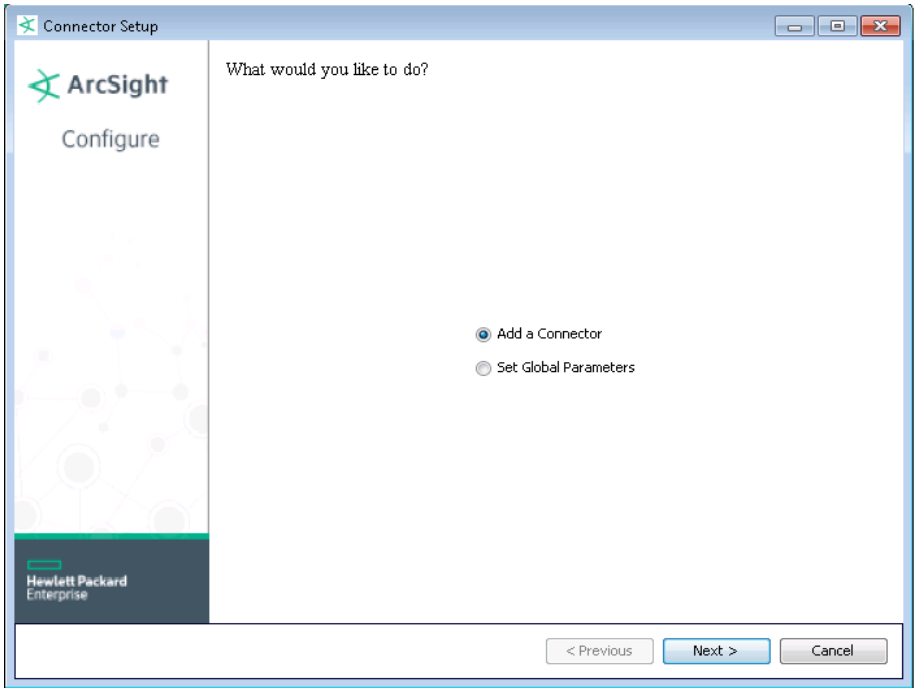
2 Start the SmartConnector installation and configuration wizard by running the executable.

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.

Global Parameter	Setting
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, Syslog File, or Syslog Pipe** 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.

Intersect Alliance SNARE Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Connector (Agent) Severity	Very High = 4; High = 3; Medium = 2; Low = 0, 1
Destination Host Name	ComputerName
Destination User Name	User
Device Custom String 1	OtherInfo
Device Custom String 2	EventlogCategory
Device Custom String 3	EventSource
Device Event Category	EventlogType
Device Event Class Id	EventSource plus EventID
Device Host Name	ComputerName
Device Product	'SNARE'
Device Receipt Time	DetectTime
Device Severity	Criticality
Device Vendor	'Intersect Alliance'
External Id	EventID
Message	Message detail
Name	Message detail

Intersect Alliance SNARE Heartbeat Mappings

ArcSight ESM Field	Device-Specific Field
Device Custom String 1	'Snare Version'
Device Event Category	_type
Device Product	'SNARE'

ArcSight ESM Field	Device-Specific Field
Device Receipt Time	Both(date, time)
Device Vendor	'Intersect Alliance'
Message	_desc