Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for Cisco Secure ACS Syslog

Configuration Guide

October 17, 2017

Configuration Guide

SmartConnector for Cisco Secure ACS Syslog

October 17, 2017

Warranty

Restricted Rights Legend

Revision History

Date	Description
10/17/2017	Added encryption parameters to Global Parameters.
04/17/2017	Updated the mappings table for Cisco Secure ACS RADIUS Accounting.
02/15/2017	End of support for versions 5.1 and 5.2 due to end of support by vendor.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
09/30/2015	Added support for Secure ACS version 5.7. Removed support for versions 4.2 and 5.0 due to end of support by vendor.
05/15/2015	Added new parameters for Syslog File.
02/16/2015	Added parameter for Syslog Daemon connector configuration. Added support for Secure ACS version 5.6.
05/15/2014	Updated "ACS Syslog Messages with More Than Two Segments" section.
09/30/2013	Added support for Secure ACS version 5.4.
05/15/2013	Added support for Secure ACS version 5.3.
12/21/2012	Added parser override information for message segment merge.
11/15/2012	Added Source Host Name mapping for Passed Authentications and Failed Attempts.

Contents

SmartConnector for Cisco Secure ACS Syslog

This guide provides information for installing the SmartConnector for Cisco Secure ACS Syslog and configuring the device for event collection. Cisco Secure ACS versions 5.3, 5.4, 5.6, and 5.7 are supported.

Product Overview

Cisco Secure Access Control Server (ACS) for Windows is a major component of Cisco trust and identity networking security solutions. It extends access security by combining authentication, user and administrator access, and policy control from a centralized identity networking framework.

Configuration

Configure Cisco ACS Syslog Logging

This section provides configuration information for alarm syslog targets, remote log targets, and global logging categories.

Log Message Severity Levels

Log messages can have the following severity levels:

ACS Severity Level	Description	Syslog Severity Level
Fatal	Emergency. ACS is not functioning and immediate action must be taken.	1
Error	Critical or error conditions exist.	3
Warn	Normal, but significant condition.	4
Notice	Audit and accounting messages. Messages of severity NOTICE are always sent to the configured log targets and are not filtered, regardless of the specified severity threshold.	5
Info	Diagnostic informational message.	6
Debug	Diagnostic message.	7

Syslog Message Header Format

Syslog messages are sent to remote syslog servers with this syslog message header format:

```
<pri_num> <YYYY Mmm DD hh:mm:ss> <xx:xx:xx:xx/host_name> <cat_name>
<msg_id> <total_seg> <seg_num>
```

Where the content of the header is described thusly:

- pri_num - The priority value of the message; a combination of the facility value and the severity value of the message. Priority value = (facility value* 8) + severity value. The facility code values are:

- Local0 (Code=16)
- Local1 (Code=17)
- Local2 (Code=18)
- Local3 (Code=19)
- Local4 (Code=20)
- Local5 (Code=21)
- Local6 (Code=22, the default)
- Local7 (Code=23)

- YYYY Mmm DD hh:mm:ss - Date of message generation, based on the local clock of the originating ACS.
  - YYYY - Numeric representation of the year.
  - Mmm - Representation of the month—Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec.
  - DD - Numeric representation of the day of the month. For single-digit days (1 to 9), a space precedes the number.
  - hh - The hour of the day—00 to 23.
  - mm - The minute of the hour—00 to 59.
  - ss - The second of the minute—00 to 59.

Some devices send messages that specify a time zone in the format -/+hhmm, where - and + identify the directional offset from the ACS server's time zone. hh is the number of offset hours and mm is the number of minutes of the offset hour. For example, +02:00 indicates that the message occurred at the time indicated by the time stamp, and on an ACS node that is two hours ahead of the ACS server's time zone.

- xx:xx:xx:xx/host_name - The IP address of the originating ACS, or the hostname.
- cat_name - The logging category name preceded by the CSCOacs string.
- msg_id - The unique message ID; 1 to 4294967295. The message ID increases by 1 with each new message. Message IDs restart at 1 each time the application is restarted.
- total_seg - Total number of segments in a log message. Long messages are divided into more than one segment.
- seg_num - The segment sequence number within a message. Use this number to determine what segment of the message you are viewing.

Create Alarm Syslog Targets

The Monitoring and Report Viewer sends alarm notifications as syslog messages. To receive the syslog messages, a syslog server must be configured with alarm syslog targets.

To configure a syslog server:

1. Navigate to **Monitoring Configuration** > **System Configuration** > **Alarm Syslog Targets**. The Alarm Syslog Targets page displays.
2. Click **Create**.
3. Enter values for the following fields:
   - Option Identification: Name - The name of the alarm syslog target. The maximum length is 255 characters.
   - Option Identification: Description - (Optional) A brief description of the alarm to be created. The maximum length is 255 characters.
   - Configuration: IP Address - IP address of the machine where the syslog server runs.
   - Use Advanced Syslog Options: Port - Port to which the syslog server listens. The default is 514. The value can be from 1 to 65535.
   - Use Advanced Syslog Options: Facility Code - Remote syslog server targets are identified by the facility code. The value can be Local0 through Local7.
4. Click **Submit.**

Configure Remote Log Targets

Logging messages for a specific logging category can be sent to remote log targets residing on a syslog server.

To create a remote log target:

1. Navigate to **System Administration** > **Configuration** > **Log Configuration** > **Remote Log Targets**. The Remote Log Targets page displays.
2. Perform one of the following options:
   - Click **Create**. The **Remote Log Targets > Create** page displays.
   - Click the check box next to the remote log target that you want to duplicate and click **Duplicate**. The Remote Log Targets > Duplicate page displays.
   - Click the check box next to the remote log target that you want to modify and click **Edit**. The Remote Log Targets > Edit page displays.
3. Enter values for the following fields:
   - General: Name - The name of the remote log target. The maximum length is 32 characters.

- General: Description - The description of the remote log target. The maximum length is 1024 characters.
- General: Type - The type of the remote log target. Syslog is the only option.
- Target Configuration: IP Address - IP address of the remote log target, in the format x.x.x.x.
- Target Configuration (v5.6 only): Target Type - Select UDP Syslog, TCP Syslog, or Secure TCP Syslog to define the type of connection used to send logg messages.
- Target Configuration: Use Advanced Syslog Options - Click to enable the advanced syslog options - port number, facility code, and maximum length.
- Target Configuration: Port - The port number of the remote log target used as the communication channel between the ACS and the remote log target. The default is 514.
- Target Configuration: Facility Code - Remote syslog server targets are identified by the facility code. The value can be one of the following: Local0 (Code=16), Local1 (Code=17), Local2 (Code=18), Local3 (Code=19), Local4 (Code=20), Local5 (Code=21), Local6 (Code=22, the default), Local7 (Code=23).
- Target Configuration: Maximum Length - The maximum length of the remote log target messages. Values can be from 200 to 1024.

4 Click **Submit.** The Remote Log Targets page displays with the new remote log target.

Configure Global Logging Categories

Select and configure global logging categories for local targets and remote syslog targets. A logging category contains message codes that describe a function of ACS, a flow, or a use case. Categories are arranged in a hierarchical structure and used for logging configuration.

To select and configure a global logging category:

1 Navigate to **System Administration** > **Configuration** > **Log Configuration** > **Logging Categories** > **Global**. The Logging Categories page displays and you can view the logging categories.

2 Click the name of the logging category you want to configure; or, click the radio button next to the name of the logging category you want to configure and click **Edit**.

3 Enter values for General: Log Severity - For diagnostic logging categories, use the drop-down list box to select the severity level. (For audit and accounting categories, there is only one severity, NOTICE, which cannot be modified.) Valid options are:

- FATAL—Emergency. ACS is not usable and you must take action immediately.
- ERROR—Critical or error condition.
- WARN—Normal, but significant condition. (Default)
- INFO—Informational message.

- DEBUG—Diagnostic bug message.

4 Configure Local Settings for Category.

- Target Configuration: Log to Local Target - Check to enable logging to the local target. (For administrative and operational audit logging category types, logging to local target is enabled by default and cannot be disabled.)

5 Configure Logged Attributes

- Display only. All attributes are logged to the local target.

6 To configure a remote syslog target, click the **Remote Syslog Target** and select targets:

- Available Targets - Select the targets you want for your configuration and move them to the Selected Targets list.

- Selected Targets - This list has the targets you want included in your configuration. You can move unwanted targets to the Available Targets list.

7 Click **Submit.** The Remote Log Targets page displays with the new remote log target.

Format of Syslog Messages in ACS Reports

Syslog messages included in ACS reports have the following format:

<n> *mmm dd hh:mm:ss XX:XX:XX:XX TAG msg_id total_seg seg# A1=V1*

The elements of the message are:

- *n* – The Priority value of the message; it is a combination of facility and severity of the syslog message.
- *mmm dd hh:mm:ss* – Date and time of the message.
- *XX:XX:XX:XX* – IP address of the machine generating this syslog message.
- *TAG* – One of the following values, depending upon the application name.
  - CisACS_01_PassedAuth–Cisco ACS passed authentications.
  - CisACS_02_FailedAuth–Cisco ACS failed attempts.
  - CisACS_03_RADIUSAcc–Cisco ACS RADIUS accounting.
  - CisACS_04_TACACSAcc–Cisco ACS TACACS+ accounting.
  - CisACS_05_TACACSAdmin–Cisco ACS TACACS+ administration.
  - CisACS_06_VoIPAcc–Cisco ACS VoIP accounting.
  - CisACS_11_BackRestore–ACS backup and restore log messages.

- CisACS_12_Replication–ACS database replication log messages.
- CisACS_13_AdminAudit–ACS administration audit log messages.
- CisACS_14_PassChanges–ACS user password changes log messages.
- CisACS_15_ServiceMon–ACS service monitoring log messages.
- CisACS_16_ApplAdmin–ACS appliance administration audit log messages.

- L*msg_id* – Unique message ID. All segments of one message share the same message ID.
- *total_seg* – Total number of segments in this message.
- *seg#* – Segment sequence number within this message segmentation.
- *A1=V1* – Attribute-value pairs delimited by a comma (,) for Cisco ACS log messages and the message itself.

Facility Codes

ACS syslog messages use the following facility values:

- **4** – Security and authorization messages. This value is used for all AAA related messaged (failed attempts, passed attempts, accounting, and so on).
- **13** – Log audit. This value is used for all other ACS report messages.

All ACS syslog messages use a severity value of 6 (informational). For example, if the facility value is 13 and the severity value is 6, the Priority value is 110 ((8 x 13) + 6). The Priority value appears according to the syslog server setu7p, and might appear as one of the following:

- **System3.Info**
- **<110>**

You cannot configure the format of the syslog facility and severity on ACS.

The following sample syslog message shows how the facility code and other information might look in a ACS-generated syslog message:

```
<110> Oct 16 08:58:07 64.103.114.149 CisACS_!#_AdminAudit  18729fp11 1 0
AAA Server=tfurman-w2k,admin-username-local_login,browser4-
ip=127.0.0.1,text-message=Administration session finished,
```

In this example, <110> represents the calculated value when the facility code is 13 (the log audit facility code).

Message Length Restrictions

When an ACS message exceeds the syslog standard length limitation or target length limitation, the message content is split into several segments:

- If all attribute-value elements fit into one segment, no segmentation is performed.
- If the message does not fit into one segment, the message is split between attribute-value pairs, keeping an attribute-value pair complete within the segment.
- In rare cases when one attribute-value pair is too long to fit in one segment all by itself, the value is segmented between sequenced segments of the message. Such segmentation might occur if an attribute value contains several hundreds of characters. In general, ACS attribute values are designed to avoid such length.

All segments of one message have exactly the same header. The `<msg_id>` and `<total_seg>` values are shared between all components. The `<seg#>` is set according to the number of segments and the relative part of the content that follows.

Use the following message length restrictions:

- For sending messages to a standard syslog server, the maximum message length should be 1024 bytes.
- For sending messages to Cisco Security Monitoring, Analysis, and Response System (MARS), the maximum message length should be 500 bytes.
- Message segmentation should be used when the original message, including header and data, exceeds length limitations.

ACS Syslog Messages with More Than Two Segments

When an ACS syslog message has more than two segments, the parser processes the first segment and appends additional key/value pairs from the segments that follow to merge them all into one event.

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.

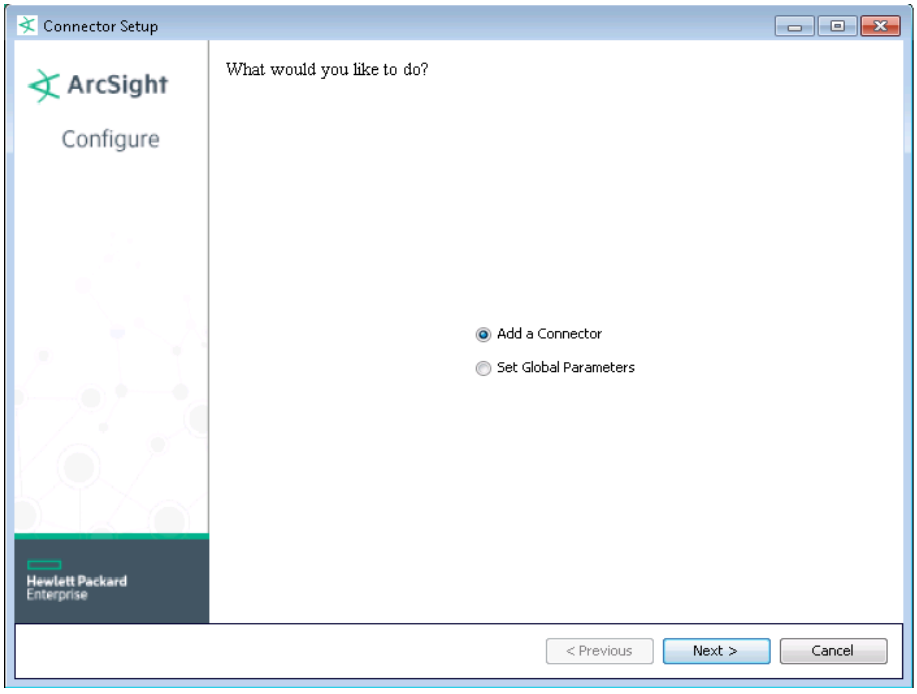
2 Start the SmartConnector installation and configuration wizard by running the executable.

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:

Parameter	Setting
FIPS mode	Select 'Enabled' 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 'Disabled'.
Remote Management	Select 'Enabled' 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 'Disabled'.
Remote Management Listener Port	The remote management device will listen to the port specified in this field. The default port number is 9001.
Preferred IP Version	When 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. The initial setting is IPv4.

The following parameters should be configured only if you are using HPE SecureData solutions to provide encryption. See the *HPE SecureData Architecture Guide* for more information.

Parameter	Setting
Format Preserving Encryption	Data leaving the connector machine to a specified destination can be encrypted by selecting ‘Enabled’ to encrypt the fields identified in ‘Event Fields to Encrypt' before forwarding events. If encryption is enabled, it cannot be disabled. Changing any of the encryption parameters again will require a fresh installation of the connector.
Format Preserving Policy URL	Enter the URL where the HPE SecureData Server is installed.
Proxy Server (https)	Enter the proxy host for https connection if any proxy is enabled for this machine.
Proxy Port	Enter the proxy port for https connection if any proxy is enabled for this machine.
Format Preserving Identity	The HPE SecureData client software allows client applications to protect and access data based on key names. This key name is referred to as the identity. Enter the user identity configured for HPE SecureData.
Format Preserving Secret	Enter the secret configured for HPE SecureData to use for encryption.
Event Fields to Encrypt	Recommended fields for encryption are listed; delete any fields you do not want encrypted and add any string or numeric fields you want encrypted. Encrypting more fields can affect performance, with 20 fields being the maximum recommended. Also, because encryption changes the value, rules or categorization could also be affected. Once encryption is enabled, the list of event fields cannot be edited.

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 proceed with "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, File, or 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 *ArcSight 101* for more information about the ArcSight data fields.

Device Vendor and Device Product fields may sometimes show UNIX rather than the actual vendor and product names.

Cisco Secure ACS General Mappings

ArcSight ESM Field	Device-Specific Field
Connector (Agent) Severity	Very High = FATAL, High = ERROR, Medium = WARN, Low = INFO, DEBUG, NOTICE, Unknown
Device Custom Number 1	ConfigVersionId
Device Event Category	msg
Device Event Class Id	tag
Device Host Name	address
Device Product	'Cisco Secure ACS'
Device Receipt Time	timestamp
Device Severity	One of (severity, mergedevent.deviceSeverity, "Unknown")
Device Vendor	'CISCO'
Device Version	ACSVersion
External ID	msgid
Message	message
Name	msg

Cisco Secure ACS Administrative and Operational Audit Mappings

ArcSight ESM Field	Device-Specific Field
Destination Address	AdminIPAddress
Destination Service Name	AdminInterface
Destination User Name	AdminName
Device Custom String 1	AdminSession

Cisco Secure ACS Failed Attempts

ArcSight ESM Field	Device-Specific Field
Application Protocol	Protocol
Destination Address	Device IP Address
Destination NT Domain	ADDomain
Destination Port	Device port
Destination Service Name	Service
Destination User Name	User
Device Custom String 1	AcsSessionID
Device Custom String 2	Port
Device Custom String 3	AuthorizationPolicyMatchedRule
Device Custom String 4	Authen-Method
Device Custom String 5	Type
Device Custom String 6	NetworkDeviceGroups
Event Outcome	Response one of (Pass=Success, Fail=Failure)
Reason	Response

ArcSight ESM Field	Device-Specific Field
Source Host Name	Remote-Address
Source User Name	UserName

Cisco Secure ACS Passed Authentications

ArcSight ESM Field	Device-Specific Field
Application Protocol	Protocol
Destination Address	oneOfAddress(DestinationIPAddress,Device IP Address)
Destination NT Domain	ADDomain
Destination Port	Destination Port
Destination Service Name	Service
Destination User Name	User
Device Custom String 1	AcsSessionID
Device Custom String 2	Port
Device Custom String 3	AuthorizationPolicyMatchedRule
Device Custom String 4	ExternalGroups
Device Custom String 5	Type
Device Custom String 6	NetworkDeviceGroups
Event Outcome	Response one of (Pass=Success, Fail=Failure)
Source Host Name	Remote-Address
Source User Name	UserName

Cisco Secure ACS TACACS Accounting

ArcSight ESM Field	Device-Specific Field
Destination Host Name	Remote-Address
Destination Service Name	Service
Destination User Name	User
Device Action	AcctRequest-Flags
Device Custom String 1	AcsSessionID
Device Custom String 2	Port
Device Custom String 4	Authen-Method
Device Custom String 5	Type
Device Custom String 6	NetworkDeviceGroups

Cisco Secure ACS TACACS Diagnostics

ArcSight ESM Field	Device-Specific Field
Destination Host Name	Remote-Address
Destination Service name	Service
Destination User Name	User
Device Custom Number 2	SessionId
Device Custom String 1	AcsSessionID
Device Custom String 3	Device Port

ArcSight ESM Field	Device-Specific Field
Device Custom String 5	Type
Event Outcome	Response one of (Pass=Success, Fail=Failure)

Cisco Secure ACS Policy Diagnostics

ArcSight ESM Field	Device-Specific Field
Application Protocol	Protocol
Device Custom String 1	AcsSessionID
Device Receipt Time	Time and Date
Source User Name	UserName

Cisco Secure ACS RADIUS Diagnostics

ArcSight ESM Field	Device-Specific Field
Destination Address	NAS-IP-Address
Destination Host Name	Called-Station-ID
Destination Mac Address	Called-Station-ID
Destination Port	DestinationPort
Destination User Name	User-Name
Device Custom Sring 5	Service-Type
Device Custom String 1	AcsSessionID
Device Custom String 2	NAS-Port
Device Custom String 3	Device Port
Source Mac Address	Calling-Station-ID

Cisco Secure ACS System Statistics

ArcSight ESM Field	Device-Specific Field
Additional data	SysStatsUtilizationNetwork
Device Custom String 1	role (Role Name)

Cisco Secure ACS Authentication Flow Diagnostics

ArcSight ESM Field	Device-Specific Field
Device Custom String 1	AcsSessionID
Source User Name	UserName

Cisco Secure ACS Administrator Authentication and Authorization

ArcSight ESM Field	Device-Specific Field
Source User Name	UserName

Cisco Secure ACS Identity Stores Diagnostics

ArcSight ESM Field	Device-Specific Field
Application Protocol	Protocol
Device Custom String 1	AcsSessionID
Source User Name	UserName

Cisco Secure ACS RADIUS Accounting

ArcSight ESM Field	Device-Specific Field
Destination Address	Device IP Address
Destination User Name	User-Name
Device Address	Destination IP Address
Device Custom String 1	AcsSessionID
Device Custom String 2	NAS-Port
Device Custom String 5	Service-Type
Device Custom String 6	NetworkDeviceGroup
Source Address	Framed-IP-Address