Micro Focus Security ArcSight Connectors

SmartConnector for SAP Security Audit File

Configuration Guide

October 22, 2018

Configuration Guide

SmartConnector for SAP Security Audit File

October 22, 2018

Warranty

Restricted Rights Legend

Trademark Notices

Revision History

Date	Description
10/04/2018	Added support for version 6.17
10/17/2017	Added encryption parameters to Global Parameters.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
05/15/2013	Updated installation parameters for version number.
03/29/2013	Added GA support for SRM, BW and R/3 on AIX 7.1.
02/15/2013	Added beta support for SRM, BW and R/3 on AIX 7.1. Updated mappings.
02/21/2012	Added support for ERP 6.0.
05/15/2012	Added new installation procedure.
02/11/2010	Added support for FIPS Suite B and CEF File transport.

SmartConnector for SAP Security Audit File

This guide provides information for installing the SmartConnector for SAP Security Audit File and configuring the device for audit log event collection. SAP ERP Versions 4.6c, 4.7,6.0 and 6.17 are supported.

When configuring the connector to use BW, set the encoding to UTF-16.

There are two SmartConnectors for SAP Security Audit:

- **SAP Security Audit File, Folder Follower (this SmartConnector)**
  This connector does not process SAP Audit logs in real time. During the installation, you configure the SmartConnector with a temporary folder that it monitors continuously for any audit log files deposited. These events are processed immediately and sent to the ArcSight Manager. Typically, audit log files are copied into this temporary folder every day just after they are rotated by the SAP Application Server.

- **SAP Real-Time Security Audit Multiple Folder File**
  This connector processes the audit logs in real time for more than one server. During installation, the SmartConnector is configured with folders into which SAP Servers log their audit records, as well as with a set of file names that contain the audit records. This allows the SmartConnector to read events from multiple SAP Servers running either the same or differing versions of SAP. The specified file names can be regular file names or can contain the current date. The date-based file names change every day and the connector automatically detects and reads new files as soon as the SAP Server starts logging into them.

Product Overview

The Security Audit Log is a tool designed for auditors who need to take a detailed look at what occurs in the SAP System. By activating the audit log, you keep a record of those activities you consider relevant for auditing. You can then access this information for evaluation in the form of audit analysis reports. With the Security Audit Log, SAP Systems keep records of all activities corresponding to designated filters.

Configuration

Security Audit Log

The Security Audit Log is a tool designed for auditors who need to take a detailed look at what occurs in the SAP System. By activating the audit log, you keep a record of those activities you consider relevant for auditing. You can then access this information for evaluation in the form of an audit analysis report.

The audit log's main objective is to record:

- Security-related changes to the SAP System environment (for example, changes to user master records)
- Information that provides a higher level of transparency (for example, successful and unsuccessful logon attempts)
- Information that enables the reconstruction of a series of events (for example, successful or unsuccessful transaction starts)

Specifically, you can record the following information in the Security Audit Log:

- Successful and unsuccessful dialog logon attempts
- Successful and unsuccessful RFC logon attempts
- RFC calls to function modules
- Successful and unsuccessful transaction starts
- Successful and unsuccessful report starts
- Changes to user master records
- Changes to the audit configuration

The audit files are located on the individual application servers. You specify the location of the files and their maximum size in the following profile parameters:

rsau/enable
: Activates the audit log on an application server. 0 (audit log is not activated) is the default value.

rsau/local/file
: Specifies the location of the audit log on the application server. The default value is `/usr/sap/<SID>/<instno>/log/ audit_<SAP_instance_number>`.

rsau/max_diskspace_local
: Specifies the maximum length of the audit log. The default value is 1,000,000 bytes.

rsau/selection_slots
: Specifies the number of selection slots for the audit. The default value is 2.

Defining Filters

You define the events that the Security Audit Log should record in filters; you can specify the following information in the filters:

- User
- SAP System client

- Audit class (for example, dialog logon attempts or changes to user master records)
- Weight of event (for example, critical or important)

The number of filters you can specify is defined in the profile parameter rsau/selection_slots .

You can either define static profiles(see "Maintaining Static Profiles") or change filters dynamically (see "Changing Filters Dynamically") using the Security Audit Log configuration tool. For each allocated filter, a tabstrip appears in the lower section of the screen.

1. Select the tabstrip for the filter you want to define.
2. Enter the **Client** and **User** names in the corresponding fields. (You can use the wildcard (*) value to define the filter for all clients or users. However, a partially generic entry such as 0* or ABC* is not possible.)
3. Select the corresponding Audit classes for the events you want to audit.
4. Audit events are divided into three categories: critical, important, and non-critical. Select the corresponding categories to audit.
   - Only critical
   - Important and critical
   - All
5. If you want to define the events to audit more specifically:
   a. Choose **Detailed configuration**. A table is displayed that contains a detailed list of the audit classes with their corresponding event classes (critical, severe, non-critical) and message texts.
   b. Select the events you want to audit. You can either select a single event by activating the **Recording** indicator for a specific event, or select all events for an entire audit class by choosing the audit class descriptor (for example, Dialog logon).
   c. Choose **Accept changes**. The filter tabstrips are redisplayed. If you have made detailed settings, then the audit class and event class indicators no longer appear in the corresponding filter tabstrip. To cancel the detailed settings and reload the default configuration, choose **Reset**.
6. To activate the filter, select the **Filter active** indicator.
7. Continue with "Defining Static Profiles" or "Changing Filters Dynamically."

Defining Static Profiles

You specify the information you want to audit in filters that you can either:

1 Create and save permanently in the database in static profiles.

   If you use this option, all of the application servers use identical filters for determining which events should be recorded in the audit log. You only have to define filters once for all application servers. You can also define several different profiles that you can alternatively activate.

2 Change dynamically on one or more application servers.

   With this option, you can dynamically change the filters used for selecting events to audit. The system distributes these changes to all active application servers.

Filters saved in static profiles take effect at the next application server start.

The following profile parameters must be set:

Profile Parameter	Description
rsau/enable	Enables the Security Audit Log.
rsau/local/file	Names and locations of the audit files.
rsau/max_diskspace/local	Maximum space to allocate for the audit files.
rsau/selection_slots	Number of filters to allow for the Security Audit Log.

Procedure:

1 To access the Security Audit Log configuration screen from the SAP standard menu, choose **Tools -> Administration -> Monitor -> Security Audit Log -> Configuration**.

   The **Security Audit: Administer Audit Profile** window is displayed with the **Static configuration** tabstrip activated. If an active profile already exists, it is displayed in the **Active profile** field.

2 Enter the name of the profile to maintain in the **Displayed profile** field.

   If you are creating a new audit profile, choose **Profile -> Create**. To change an existing profile, choose **Profile -> Display <-> Change**. To display an existing profile before changing it, choose **Profile -> Display**.

The lower section of the screen contains tabstrips for defining filters. The number of tabstrips correspond to the value of the profile parameter rsau/selection_slots . Within each tabstrip, you define a single filter.

1 Define Filters for your profile.

2 Make sure the **Filter active** indicator is set for each of the filters you want to apply to your audit.

3 Save the data.

4 To activate the profile, choose **Profile ' Activate**.

5 Shut down and restart the application server to make the changes effective.

The filters you define are saved in the audit profile. If you activate the profile and restart the application server, actions that match any of the active filter events are then recorded in the Security Audit Log.

> On some UNIX platforms, you also need to clear shared memory by explicitly executing the program cleanipc. Otherwise, the old configuration remains in shared memory and the changes to the static profile do not take effect.

Changing Filters Dynamically

You specify the information you want to audit in filters that you can either:

- **Create and save permanently in the database in static profiles.** If you use this option, all of the application servers use identical filters for determining which events should be recorded in the audit log. You only have to define filters once for all application servers. You can also define several different profiles that you can alternatively activate.
- **Change dynamically.** With this option, you can dynamically change the filters used for selecting events to audit. The system distributes these changes to all active application servers.

This topic concentrates on dynamically changing filters. For information on defining filters in static profiles, see "Maintaining Static Profiles."

> These changes are active until they are changed or the application server is shut down.

The following profile parameters must be set:

Profile Parameter	Description
rsau/enable	Enables the Security Audit Log.
rsau/local/file	Names and locations of the audit files.
rsau/max_diskspace/local	Maximum space to allocate for the audit files.
rsau/selection_slots	Number of filters to allow for the Security Audit Log.

1 To access the Security Audit Log configuration screen from the SAP standard menu, choose **Tools -> Administration -> Monitor -> Security Audit Log -> Configuration**. The **Security Audit: Administer Audit Profile** window is displayed with the **Static configuration** tabstrip activated.

2 Choose the **Dynamic configuration** tabstrip or **Goto Dynamic configuration** from the menu. In the upper section of the window, you receive a list of the active instances and their auditing status. The lower section of the window contains tabstrips for maintaining filters.

3 Choose **Configuration -> Display <-> Change**.

4 Define filters for the application server.

5 Make sure the **Filter active** indicator is set for each of the filters you want to apply to the audit on the application server.

6 To distribute the filter definition to the application servers, choose **Configuration -> Activate Audit** and confirm that you want the filter configuration distributed to all application servers.

If you receive a program failure, make sure you have the authorization S_RFC with the value SECU in your authorization profile. (The system uses remote function calls to obtain a list of servers and therefore, you need the appropriate authorizations.)

If you receive a program failure, make sure you have the authorization S_RFC with the value SECU in your authorization profile. (The system uses remote function calls to obtain a list of servers and therefore, you need the appropriate authorizations.)

The audit filters are dynamically created on all active application servers. If you activate the profile or profiles, any actions that match any of these filters are recorded in the Security Audit Log. Changes to the filter definitions are effective immediately and exist until the application server is shut down.

Example Filters

With the Security Audit Log, SAP Systems keep records of all activities corresponding to designated filters.

Typical scenarios for using the Security Audit Log include:

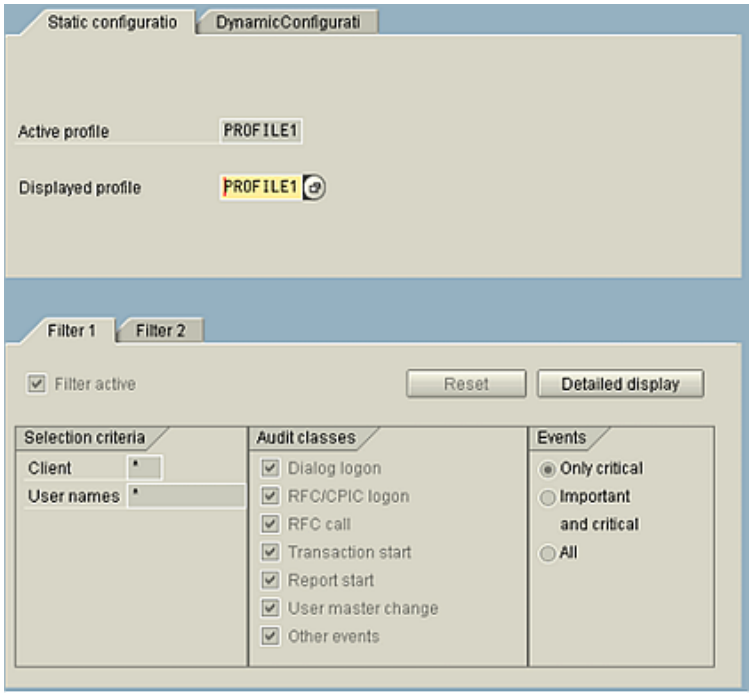
- Recording specific security-critical events, for example, to monitor logon attempts using the standard user SAP*.
- Recording the activities that a specific user executes, for example, to monitor the activities performed by a remote support user.

Filter for Recording All Security-Critical Events

To set up a filter for recording all security-critical events, define a static filter with the following criteria defined:

Field or Group	Entry
Client	*
User	*
Audit classes	Activate all classes
Events	Select *Only critical*

All critical events will be recorded for all users in all clients. See the following figure.



You can define the filter more specifically by choosing individual audit classes or entering more detailed data (for example, by entering SAP* as the User name.) Choose **Detailed display** to even more specifically define the various events to audit.

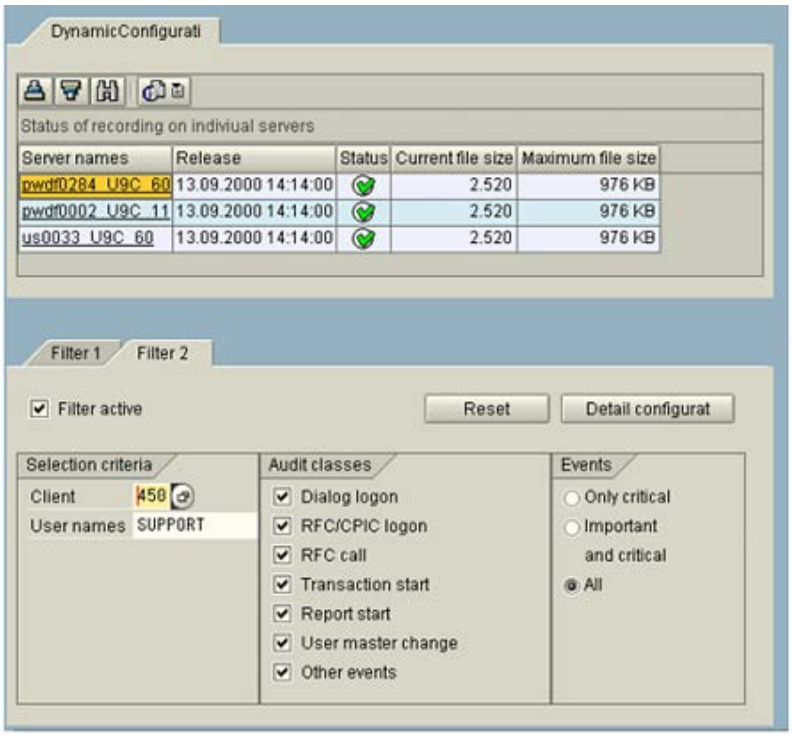
Filter for Recording Activities Performed by a Specific User

To set up a filter for recording security-critical events, define a dynamic filter with the following criteria defined:

Field or Group	Entry
Client	<client>
User	<user_ID>
Audit classes	Activate all classes
Events	Select *All*

By defining the filter as dynamic, you can activate the filter for the time frame that the user works in the system and deactivate it when the user is finished (for example, for a remote support user).

The following figure shows a filter that is activated to monitor the activities performed by the user SUPPORT in client 450.



Deleting Old Audit Files

The Security Audit Log saves its audits to a corresponding audit file on a daily basis. Depending on the size of your SAP System and the filters specified, you may be faced with an enormous quantity of data within a short period of time. SAP recommends archiving your audit files on a regular basis and deleting the original files as necessary.

Use this procedure to delete old audit files. You can either delete the files from all application servers or from only the local server where you are working. If an application server is not currently active, it will be included in the next reorganization.

This procedure only deletes the audit log file(s)! It does not perform any other administrative tasks such as archiving. If archives are necessary for future references, you must manually archive them before deleting.

You cannot purge files that are less than 3 days old!

1. To access the Security Audit Log reorganization tool from the SAP standard menu, choose **Tools -> Administration -> Monitor -> Security Audit Log -> Reorganization**. The **Security Audit: Delete Old Audit Logs** window is displayed.

2. Enter the **Minimum age of files to delete** (default = 30 days). This value must be greather than 3.

3. Activate the **To all active instances** indicator to delete the audit files from all application servers. Leave the indicator blank if you want to delete only the files from the local application server.

4 Activate the **Simulation only** indicator if you do not actually want to delete the files. In this case, the action is only simulated.

5 Choose **Audit Log -> Continue**. The system deletes the corresponding audit files (unless you chose to simulate). You receive a list showing how many files were deleted and how many were retained on each application server.

Install the SmartConnector

The following sections provide instructions for installing and configuring your selected SmartConnector.

> Connector Appliance/ArcSight Management Center supports mounting for Network File System (NFS) and CIFS (Windows) shares. When you install this connector on one of these devices, establish a CIFS mount on the device before adding the connector. Provide this share name during connector configuration. For more information, see **Remote File Systems** in the Connector Appliance or ArcSight Management Center Administrator's Guide.

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 Micro Focus SSO and Protect 724 sites.

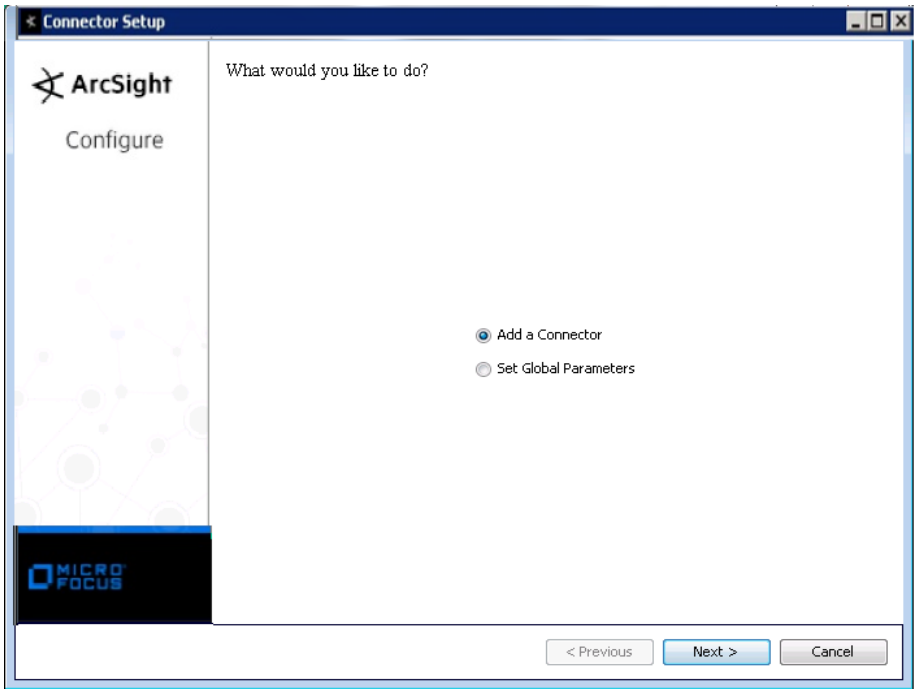
1 Download the SmartConnector executable for your operating system from the Micro Focus SSO site.

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

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.

Parameter	Setting
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.

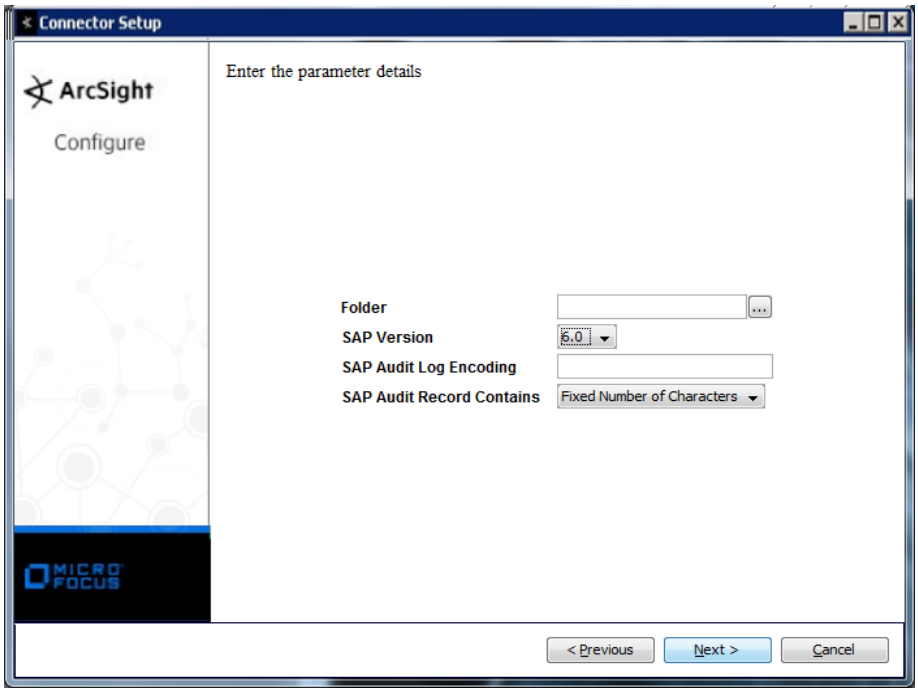
The following parameters should be configured only if you are using Micro Focus SecureData solutions to provide encryption. See the *Micro Focus SecureData Architecture Guide* for more information.

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 Micro Focus 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 Micro Focus 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 Micro Focus SecureData.
Format Preserving Secret	Enter the secret configured for Micro Focus 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 **SAP Security Audit File** and click **Next**.
3. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



Parameter	Description
Log Folder Directory	Enter the absolute path to the directory containing the audit and C2 log files.
SAP Version	Select the version number of your SAP System – either 4.6c, 4.7, 6.0, or 6.17 The default value is 4.6c.
SAP Audit Log Encoding	Enter the character set or encoding used in SAP Audit Logs. For example, UTF-8 (8-bit UCS transformation format), UTF-16 (16-bit UCS transformation format)... If this field is left empty, the connector assumes the audit logs are in the default encoding determined by the operating system and locale settings.
SAP Audit Record Contains	Select whether the SAP Audit Record contains a 'Fixed number of characters' or a 'Fixed number of bytes'.

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.

SAP Audit Mappings to ArcSight Events

ArcSight ESM Field	Device-Specific Field
ArcSight Severity - High	Device Severity = 4
ArcSight Severity - Low	Device Severity = 0, 1, or 2
ArcSight Severity - Medium	Device Severity = 3
ArcSight Severity - Very High	Device Severity = 5;
Device Custom Number 1	Process ID
Device Custom Number 2	Session Number
Device Custom String 1	Terminal
Device Custom String 2	Transaction
Device Custom String 3	Report
Device Custom String 4	Client
Device Custom String 5	RFC Function Name
Device Custom String 6	Authorization
Device Event Category	Event Class
Device Event Class Id	EventID
Device Product	'Security Audit Log'
Device Receipt Time	EventTime
Device Vendor	'SAP'
Source Address	Extract Address from Terminal2
Source Host Name	Extract Host Name from Terminal2
Source User Name	User name in events other than login/logout