



ArcSight SmartConnectors

Software Version: CE 24.4

Configuration Guide for SAP Security Audit File SmartConnector

Document Release Date: October 2024

Software Release Date: October 2024

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2024 Open Text.

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Trademark Notices

“OpenText” and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

<https://www.microfocus.com/support-and-services/documentation>

Contents

Configuration Guide for SAP Security Audit File SmartConnector	4
Product overview	5
Configuration	6
Security audit log	6
Defining filters	7
Defining static profiles	8
Changing filters dynamically	9
Example filters	11
Filter for recording all security-critical events	11
Filter for recording activities performed by a specific user	12
Deleting old audit files	14
Creating shared folder to read SAP logs	14
Installing the SmartConnector	16
Preparing to install the SmartConnector	16
Installing and configuring the SmartConnector	16
Configuring advanced log processing parameters	18
Using a service/user account with the write permission	18
Using a service/user account having read-only permission	18
Migrating Connectors from one server to another using a Service/User account with read-only permission	19
Device event mapping to ArcSight fields	20
SAP audit mappings to ArcSight events	20
Send Documentation Feedback	21

Configuration Guide for SAP Security Audit File SmartConnector

This guide provides information for installing the SmartConnector for SAP Security Audit File and configuring the device for audit log event collection.



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

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight software and its environment.

Additional Documentation

The ArcSight SmartConnector documentation library includes the following resources:

- [Technical Requirements Guide for SmartConnector](#), which provides information about operating system, appliance, browser, and other support details for SmartConnector.
- [Installation and User Guide for SmartConnectors](#), which provides detailed information about installing SmartConnectors.
- [Configuration Guides for ArcSight SmartConnectors](#), which provides information about configuring SmartConnectors to collect events from different sources.
- [Configuration Guide for SmartConnector Load Balancer](#), which provides detailed information about installing Load Balancer.

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the [documentation site for ArcSight SmartConnectors](#).

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to MFI-Documentation-Feedback@opentext.com.

For specific product issues, [contact Open Text Support for Micro Focus products](#).

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.

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.

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 log-on attempts
- Successful and unsuccessful RFC log-on 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 <i>Only critical</i>

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

Static configuration DynamicConfigurati

Active profile PROFILE1

Displayed profile PROFILE1

Filter 1 Filter 2

☒ Filter active Reset Detailed display

Selection criteria	Audit classes	Events
Client *	<input checked="" type="checkbox"/> Dialog logon	<input checked="" type="radio"/> Only critical
User names *	<input checked="" type="checkbox"/> RFC/CPIC logon	<input type="radio"/> Important and critical
	<input checked="" type="checkbox"/> RFC call	<input type="radio"/> All
	<input checked="" type="checkbox"/> Transaction start	
	<input checked="" type="checkbox"/> Report start	
	<input checked="" type="checkbox"/> User master change	
	<input checked="" type="checkbox"/> Other events	

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>

Field or Group	Entry
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.

Dynamic Configuration

Status of recording on individual servers

Server names	Release	Status	Current file size	Maximum file size
pwdt0284 U9C 60	13.09.2000 14:14:00	✓	2.520	976 KB
pwdt0002 U9C 11	13.09.2000 14:14:00	✓	2.520	976 KB
us0033 U9C 60	13.09.2000 14:14:00	✓	2.520	976 KB

Filter 1 **Filter 2**

☒ Filter active Reset Detail configuration

Selection criteria	Audit classes	Events
Client 450	<input checked="" type="checkbox"/> Dialog logon	<input type="radio"/> Only critical
User names SUPPORT	<input checked="" type="checkbox"/> RFC/CPIC logon	<input type="radio"/> Important and critical
	<input checked="" type="checkbox"/> RFC call	<input checked="" type="radio"/> All
	<input checked="" type="checkbox"/> Transaction start	
	<input checked="" type="checkbox"/> Report start	
	<input checked="" type="checkbox"/> User master change	
	<input checked="" type="checkbox"/> Other events	

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 greater 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.

Creating shared folder to read SAP logs

Many customers do not prefer to install SmartConnectors on the SAP servers in their production environment.

As a best practice, OpenText recommends that you create a shared folder to periodically dump the SAP logs. You can configure SmartConnector with a service/user account that has the required privileges to read the SAP logs from this shared folder.

Installing 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.

Preparing to install the SmartConnector

Before you install any SmartConnectors, make sure that the OpenText ArcSight products with which the connectors will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger).

For complete product information, refer to the *Administrator's Guide to ArcSight Platform*, available on [ArcSight Documentation](#).

If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* available on [ArcSight Documentation](#) for instructions.

Before installing the SmartConnector, make sure that the following are available:

- Local access to the machine where the SmartConnector is to be installed
- Administrator passwords

Installing and configuring the SmartConnector

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.
3. Specify the relevant [Global Parameters](#), when prompted.
4. In the **Type** list, select **SAP Security Audit File**, then click **Next**.

5. In the **Enter the parameter details** page, select the required value for the following parameter, and then click **Next**:

Parameter	Description
Folder	Enter the absolute path to the directory containing the audit and C2 log files. <Installation path>\logs For example: C:\arcsight\connectors\SAP_samplelogs\logs
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'.

6. Select a [destination and configure parameters](#).
7. Specify a name for the connector.
8. (Conditional) 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 then click **Next**. The certificate is imported and the **Add connector Summary** window is displayed.



If you select **Do not import the certificate to connector from destination**, the connector installation will end.

9. Select whether you want to install the connector as a service or in the standalone mode.
10. Complete the installation.
11. Optionally, configure advanced parameters in the agent.properties file to make any changes in the default behavior of the connector.
12. [Run the SmartConnector](#).

Configuring advanced log processing parameters

When you install the SmartConnector to read logs from a shared location, by default it reads and processes all the old and present log files in the shared folder and sends the files to the configured destination. However, the SmartConnector repeats the reading and processing of log files during every restart. To avoid this, you must configure the advanced parameters in the `agent.properties` file depending on whether the service/user account has a read permission or a write permission.

Using a service/user account with the write permission

If the service/user account has write permission, add the following parameters with the specified values in the `agent.properties` file to make sure that the connector does not read all the log files every time the SmartConnector is restarted.

```
agents[0].mode=RenameFileInTheSameDirectory  
agents[0].modeoptions=processed
```

In this scenario, when the connector runs for the first time after installation, it reads and processes all the old and current SAP logs from the shared folder and bookmarks the processed log files by renaming them with a `.processed` extension and these files are not read when the SmartConnector restarts. For example, a log file with name `20240602_000004.AUD` is renamed to `20240602_000004.AUD.processed` after it is processed.

Using a service/user account having read-only permission

If the service/user account has read-only permission, add the following parameters with the specified values in the `agent.properties` file to make sure that the connector does not read all the log files every time the SmartConnector is restarted.

```
agents[0].mode=PersistFile  
agents[0].modeoptions=processed
```

In this scenario, when the connector runs for the first time after installation, it reads and processes all the old and current SAP logs from the shared folder and bookmarks the processed log files by placing them inside the `persisted.properties` file that is automatically created. The logs that are inside the `persisted.properties` file are not read when the SmartConnector restarts.



When the write permission is not granted, the log files will not be renamed and instead `persisted.properties` folder will be used for bookmarking and if write permission is granted, the `persisted.properties` folder will not be created and instead the log files will be renamed for bookmarking.

Migrating Connectors from one server to another using a Service/User account with read-only permission

If the advanced parameters are not configured when migrating SmartConnector from one server to another with a new installation, the SmartConnector will start reading all the files that are inside the shared folder, that were processed by the connector in the old server. To make sure that the logs that were processed in the old server are not reprocessed by the newly installed connector in the new server, do the following:

1. Copy the `persisted.properties` file from the following path of the old SmartConnector:
`<Home>\current\user\agent\`
2. Paste the file in the following path of the new SmartConnector:
`<Home>\current\user\agent\`
3. Open the `persisted.properties` file and replace the old connector agent ID with the new connector agent ID in the following format:
`<agent ID>.<log file path>=true`

For example:

```
3zM7KM5EBABC1TmejK2C0rw\=\.C\:\\arcsight\\connectors\\SAP_
samplelogs\\New\ folder\\20240602_000005.AUD=true
```

Device event mapping to ArcSight fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. For more information about the ArcSight data fields, see *ArcSight Console User's Guide*.

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

Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

**Feedback on Configuration Guide for SAP Security Audit File SmartConnector
(SmartConnectors CE 24.4)**

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!