Security Audit Log

HELP.BCCSTADM

Release 4.6C

Copyright

Icons

Icon	Meaning
	Caution
	Example
	Note
	Recommendation
	Syntax

Inhalt

Security Audit Log

Purpose

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

Implementation Considerations

The Security Audit Log contains personal information that may be protected by data protection regulations. Before using the Security Audit Log, make sure that you adhere to the data protection laws that apply to your area of application!

Integration

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

For a detailed description on the technical aspects of the audit log, see The Design of the Security Audit Log [Seite 7].

The Security Audit Log complements the system log; however, the Security Audit Log has a slightly different purpose and a different audience (see Comparing the Security Audit Log and the System Log [Seite 9]).

Activities

For more information about the various activities that you need to perform when using the Security Audit Log, see:

- Defining Filters [Seite 15] to enable auditing and configure the information you wish to audit.
- Displaying the Audit Analysis Report [Seite 17] for a detailed description on how to specify your audit analysis report. You can view the recorded information as desired. You can view

everything that you have logged, or you can select a sub-group (for example, certain transactions or certain users).

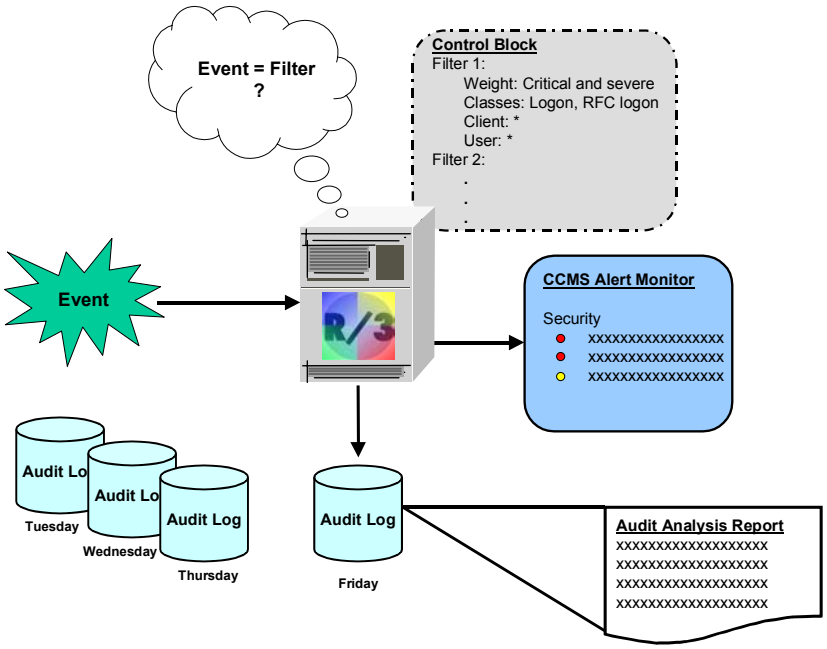
- Deleting Old Audit Files [Seite 21] for information on archiving and deleting your audit files.

The Design of the Security Audit Log

Overview

The Security Audit Log keeps a record of security-related activities in SAP Systems. This information is recorded daily in an audit file on each application server. To determine what information should be written to this file, the audit log uses filters, which are stored in memory in a control block. When an event occurs that matches an active filter (for example, a transaction start), the audit log generates a corresponding audit message and writes it to the audit file. A corresponding alert is also sent to the CCMS alert monitor. Details of the events are provided in the Security Audit Log's audit analysis report. See the graphic below:

Security Audit Log Architecture



SAP Systems maintain their audit logs on a daily basis. The system does not delete or overwrite audit files from previous days; it keeps them until you manually delete them. Due to the amount of information that may accumulate, you should archive these files on a regular basis and delete the originals from the application server (see Deleting Old Audit Files [Seite 21]).

The Audit File / The Audit Record

The audit files are located on the individual application servers. You define the name and location of the files in the profile parameter `rsau/local/file`. When an event occurs that is to be audited, the system generates a corresponding audit record, also called an audit message, and writes it to the file. The audit record contains the following information (if known):

- Event identifier (a 3-character code)
- SAP user ID and client

- Terminal name
- Transaction code
- Report name
- Time and date when the event occurred
- Process ID
- Session number
- Miscellaneous information

You define the maximum size of the audit file in the profile parameter `rsau/max_diskspace/local`. The default is 1000000 bytes (= 1 MB). If the maximum size is reached, then the auditing process stops.

Filters

You define the events you want to audit in filters. This information is stored in the control block, which is located in the application server's shared memory. The SAP System uses this information to determine which audit messages should be written to the audit file.

Filters consist of the following information:

- Client
- User
- Audit Class
  - Dialog logon
  - RFC/CPIC logon
  - RFC function call
  - Transaction start
  - Report start
  - User master change
  - Other
- Weight of Events to Audit
  - Only critical
  - Important and critical
  - All

For more details, see Defining Filters [Seite 15].

The Audit Analysis Report

You can view the contents of the audit files in the audit analysis report. For more information, see Displaying the Audit Analysis Report [Seite 17] and Reading the Audit Analysis Report [Seite 19].

Alerts in the Computing Center Management System Alert Monitor

The Security Audit Log also generates security alerts for the events recorded in the Computing Center Management System (CCMS) alert monitor. For more information, see Security Alerts in the CCMS Alert Monitor [Seite 22].

Comparing the Security Audit Log and the System Log

The Security Audit Log complements the System Log. Both are tools used to keep a record of activities performed in SAP Systems. However, they use slightly different approaches and have different objectives. We show how these two types of logging compare in the table below.

The Security Audit Log	The System Log
Objective	
Records security-related information that can be used to reestablish a series of events (for example, unsuccessful logon attempts or transaction starts).	Records information that may signal system problems (for example, database read errors, rollbacks).
Audience	
Auditors	System administrators
Flexibility of Use	
You can activate and deactivate the Security Audit Log as necessary. Although you may wish to audit your system on a daily basis, you do not have to. For example, you may wish to activate the Security Audit Log for a period of time before a pre-designated audit and deactivate it between audits.	The system log is needed on a continuous basis. You do not deactivate the system log.
Log Availability	
The audit logs are local logs maintained on each application server. However, in contrast to the system log, the system maintains its audit logs on a daily basis and you have to archive or delete the log files manually. This way, you can refer to logs from previous days and the time frame for available logs is increased.	There are two types of system logs, local and central. Local logs are maintained on each individual application server. These files are circular, meaning that once they are full, they are overwritten from the beginning. The sizes of these logs, as well as the time frame where they are available, are limited. You also have the option to maintain a central log. However, the central log is currently not completely platform independent. At the current time, it can only be maintained on a UNIX platform. The central log is also not kept indefinitely.

Handling Sensitive Data

The Security Audit Log contains personal information that may fall under data protection regulations. You need to pay close attention to the data protection regulations before you activate the Security Audit Log.	The system log does not contain any personal data.

Maintaining Static Profiles

Use

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.

This topic concentrates on permanently saving filters in static profiles in the database. For information on changing the filters dynamically, see Changing Filters Dynamically [Seite 13].

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

Prerequisites

The following profile parameters must be set:

Audit Log Profile Parameters

Profile Parameter	Description
rsau/enable	Enable 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* screen appears 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.

3. 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.

4. Define filters [Seite 15] for your profile.

5. Make sure the *Filter active* indicator is set for each of the filters you want to apply to your audit.
6. Save the data.
7. To activate the profile, choose *Profile* → *Activate*.
8. Shut down and restart the application server to make the changes effective.

Result

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

Use

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.

This topic concentrates on dynamically changing filters. For information on defining filters in static profiles, see Maintaining Static Profiles [Seite 11].

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

Prerequisites

The following profile parameters must be set:

Audit Log Profile Parameters

Profile Parameter	Description
rsau/enable	Enable the Security Audit Log
rsau/local/file	Names and locations of 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* screen appears 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 screen, you receive a list of the active instances and their auditing status. The lower section of the screen contains tabstrips for maintaining filters.

3. Choose *Configuration* → *Display* <-> *Change*.
4. Define filters [Seite 15] 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. If you want to distribute the filter definition to all of the application servers, choose *Configuration* → *Distribute configuration*.

7. To change the auditing status on a single application server, select the status indicator in the *List of active instances* table.
   -  indicates an activated audit.
   -  indicates a deactivated audit.
8. To activate the filter (or filters) on all of the application servers, choose *Configuration* → *Activate* audit. (To deactivate the filters on all of the application servers, choose *Configuration* → *Deactivate audit*.)

   If you receive a program failure, then 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.)

Result

The audit filters are dynamically created on all active application servers. If you activate the profile(s), then 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.

Defining Filters

Use

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)

For examples of filters, see Example Filters [Seite 26].

You can define filters that you save in static profiles in the database (see Maintaining Static Profiles [Seite 11]) or you can define them dynamically for one or more application servers (see Changing Filters Dynamically [Seite 13]).

Prerequisites

- The number of filters you can specify is defined in the profile parameter `rsau/selection_slots`.
- You are either defining static profiles [Seite 11] or changing filters dynamically [Seite 13] using the Security Audit Log configuration tool. For each allocated filter, a tabstrip appears in the lower section of the screen.

Procedure

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 appears containing a detailed list of the audit classes with their corresponding event classes (critical, severe, non-critical) and message texts. (The message texts correspond to the system log messages AU<X>.)

   b. Select the events you want to audit. You can either:
      - Select a single event by activating the *Recording* indicator for a specific event.
      - 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 reappear.

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 [Seite 11] or changing filters dynamically [Seite 13].

Displaying the Audit Analysis Report

Use

The Security Audit Log produces an audit analysis report that contains the audited activities. By using the audit analysis report you can analyze events that have occurred and have been recorded on a local server, a remote server, or all of the servers in the SAP System.

The audit analysis report produced by the Security Audit Log is designed analog to the System Log [Extern].

Procedure

1. To access the Security Audit Log analysis screen from the *SAP standard menu*, choose *Tools* → *Administration* → *Monitor* → *Security Audit Log* → *Analysis.*

   The *Security Audit Log: Local Analysis* screen appears; local analysis is the default.
2. If you want to analyze a remote server, choose *Security Audit Log* → *Choose* → *Remote Audit Log*. To analyze all servers, choose *Security Audit Log* → *Choose* → *All audit logs*.

   Your choice is displayed next to the *Imported audit log* entries field.
3. If you choose to analyze a remote server, then enter the name of the application server in the *Instance name* field.
4. Enter any restrictions you want to apply to the audit analysis report in the appropriate fields or by selecting the desired indicators (for example, *From date/time, To date/time, User, Transaction, Audit classes*, or *Events to select*).

   Events are classified into three categories, critical, important, and non-critical, with critical being the most important. You can view critical events only, critical and severe events, or all events.
5. If you want to include or exclude specific messages from your report:
   a. Choose *Edit* → *Expert mode*.
   b. Choose *Message filter*.
   c. Select either *Only these messages* or *All except these messages* as appropriate.
   d. Enter the message numbers you want to include or exclude. (The message numbers correspond to the system log messages AU<X>.)
   e. Choose *Use*.
6. To modify the output format, change the options in the *Format* section. For more information, see The Audit Log Display Options [Seite 25].
7. To read the Security Audit Log, choose one of the following options:
   - Choose *Security Audit Log* → *Re-read audit log* to initially read or to replace a previously read log.
   - Choose *Security Audit Log* → *Re-display only* to view the last audit log you read. For example, you can change the *Selection* options to modify the audit analysis report without having to re-read the log.
   - Choose *Security Audit Log* → *Read audit log* to merge new information using different selection criteria with the current information in the audit analysis report.

The *Imported audit log entries* field tells how many log entries the system has read from the log file. When you first enter the *Audit Log: Analysis* initial screen, this field is set to the value "0".

Sorting the Audit Log Display

To sort the audit analysis report, choose *Security Audit log → Sort → <sort option>.*

The following sort options are available:

- Write sequence
- Time
- Instance

Result

The result is the audit analysis report containing the messages that correspond to your selection criteria. By selecting an individual message, you can view more detailed information (see Reading the Audit Analysis Report [Seite 19]).

Reading the Audit Analysis Report

In this section, we describe how to read the audit analysis report produced from the procedure Displaying the Audit Analysis Report [Seite 17].

The Main Audit Analysis Report

The audit analysis report is divided into four main sections:

- Introductory information
- Audit report
- Statistical analysis
- Contents

Introductory Information

At the top of the report, you find the selection options applied to the audit file to generate this report (for example, *From date/time*, *To date/time, User,* and *Audit classes)*.

Audit report

The audit report follows the introductory data and contains the following information for each audit event found in audit file that applies to your selection criteria (depending on your display configuration):

- Date
- Time
- Instance
- Category (dialog or batch)
- Message number
- Audit class code (For example, a dialog logon attempt belongs to class number 002.)
- User
- Transaction code
- Terminal number

Summary information is included at the end of the list (for example, the number of records read, the number of records selected, and audit file names).

Statistical analysis

If you included *With statistical analysis* in the display options, then the following blocks of information are included after the audit data:

- Instance statistics (when analyzing all instances)
- Client statistics
- Report statistics
- Transaction statistics
- User statistics
- Message statistics

Contents

A list of contents is provided at the end of the report.

The Detailed Audit Analysis Report

To view details about a specific message, place the cursor on the entry and choose *Edit* → *Details*. A detailed description of the message including information such as the task name, class, message documentation, and the technical details of the audit record appears.

Deleting Old Audit Files

Use

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.

We recommend 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!

Procedure

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* screen appears.
2. Enter the *Minimum age* of files to delete (default = 30 days).

   This value must be > 3.
3. Activate the *To all active instances* indicator to delete the audit files from all application servers. Leave the indicator blank if you only want to delete 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*.

Result

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.

Security Alerts in the CCMS Alert Monitor

When the Security Audit Log records events, it also triggers a corresponding security alert in the Computing Center Management System (CCMS) alert monitor.

The security alerts that are created correspond to the audit classes of events as defined in the Security Audit Log, which include:

- Dialog logon attempts
- RFC/CPIC logon attempts
- Transaction starts
- Report starts
- RFC function calls
- Changes to user master records
- Changes to the Security Audit Log configuration

By monitoring the security alerts in the CCMS alert monitor, you can quickly identify security-related problems in your system. After performing the immediate on-alert action to resolve the alert, you can analyze the Security Audit Log files for more information about the specific event that caused the alert.

You can view the security alerts directly in the CCMS alert monitor (see the topic Viewing Security Alerts [Seite 23]) or use BAPIs (Business Application Program Interfaces) to access the alerts from external programs (see the topic Reading Security Alerts Using BAPIs [Seite 24]).

Viewing Security Alerts

Prerequisites

The Security Audit Log must be activated on the application server so that the event is also triggered in the CCMS alert monitor.

Procedure

1. To access the CCMS alert monitor from the *SAP standard menu*, choose *Tools* → *CCMS* → *Control/Monitoring* → *Alert monitor*.

   The *CCMS monitor sets* appear.
2. To locate the security alerts, expand the node *SAP CCMS Monitor Templates*.
3. Place the cursor on the *Security* node and choose *Monitor* → *Load monitor*.

   The *Security* monitor appears.

   The alerts triggered by the Security Audit Log are located under the nodes for each application server.
4. Expand the node for the specific application server (or servers) that you want to examine.

   The categories that appear correspond to the audit classes recorded in the Security Audit Log. Entries with active alerts are indicated in red or yellow, depending on the highest alert level (critical or important) existing in the category.
5. Select the categories you want to examine on each application server or the complete application server node.
6. Choose *Edit* → *Alerts* → *Display alerts*.

   A list containing the chosen categories appears.
7. Process the alerts as necessary.

   For more information on the CCMS alert monitor and how to process alerts, see The Alert Monitor [Extern].

Reading Security Alerts Using BAPIs

The security alerts are also available to external programs using BAPIs (Business Application Programming Interfaces). The report RSAU_READ_AUDITLOG_EXTERNAL is a sample SAP program that you can use as a template for accessing the security alerts using BAPIs.

The Audit Log Display Options

Option	Meaning
No. pages for individual entries	Specifies the maximum number of pages you want to view. This only applies to the main section of the report, not to the introductory information or summaries.
With statistical analysis	If you activate this option, then the following statistics are included with your report. • Instance statistics (when analyzing all instances) • Client statistics • Report statistics • Transaction statistics • User statistics • Message statistics
Settings	Specifies the layout and output devices.

Example Filters

In the following example, the Security Audit Log is enabled on the server `pawdf050`. The active profile is `PROFILE1`.

For *Filter 1*, the system will record any dialog logon attempts, RFC or CPIC logon attempts, or transaction starts that are categorized as important or critical events. The events are recorded for all users and for events in any of the SAP System clients.

For *Filter 2*, the system only records events categorized as critical in client 000 for `TESTUSER`.

Both filters are active in the system.

Filter 1


Profile Edit Goto Environment System Help
SAP
Security Audit: Change Audit Profile
Static configuratio
Active profile
PROFILE1
Displayed profile
PROFILE1
Filter 1
Filter 2
Filter active
Reset
Detail configurat
Selection criteria
Client
*
User names
*
Audit classes
Dialog logon
RFC/CPIC logon
RFC function call
Transaction start
Report start
User master change
Other
Events
Only critical
Important
and critical
All
A9B (1) (000)
pawdf050
INS

Example Filters

Filter 2