# How to configure an audit log in SAP with SM19 and review user activity with SM20

Audit logging lets you monitor what users do in your SAP system. It matters most when you assign broad access, such as the SAP_ALL profile, during an emergency. This guide explains how to configure an audit log in SAP using transaction SM19, how to review the results with SM20 and the remote analysis screen, and how to manage the RSAU parameters that control filters and file sizes.

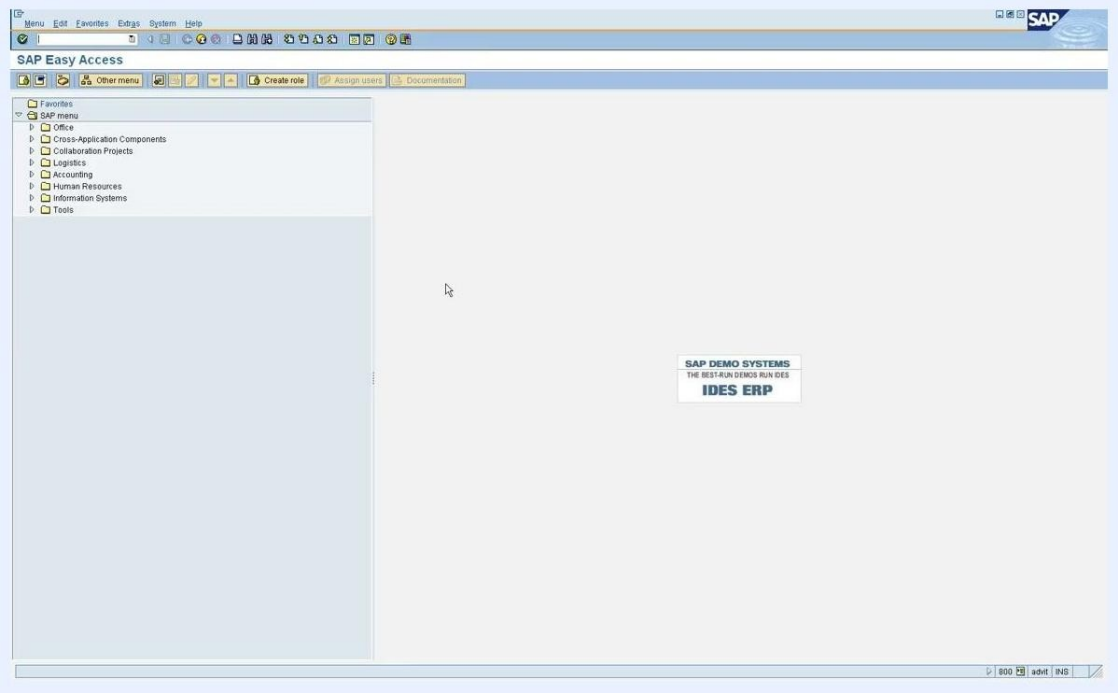
## Prerequisites

- You have SAP GUI installed and can log in to your SAP system.
- You can open the **SAP Easy Access** screen and run transaction codes from the command field.
- You have enough disk space at the operating system level for audit log files, because they can grow large over time.

## Step 1: Open the SAP Easy Access screen

1. Launch SAP GUI and log in to your SAP system.
2. Confirm that the **SAP Easy Access** screen appears. The left panel shows the SAP menu with folders such as Office, Cross-Application Components, Collaboration Projects, Logistics, Accounting, Human Resources, Information Systems, and Tools.

3. Check that the main area displays "SAP DEMO SYSTEMS – THE BEST-RUN DEMOS RUN IDES – IDES ERP".




**SAP Easy Access screen with the SAP menu and the IDES ERP demo system logo**

## Step 2: Open the Security Audit Log tool

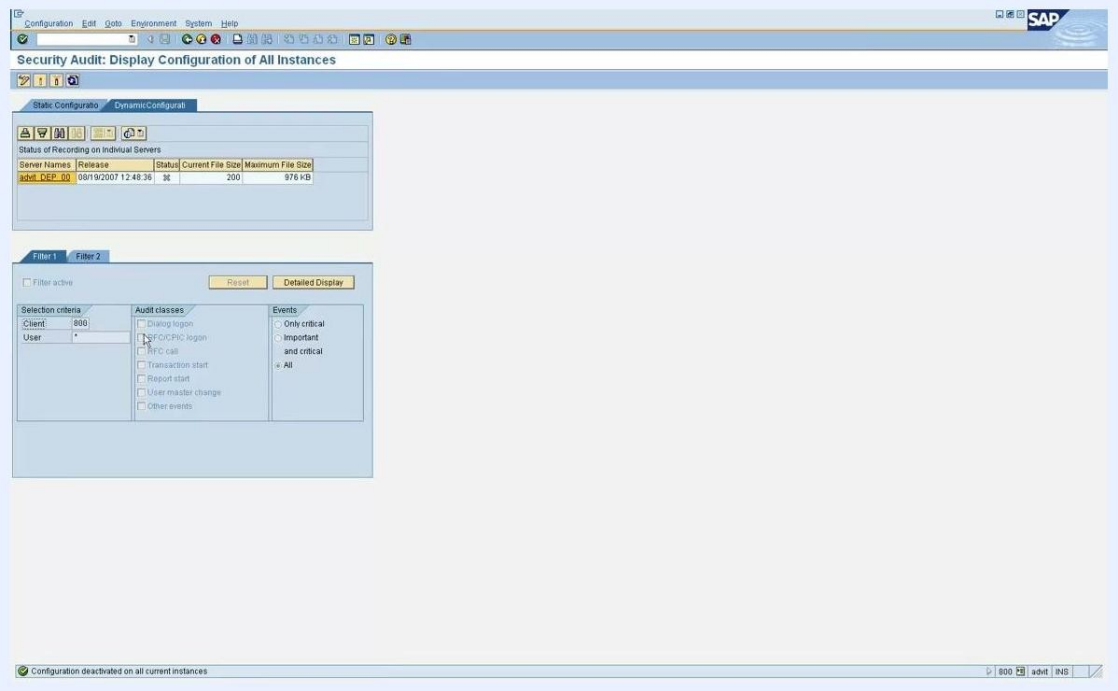
SAP provides a dedicated tool to configure an audit log in SAP. You access it with transaction code **SM19**.

1. Enter SM19 in the command field and press Enter.
2. Wait for the **Security Audit: Display Configuration of All Instances** screen to appear.

The screen has two main sections:

- **Status of Recording on Individual Servers**: shows the server name, release, status, current file size, and maximum file size.
- **Filter section**: lets you set selection criteria (Client, User), choose audit classes, and select event types.

The audit classes are Dialog logon, RFC/CPIC logon, RFC call, Transaction start, Report start, User master change, and Other events. The event types are Only critical, Important and critical, and All.




**Security Audit: Display Configuration of All Instances screen with server status and filter options**

## Step 3: Set the filter criteria

Filters let you specify which users and clients to monitor. Each filter has its own selection criteria:

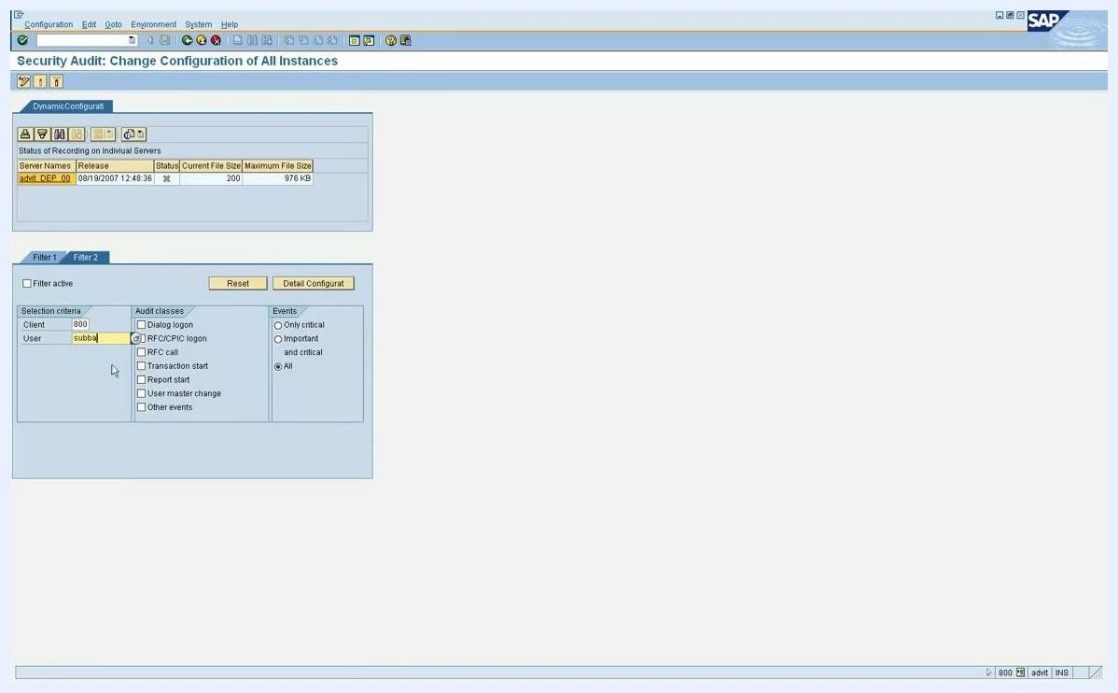
- **Client**: Enter a specific client number, such as 800, to monitor all users in that client.
- **User**: Leave the field blank to monitor all users, or enter a username to monitor only that user.

The combination of Client and User determines what the filter monitors:

- If both fields are set to * (wildcard), the filter monitors all users in all clients.
- If Client is 800 and User is blank, the filter monitors all users in client 800.
- If Client is * and User is subba, the filter monitors user "subba" across all clients.

- If both Client and User are specified, the filter monitors only that user's activities in that client.

For this example, set **Client** to 800 and **User** to subba. This configuration monitors only the activities of user "subba" in client 800.

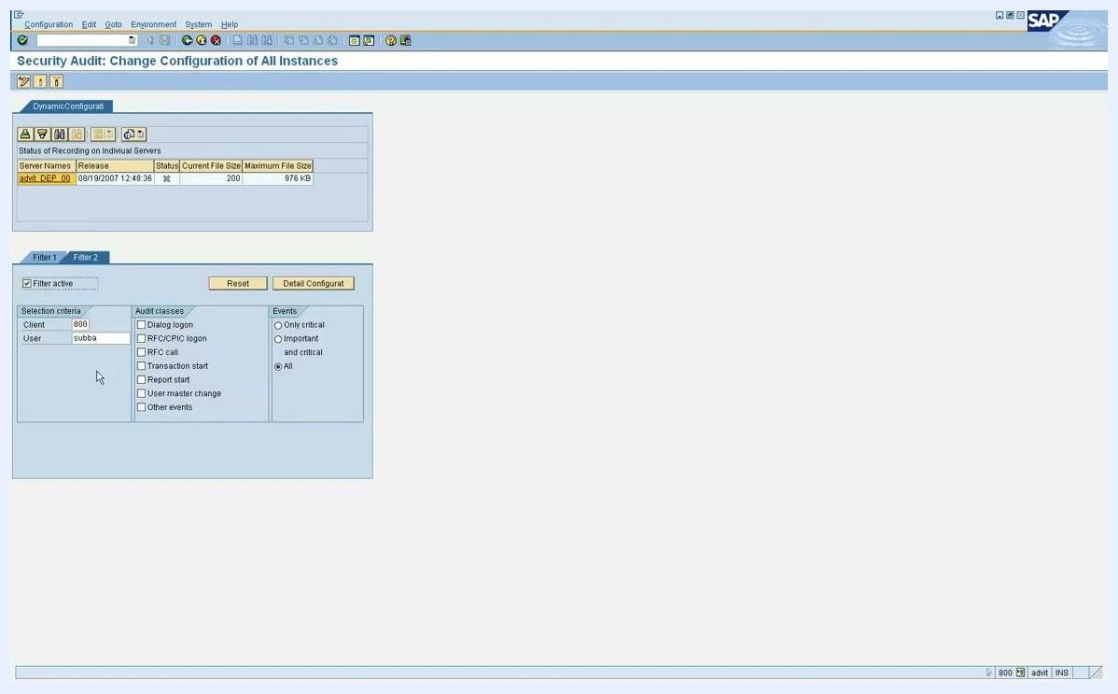



**Security Audit: Change Configuration of All Instances screen showing the filter for Client 800 and User subba, with audit class and event options**

Use filters to tailor audit logging to your organization's monitoring needs. You can adjust the number of filters for more detailed monitoring. Always review your filter settings before you activate audit logging.

## Step 4: Activate the filter

After you configure the filter (for example, Client = 800, User = subba), select the **Filter active** checkbox. This ensures the system uses the criteria you set for monitoring.



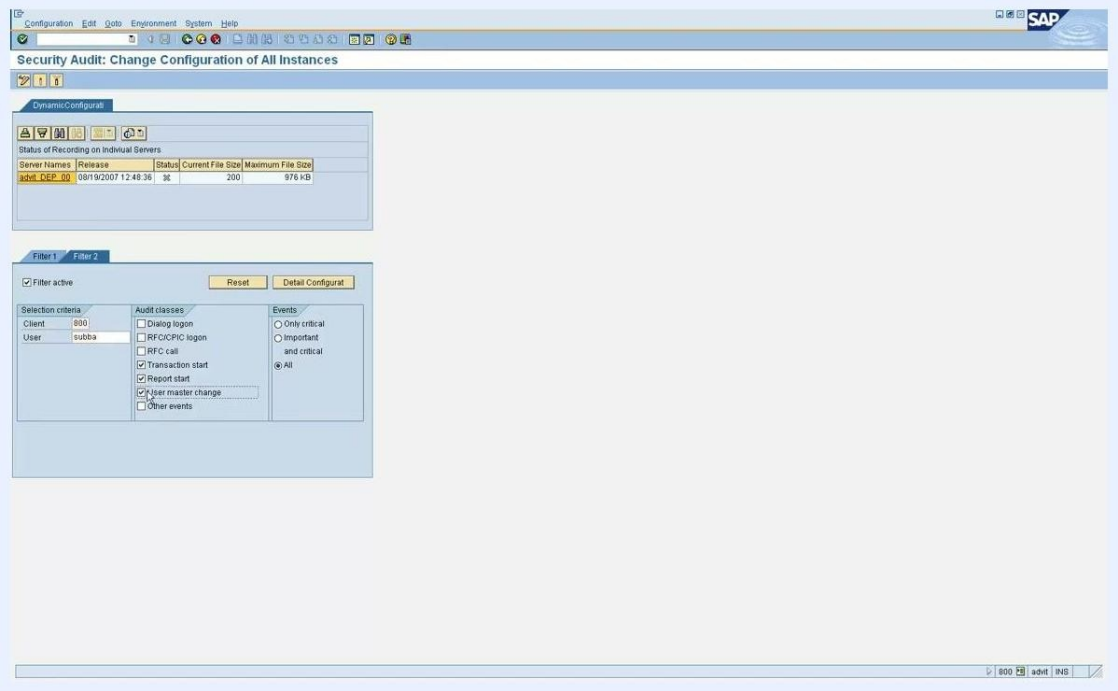

**Security Audit: Change Configuration of All Instances screen with Filter active selected, Client 800, User subba, and audit class options visible**

## Step 5: Select the audit classes to monitor

Choose the types of activity you want to monitor for the specified user and client:

- **Transaction start**: Monitors which transaction codes the user starts in this client.
- **Report start**: Monitors which reports the user executes in this client.
- **User master change**: Monitors the changes the user makes to user master records in client 800.

You can also select other audit classes, such as Dialog logon, RFC/CPIC logon, RFC call, and Other events, as needed.




**Audit class selection with Transaction start, Report start, and User master change selected**

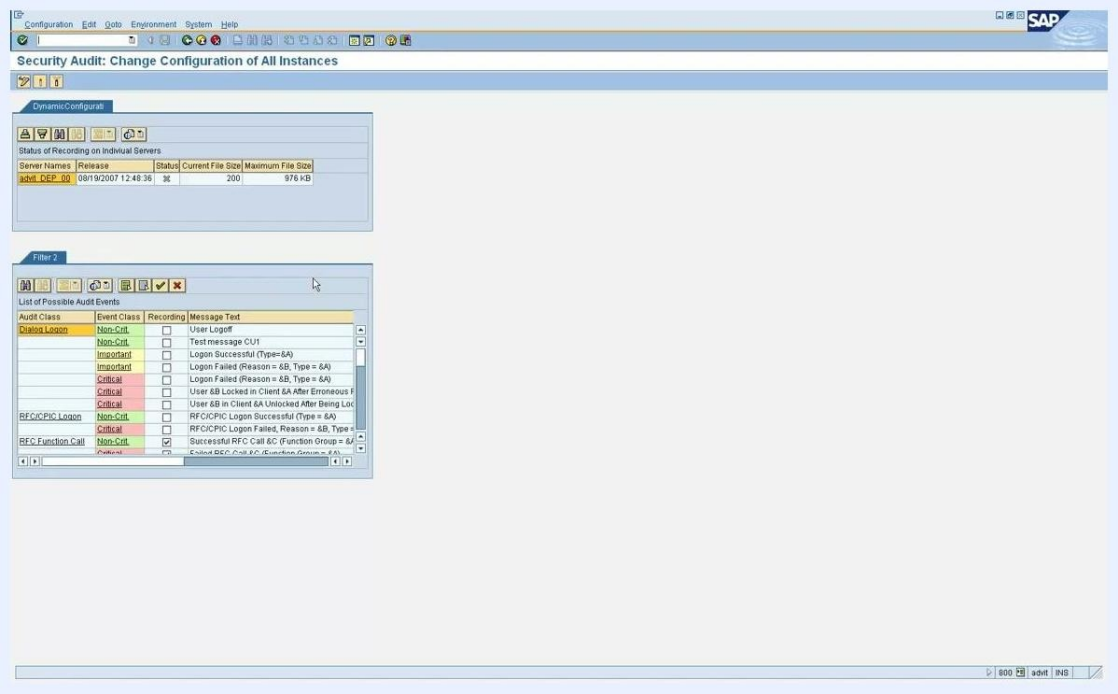
## Step 6: Choose the event severity to log

In the **Events** section, select the level of events to log:

- **Only critical**
- **Important and critical**
- **All** (recommended for comprehensive monitoring)

## Step 7: Open the detailed configuration

Click the **Detail Configuration** button to review and fine-tune which specific events the system monitors. A window opens with a list of possible audit events for the selected audit classes.




**Detailed configuration window showing the List of Possible Audit Events with Audit Class, Event Class, and Recording Message Text**

## Step 8: Review and select specific audit events

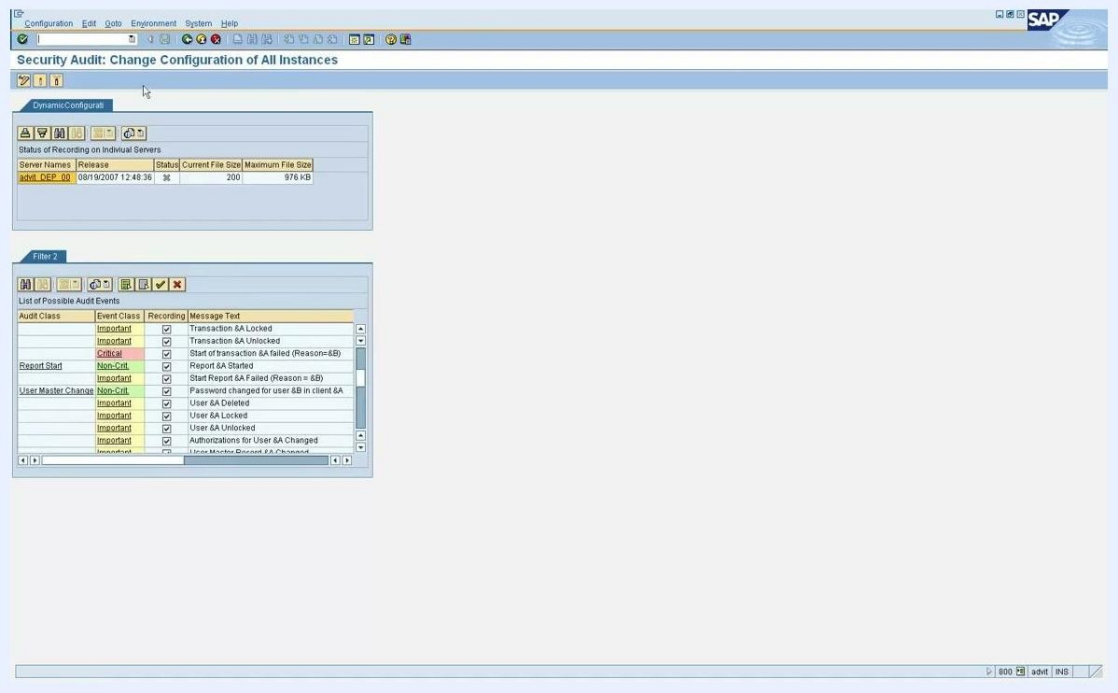
In the detailed configuration window, review the list of possible audit events. For each audit class, such as Dialog Logon, RFC/CPIC Logon, RFC Function Call, Report Start, or User Master Change, you can:

- See the **Event Class** (Non-Critical, Important, or Critical).
- Read the **Recording Message Text**, for example "User Logoff", "User 6A Locked in Client 6A after erroneous password checks", or "User 6A Deleted".
- Select or clear the checkbox to enable or disable logging for each event.

Examples of events you can monitor include:

- User logoff
- Failed logons, with reasons

- User locked or unlocked
- Transaction and report starts and failures
- User master record changes, such as a password change or a deleted user



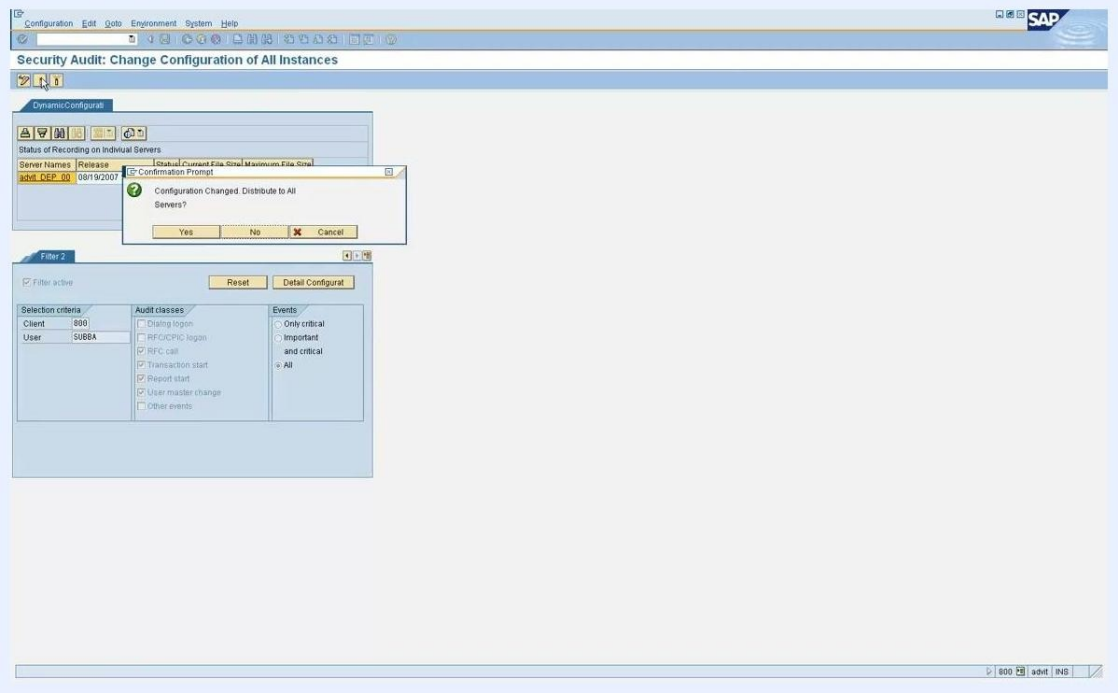

**Detailed configuration window with specific audit events selected, including user lock/unlock and report start events**

## Step 9: Save and distribute the audit log configuration

1. After you finalize your filter and event selections, click the **Save** icon (floppy disk) in the toolbar.
2. In the **Confirmation Prompt** window, read the message "Configuration Changed. Distribute to All Servers?"
3. Choose one of the three options:

- **Yes**: Distributes the configuration to all servers in your SAP landscape. The settings you defined (for user "SUBBA" in client 800) then apply consistently across all servers.
- **No**: Applies the configuration to the current server only.

- **Cancel**: Aborts the distribution and returns you to the configuration screen without saving changes.



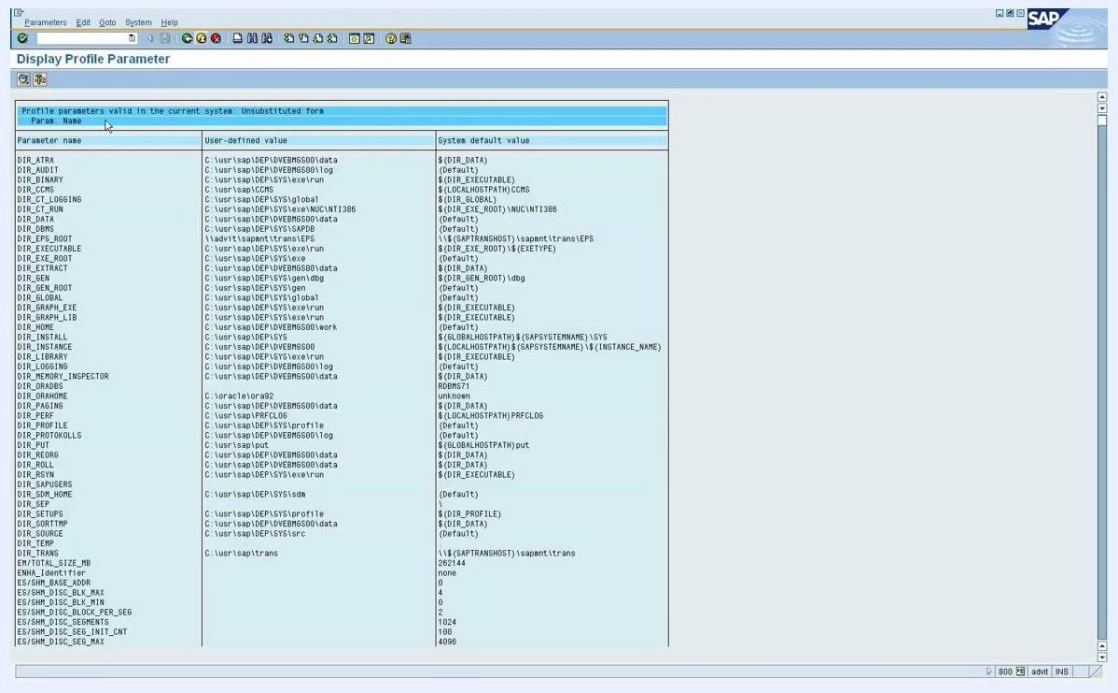

**Confirmation Prompt asking "Configuration Changed. Distribute to All Servers?" with Yes, No, and Cancel buttons; Filter 2 shows Client 800, User SUBBA, and the selected audit classes and events**

## Step 10: Generate user activity to monitor

With the filter active, user activity is now recorded. To perform user-related actions, run transaction codes such as SU01 or SU10. To run a specific program, use transaction code SU38.

1. Go to the **SAP Easy Access** screen.

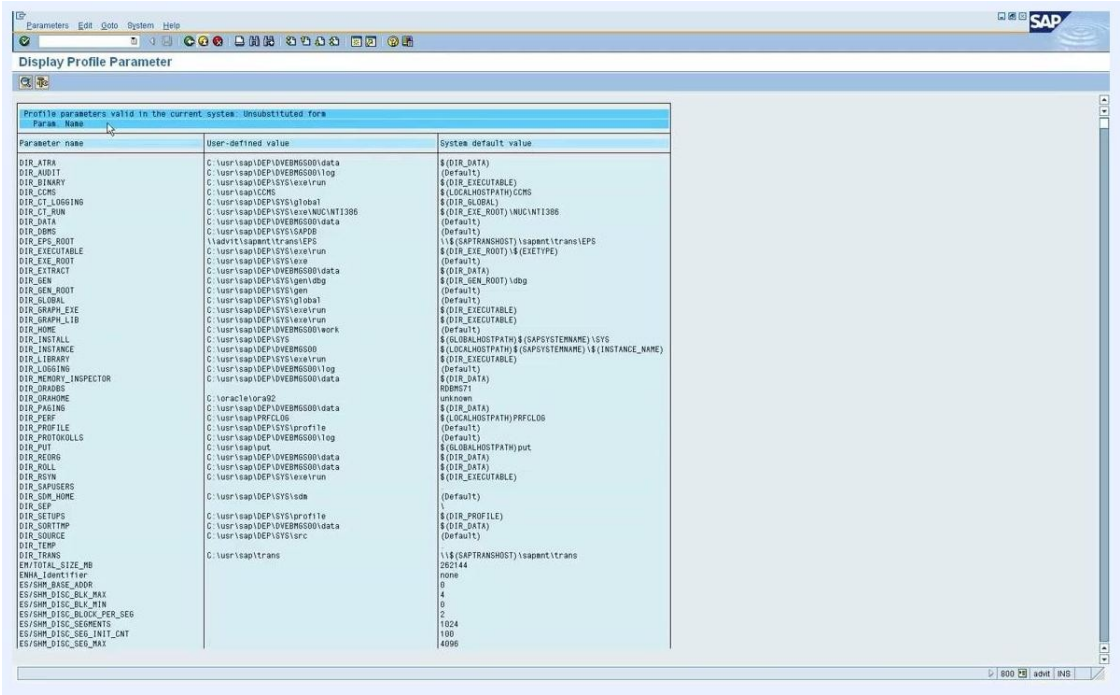
2. Enter the transaction code in the command field and press Enter.




**SAP Easy Access screen with the menu tree and IDES ERP logo, ready for a transaction code entry**

## Step 11: Review the security audit configuration after the activity

Return to the **Security Audit: Display Configuration of All Instances** screen to check the updated status. Look for changes in **Current File Size** or other audit indicators. For example, the file size may increase, which indicates new log entries.



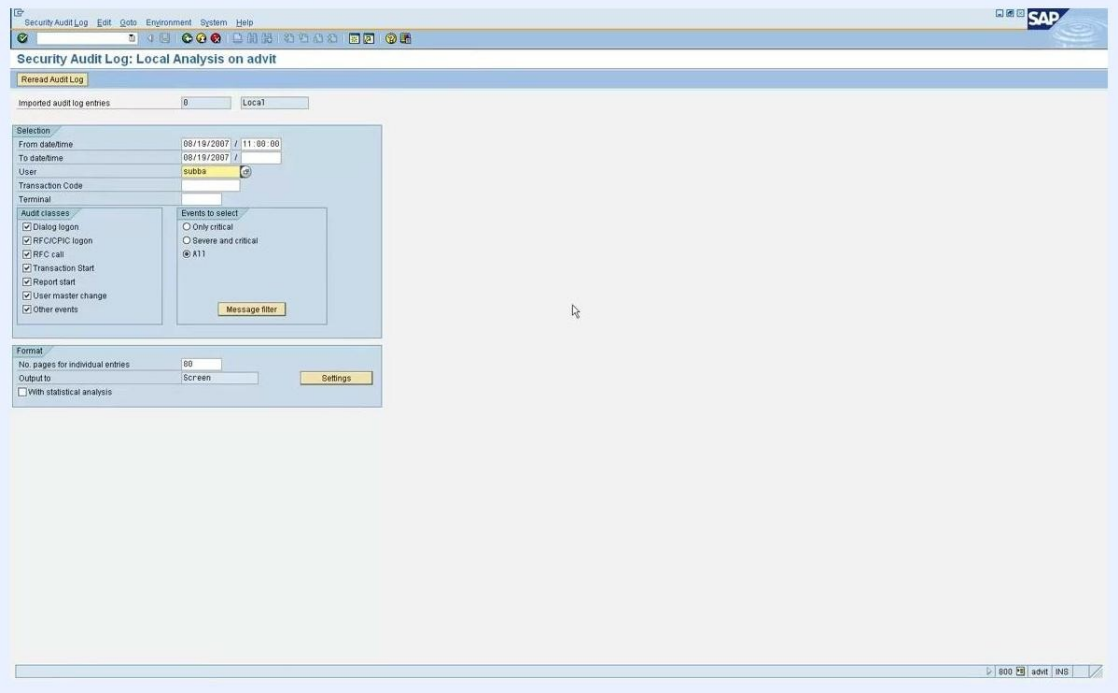

**Security Audit: Display Configuration of All Instances screen showing the updated file size and filter criteria**

## Step 12: Check the audit log locally with SM20

To check what actions a user has performed, use transaction code SM20. On the **Security Audit Log: Local Analysis** screen:

1. Enter the date and time range, for example 08/19/2007 11:00:00.
2. Enter the **User**, for example subba.
3. Optionally, specify a transaction code or terminal.
4. Select the **Audit classes**, such as Dialog logon, RFC/CPIC logon, Transaction Start, Report start, User master change, and Other events.
5. Under **Events to select**, choose "All".
6. Set the number of pages for individual entries, for example 80.
7. Set **Output to:** "Screen".

8. Click "Settings" or "Message filter" as needed to refine your search.



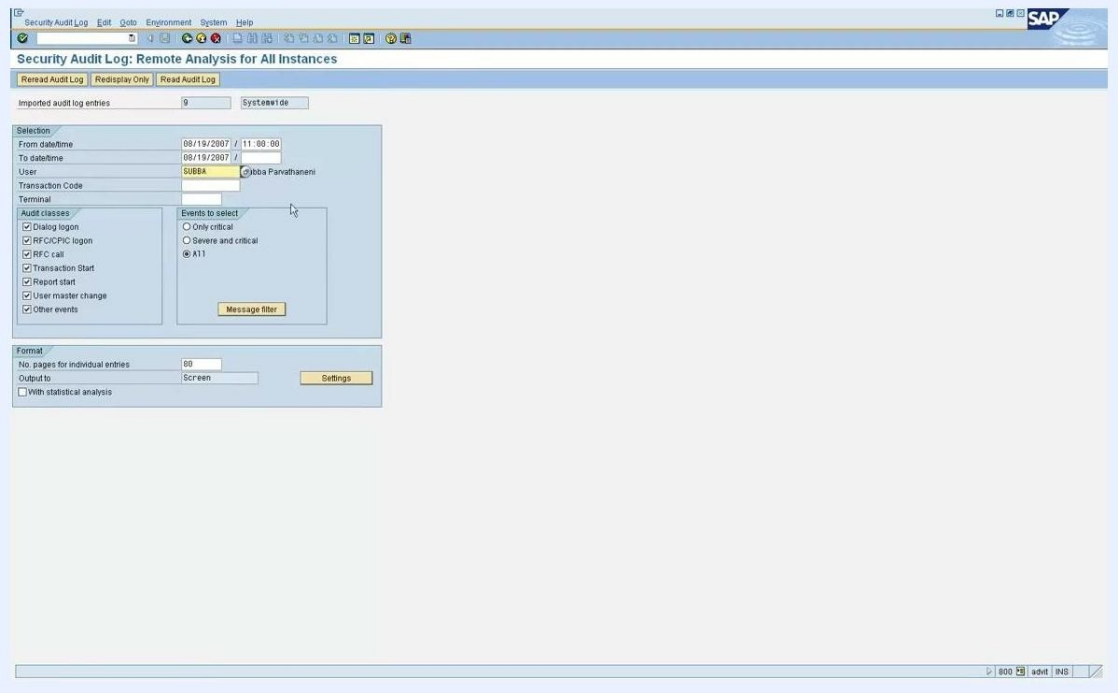

**Security Audit Log: Local Analysis screen with user subba, date/time range, audit classes, and output settings**

## Step 13: Set the criteria for a systemwide analysis

To analyze the audit log across all application servers, open the **Security Audit Log: Remote Analysis for All Instances** screen. It offers options to reread, redisplay, or read the audit log. The "Imported audit log entries" field shows the number of entries, for example 9.

1. In the "Selection" section, enter 08/19/2007 11:00:00 as **From date/time** and 08/19/2007 as **To date/time**.
2. Enter SUBBA as the **User**. You can also use the **Transaction Code** and **Terminal** fields for further filtering.
3. In the "Audit classes" section, select Dialog logon, RFC/CPIC logon, RFC call, Transaction Start, Report start, User master change, and Other events.
4. In "Events to select", choose "All".
5. Set the number of pages for individual entries to 80.
6. Set **Output to:** "Screen".

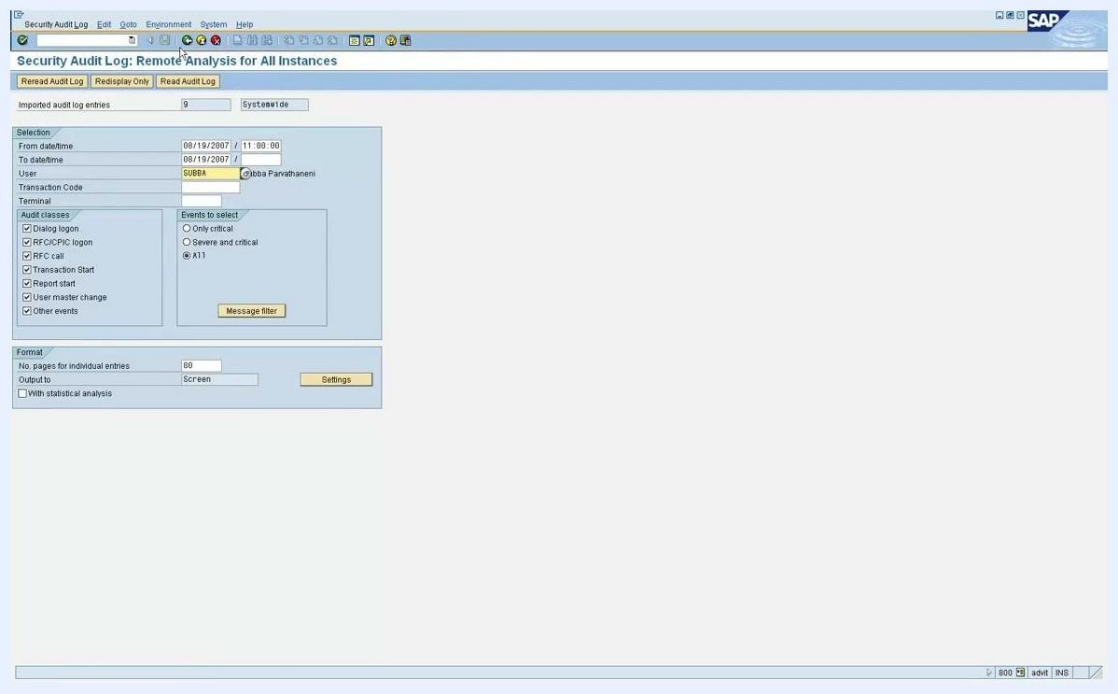
7. Optionally, click "Settings" or "Message filter" to refine your search.




**Security Audit Log: Remote Analysis for All Instances screen with user SUBBA, date/time range, audit classes, and the Systemwide option**

## Step 14: Include all application servers

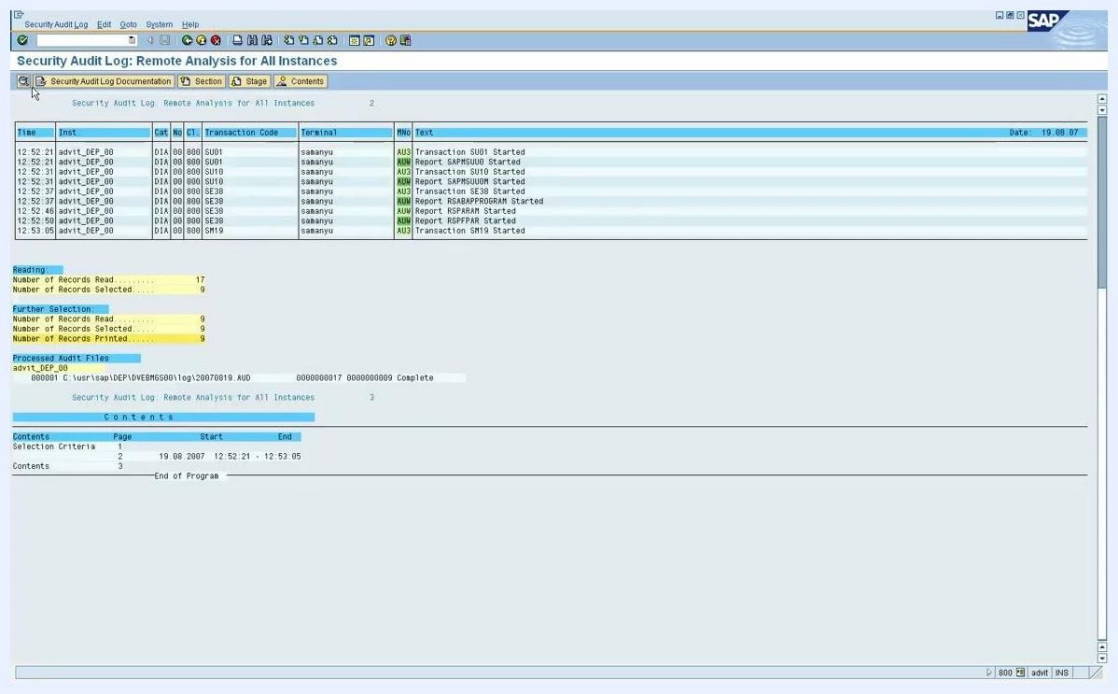
Click the "Systemwide" button to include logs from all application servers. This matters if your SAP system has multiple application servers, because checking only one server may not give you a complete picture.




**Systemwide option highlighted on the Security Audit Log: Remote Analysis for All Instances screen**

## Step 15: Run the log analysis

After you set your criteria, click the appropriate button (for example, "Read Audit Log") to run the analysis. The system processes your request and displays the results.



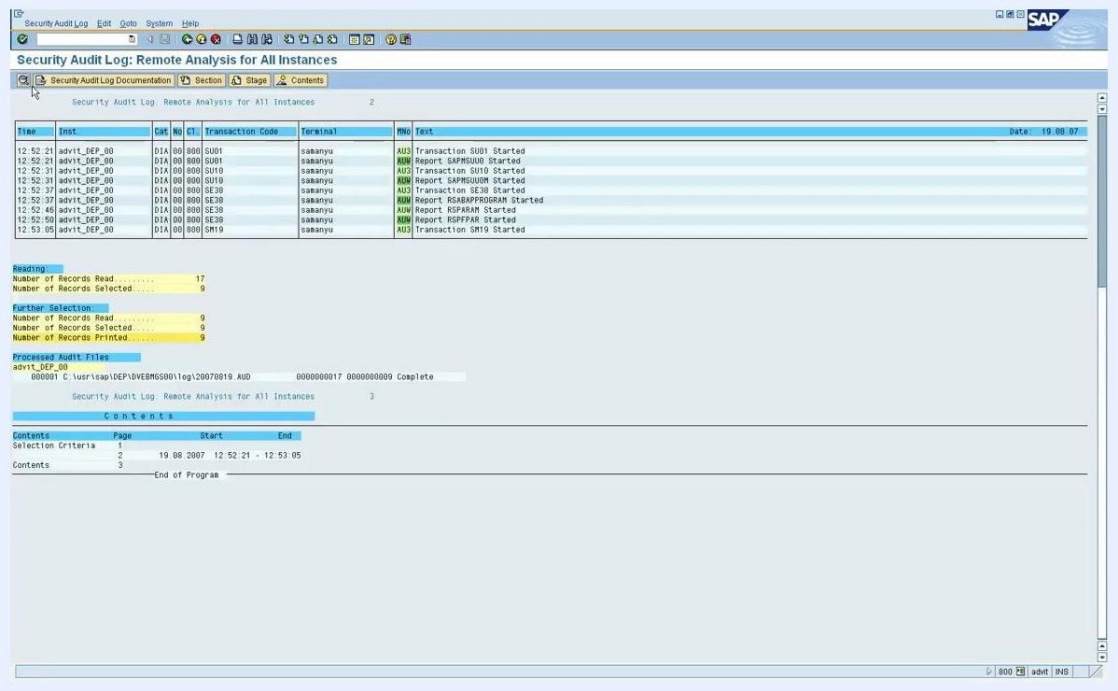

**Security Audit Log: Remote Analysis for All Instances screen with the selection criteria set and ready to run**

## Step 16: Review the audit log results

The results screen shows a table with these columns:

- **Time**: Timestamp of the event, for example 12:52:51.
- **Server**: Server name, for example advit_DEP_00.
- **Cat**: Category, for example DIA.
- **No**: Number, for example 800.
- **Transaction Code**: The code executed, for example SU01, SU10, SU38, or SM19.
- **Terminal**: Terminal or user, for example samanyu.
- **MNo**: Message number, for example AU3.
- **Text**: Description, for example Transaction SU01 Started or Report SAPMSUUU Started.

The lower section summarizes the number of records read, selected, and printed. It also lists the processed audit files with their paths, and the selection criteria and contents.




**Security Audit Log: Remote Analysis for All Instances results screen showing transaction codes and reports started by user SUBBA**

Use the results to determine which transaction codes were executed, which programs or reports were started, and the sequence and timing of user actions. The audit log shows the program or transaction name, but not the detailed actions performed within each transaction.

## Step 17: Deactivate the filter when you no longer need it

To stop logging further actions, return to transaction SM19 and deactivate the filter.

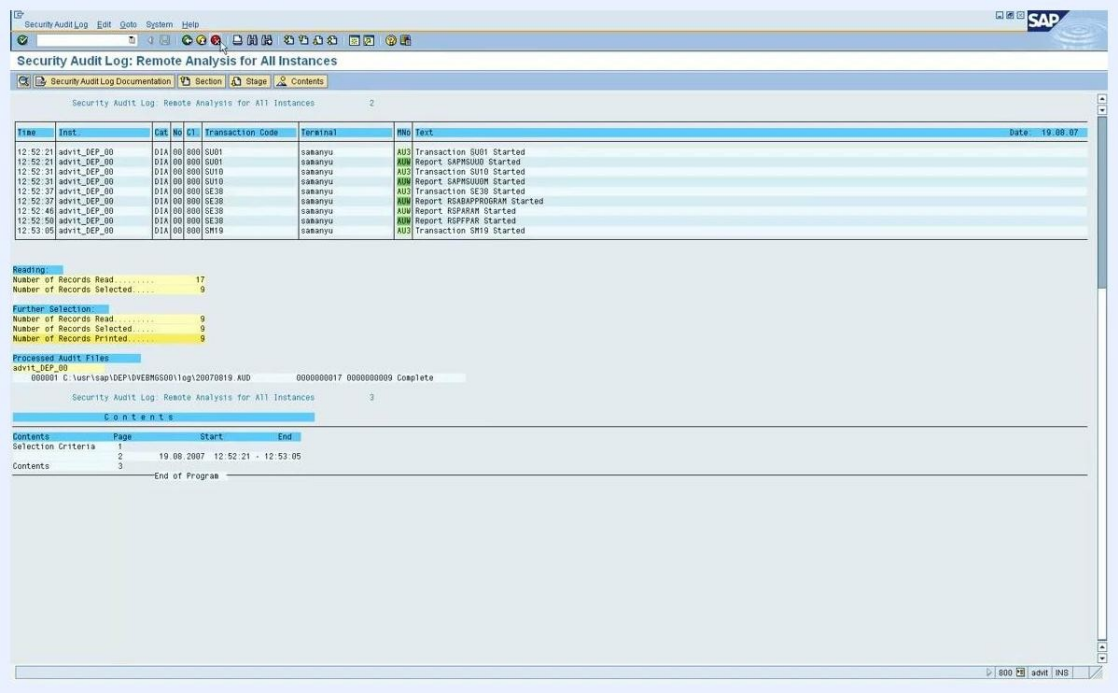
## Step 18: Understand the SM19 filter limits

In SM19, you typically see only two filters: **Filter 1** and **Filter 2**. These filters define which activities to log based on client, user, audit classes, and event types.

You could keep a filter active indefinitely and use wildcards (* *) to log all activities for all users and clients. This requires enough disk space at the operating system level, because audit logs can grow large over time.

The **Status of Recording on Individual Servers** section in this example shows:

- **Server Name:** advit_DEP_00
- **Status:** *
- **Current File Size:** 3,320 KB
- **Maximum File Size:** 976 KB




**Security Audit: Display Configuration of All Instances screen showing Filter 1 and Filter 2, with status and file size information for server advit_DEP_00**

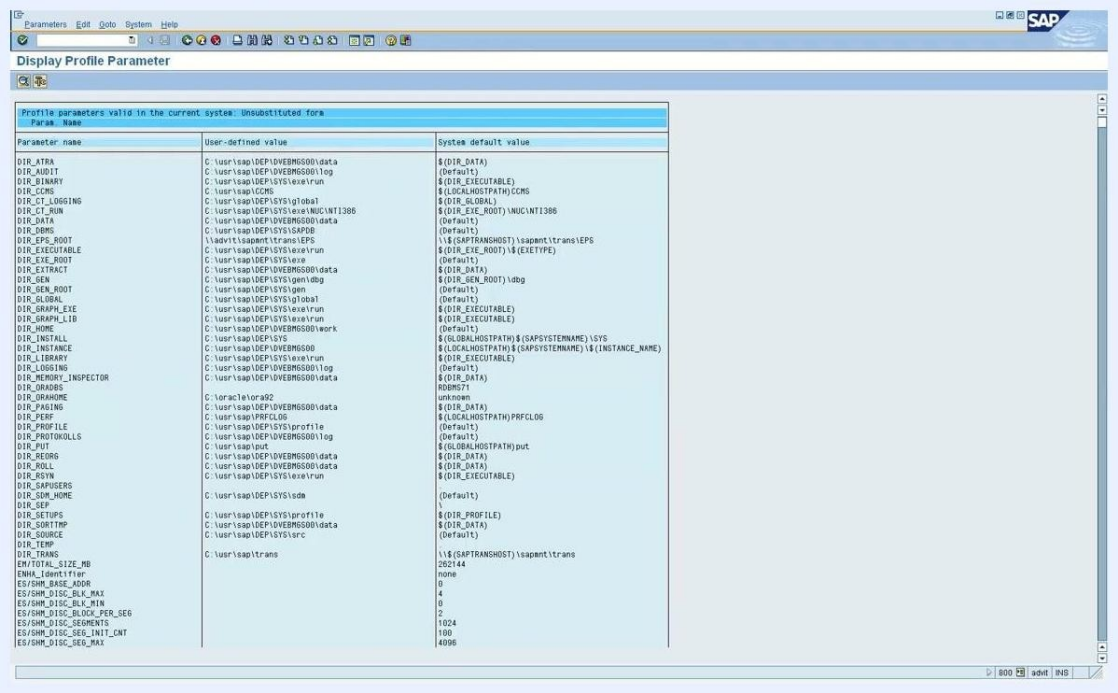
## Step 19: Review the RSAU parameters

1. Open the **Display Profile Parameter** screen in SAP.
2. Use the Find function to search for rsau parameters.
3. Review the parameters related to audit logging, such as:

- rsau/max_diskspace/local
- rsau/max_diskspace/per_day
- rsau/max_diskspace/per_file
- rsau/selection_slots

- rsau/user-selection
- rsau/SQL-Audit/filename
- rsau/SQL-Audit/filesize
- rsau/SQL-Audit/logdir
- rsau/SQL-Audit/switch
- rsau/enable

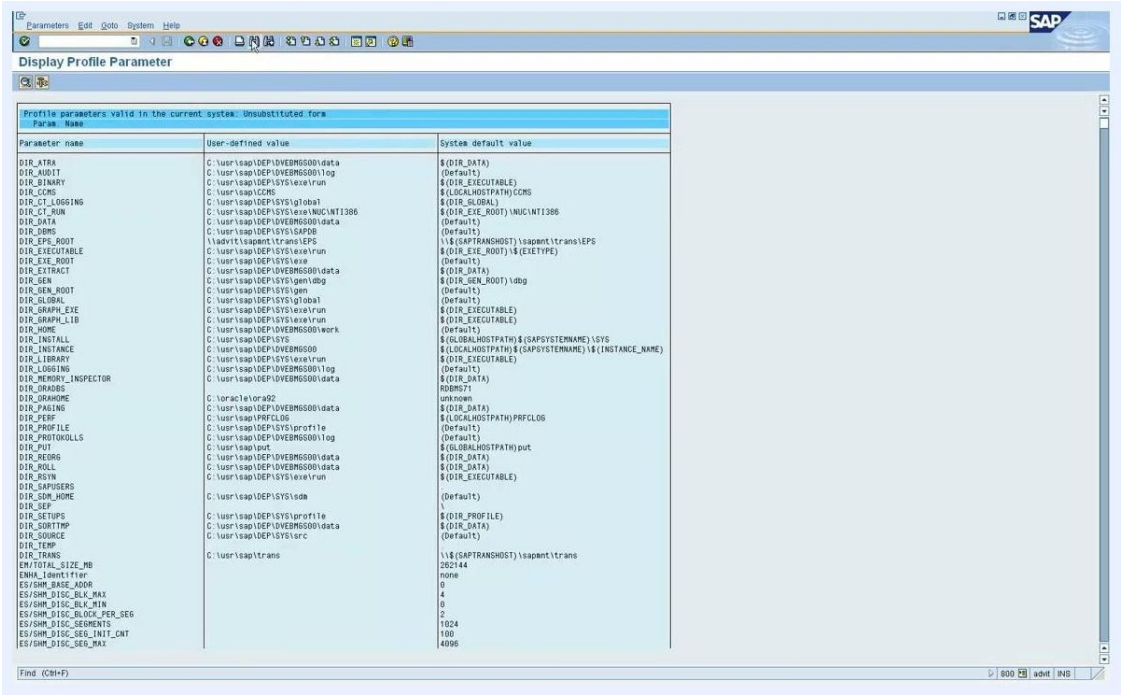
Note the current values and paths, such as the log directory C:\usr\sap\DEP\DVEBMGS00\log.




**SAP Display Profile Parameter screen with the Find dialog showing RSAU-related parameters and their values**

## Step 20: Adjust the number of selection slots

The parameter rsau/selection_slots controls how many filter tabs SM19 displays. If you set rsau/selection_slots = 10, SM19 displays 10 filter tabs. If you set it to 12, SM19 displays 12 tabs. Adjust this value according to your audit requirements.




**Find dialog in the Display Profile Parameter screen highlighting rsau/selection_slots and related parameters**

## Step 21: Apply and verify the parameter changes

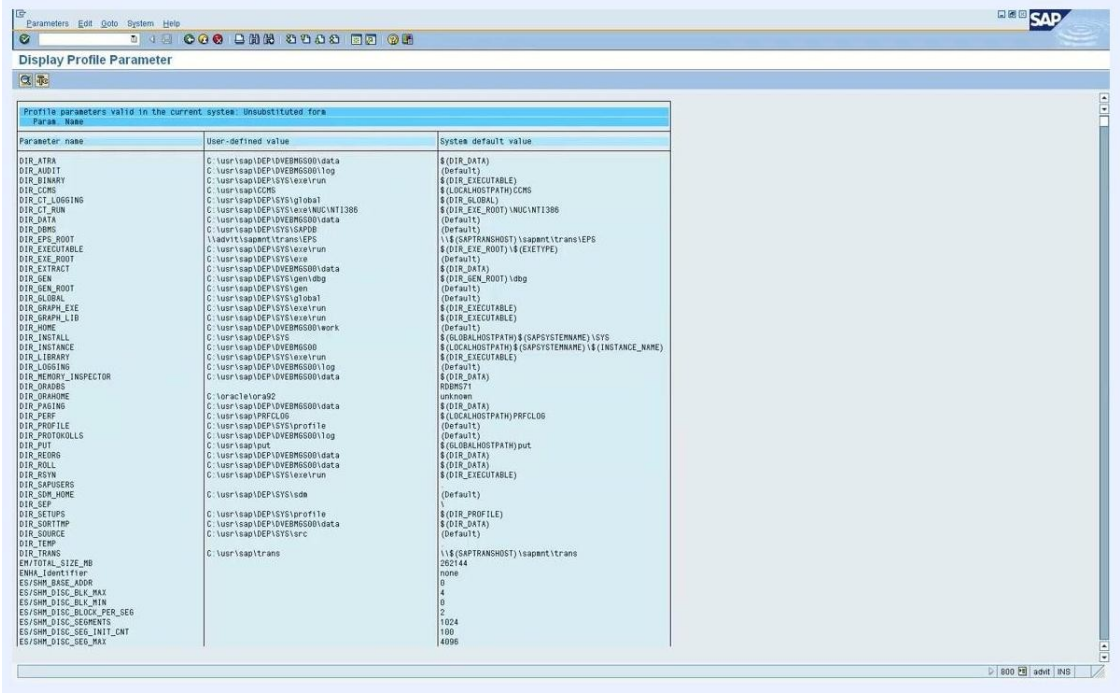
1. After you adjust the RSAU parameters, save your changes.
2. Restart the SAP instance if required for the changes to take effect.
3. Return to SM19 and verify that the number of filter tabs matches the value in rsau/selection_slots.

Test parameter changes in a non-production environment before you apply them to live systems.

## Step 22: Monitor audit log file growth

If audit logging is enabled for all users, the audit log files grow rapidly. The more users you log, the faster the files reach their maximum size. When the maximum is reached, additional log files are created as configured, but performance issues can still occur if you don't manage this.

1. Return to the **Security Audit: Display Configuration of All Instances** screen.
2. Check the **Current File Size** and **Maximum File Size** columns for each server. In this example, server advit_DEP_00 shows a current size of 3,320 KB and a maximum of 976 KB.
3. If the current size exceeds the maximum, the log files are growing too quickly, likely because of high user volume.

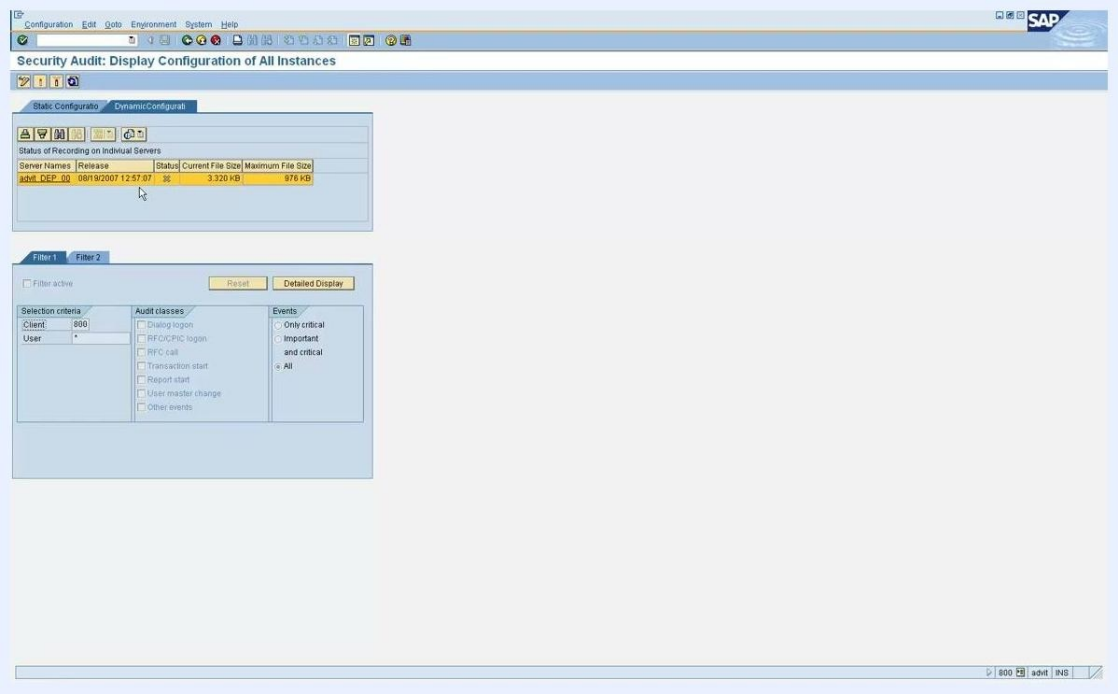



**Security Audit: Display Configuration of All Instances screen showing a file size that exceeds the maximum**

If audit log files exceed their maximum size, the system may experience errors, dumps, or degraded performance. Customers may encounter performance-related problems if log file management is not properly configured.

## Step 23: Keep the configuration available for audits

The audit log settings and file size monitoring are essential from an audit point of view. Make sure the configuration is documented and available to auditors as needed.




**Security Audit: Display Configuration of All Instances screen with audit filters and file size details**

## Summary

You now know how to configure an audit log in SAP. You set filters in SM19, activated them, selected audit classes and events, saved and distributed the configuration, and reviewed user activity with SM20 and the systemwide remote analysis. You also learned how the RSAU parameters control the number of filters and how to watch file sizes. Monitor disk usage and adjust your filter settings to balance audit requirements with system performance and storage.

## What's next

- Review the audit log results regularly to see which transactions and reports users started.
- Adjust rsau/selection_slots if you need more filters for detailed monitoring.
- Check the current and maximum file sizes on a regular basis.

- Deactivate filters in SM19 when you no longer need to log activity.