

Reading Sample

In these chapters you will learn how to secure SAP system clients and how to log system activities and prepare for audits.



“Securing Clients”

“Auditing and Logging”



Contents



Index



The Authors

Joe Markgraf and Alessandro Banzer

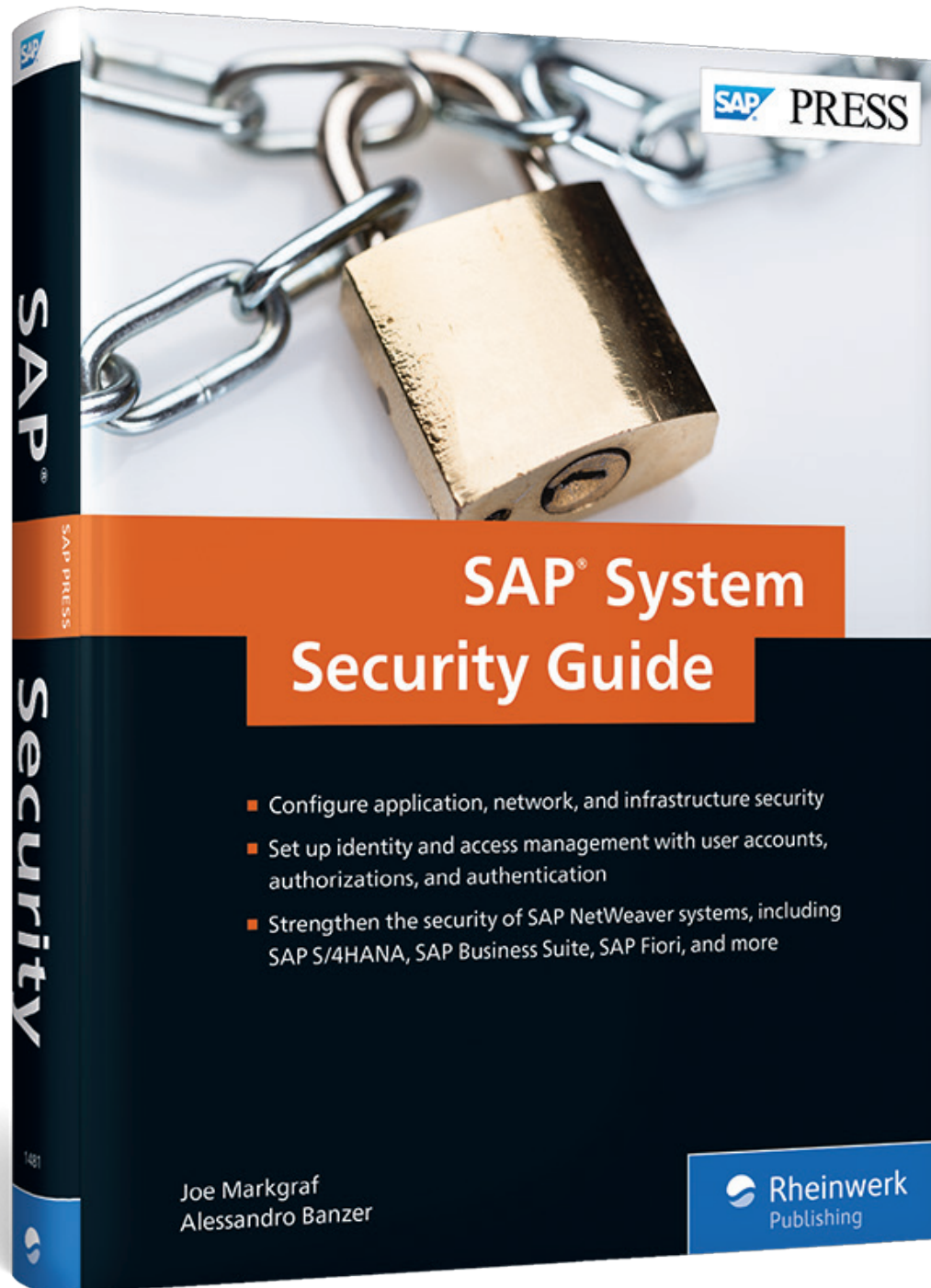
SAP System Security Guide

574 Pages, 2018, \$79.95

ISBN 978-1-4932-1481-5



www.sap-press.com/4307



Chapter 4

Securing Clients

Before reading this chapter, you must have a basic understanding of the client concept in an SAP system. You must also understand how to navigate within SAP GUI.

In an SAP NetWeaver system, all business data is isolated on the client level. This means that users that work in one client can't access the data of another client. This architecture is ideal for shared systems that multiple organizations might use. It also allows for the separation of different clients for different activities or use cases. For example, testing clients and development clients could be created on the same SAP installation to allow users to develop and test in the same system without getting in each other's way. Some organizations will choose to have multiple development clients, or multiple test clients. Others will use different clients to separate HR and finance activities. Some organizations will have each of their subsidiaries operate in a separate client in the same master system.

Here are the basic rules that define clients:

- Clients can never read or write to other clients.
- The business data of a client is separated from other clients.
- Clients share the same SID but have different client numbers.
- Multiple clients may exist in an SAP system.
- Clients may be copied or deleted and won't affect other clients.

How is a client different than just having another system? To start, multiple clients can exist in a single system. A client will typically represent a separate organization or company within an SAP system but share the same technical SAP NetWeaver instance. Therefore, the overhead to maintain the instance is shared. However, some organizations will adhere to a strict, productive single client per system. It all depends on the architecture your organization has chosen.

You can think of clients as floors of an office building. Multiple organizations can occupy offices on different floors in an office building. All the building tenants share

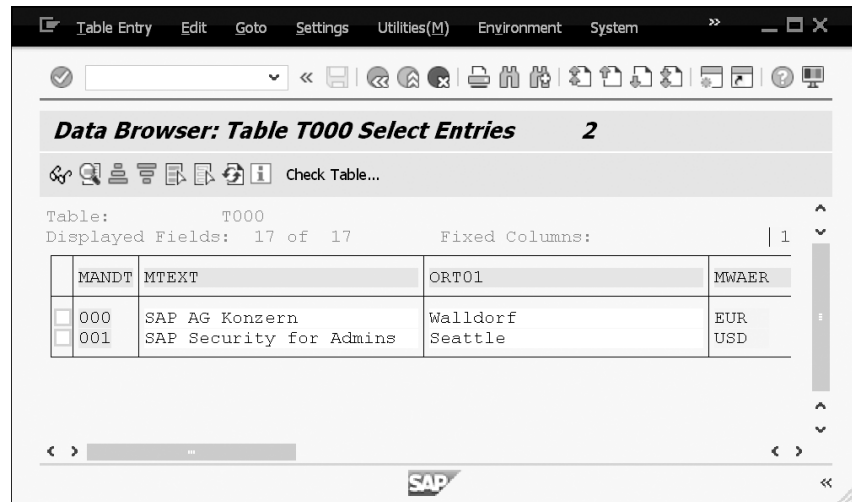
the same infrastructure (power, water, Internet, heating), but they operate as separate entities isolated from each other by the floor and ceiling. What's said on one floor isn't overheard on another. A disruption on the top floor won't affect the bottom floor.

One key takeaway from this example is that in the office building some infrastructure is shared; in an SAP system, this shared infrastructure is called *client-independent*. Client-independent objects or tables are common for all clients. On the other hand, *client-dependent* objects are never shared with other clients.

Client-Dependent Database Tables: MANDT Field

The technical table field that denotes a client is the MANDT field. This field is present in all client-dependent tables. Client-independent tables don't have a MANDT field and represent any and all clients. Use care when changing client-independent tables as they affect all clients.

Most SAP NetWeaver systems have at least two clients, if not more. To identify what clients exist in your SAP system, simply look at table T000, the clients table (see Figure 4.1).



MANDT	MTEXT	ORT01	MWAER
<input type="checkbox"/> 000	SAP AG Konzern	Walldorf	EUR
<input type="checkbox"/> 001	SAP Security for Admins	Seattle	USD

Figure 4.1 Table T000: Client List

Common clients you will see are client 000, client 001, and client 066. These clients are usually delivered/created by SAP. You may see more or fewer clients, depending

on how your SAP system has been set up. You'll also see one or more productive clients, or clients that contain your business data. These are clients that your users will log in to and perform work on. Later in this chapter (Section 4.1.3), we'll cover more about securing clients, but for now let's explore the basics.

Now that you're familiar with the concept of multiple clients, let's explore the possible settings for each client. Some clients will be used to change code, others could be used for testing, and some will always be used by business end users in production. Client settings tell the SAP system what's allowable and what's restricted in each of these clients.

In a production or testing client, you wouldn't want a developer to be able to change objects. On the other hand, in a development client you would want this activity to be allowed. Settings like this are what we use to achieve a desired client scenario. In Section 4.1, we'll walk through how to check the current settings for a client.

As security administrators, we're interested in client settings because we'd like to prevent users from being able to change objects unless absolutely necessary. Even if the client settings are correct in one client, an errant setting in another client could lead to changes being made and passed to another client within the same system, *even if that client had the correct settings*. It's imperative that client settings are closely managed for all clients within both an SAP system and all SAP systems within a landscape.

From time to time an administrator may be asked to change the settings of a client. This activity should always be done temporarily because a client should have a steady state in which its settings are fixed. Often, clients are opened for simple changes and are then forgotten about and stay open until the next audit—or even worse, a malicious user—discovers the issue. Take care not to let this happen in your organization.

4.1 Client Settings

It's important for a security administrator to know and understand the different possible client settings and what they may be used for. Before we explore specific settings in depth, let's walk through how to check client settings in the system.

To check client settings, follow these steps:

1. Navigate to Transaction SCC4 (see Figure 4.2).
2. Double-click the client you'd like to view. For this example, client 001 has been selected (Figure 4.3).

Client	Name	City	CrCY	Cl-#
000	SAP AG Konzern	Waldorf	EUR	
001	SAP Security for Admins	Seattle	USD	29

Figure 4.2 Transaction SCC4: Display Clients

Client: 001 SAP Security for Admins

City: Seattle Last Changed By: I851675

Logical System: Date: 29.04.2017

Currency: USD Client role: Production

Changes and Transports for Client-Specific Objects

Changes without automatic recording

Automatic recording of changes

No changes allowed

Changes w/o automatic recording, no transports allowed

Cross-Client Object Changes

Changes to repository and cross-client customizing allowed

Client Copy and Comparison Tool Protection

Protection level 0: No restriction

CATT and eCATT Restrictions

eCATT and CATT Not Allowed

Restrictions

Locked due to client copy

Protection against SAP upgrade

Figure 4.3 Details of Client 001 in a Demo System

Now that you know how to navigate to these settings, let's explore the information on this screen in more detail.

4.1.1 Client Setting Fields

When viewing a client's settings, you'll see the following fields:

- **Client number**
This is a three-digit number that identifies the client within the system. This must be unique and is assigned when the client is created.
- **Client name or short text**
Each client can have a short name assigned to it that helps identify it.
- **City**
The city designation helps differentiate different clients when multiple organizations or divisions are used.
- **Logical System**
The logical system is a technical identifier that comes into play when using system-to-system communication. It's very important to have a proper logical system name defined.
- **Currency**
This field denotes what standard currency the client uses.
- **Last Changed By**
This field denotes which user last changed the settings of the client. It is often checked for auditing purposes.
- **Date**
This field denotes the date the client was last changed.
- **Client Role**
Possible choices are as follows:
 - **Production**
For the active use of business users. It's essential that no changes are made in this client.
 - **Test**
Developers use this client setting to test their Customizing settings and workbench developments.
 - **Customizing**
For the creation of Customizing settings and workbench developments.

- **Demo**
For demonstration or prototyping purposes.
- **Training/Education**
Typically used to train users on changes before import into production.
- **SAP Reference**
Clients used by SAP.
- **Changes and Transports for Client-Specific Objects**
Client-specific objects have values based on a client value. This means that a client-specific object can have a different value based on what client it's contained in. These options cover changes to these objects and how they're transported using the transport system. Possible choices are as follows:
 - **Changes without automatic recording**
This means that changes in the customizing settings of the client are allowed. They aren't automatically captured in a transport for moving to other systems or clients. Changes can be manually transported to other clients or systems.
 - **Automatic recording of changes**
This means that changes to the customizing settings of the client are allowed. They're automatically captured in a transport for moving to other systems or clients.
 - **No changes allowed**
Changes to the customizing settings of the client aren't allowed with this setting.
 - **Changes w/o automatic recording, no transports allowed**
Changes are allowed to the customizing settings of the client but may not be transported with this setting.
- **Cross-Client Object Changes**
Cross-client objects have a single value for the entire system. This means that cross-client objects have the same value regardless of what client the user's logged into. These options cover changes to these objects and how they're transported using the transport system. Possible choices are as follows:
 - **Changes to repository and cross-client customizing allowed**
There are no restrictions on the changes of cross-client objects for the client when this setting is used. Both cross-client Customizing objects and objects of the SAP repository can be changed.

- **No changes to cross-client customizing objects**
Cross-client Customizing objects can't be changed in a client with this setting.
- **No changes to repository objects**
Objects of the SAP repository can't be maintained in a client with this setting.
- **No changes to repository/cross-client customizing objects**
Combination of both previous restrictions: neither cross-client Customizing objects nor objects of the SAP repository can be changed in a client with this setting.
- **CATT and eCATT Restrictions**
This setting either allows or restricts the Computer-Aided Test Tool (CATT) and enhanced CATT (eCATT), which are scripting utilities used for automated testing. This setting either permits these scripts to run or prevents them from doing so.
- **Restrictions**
This setting outlines other restrictions that can be made to the client. The options are:
 - **Locked due to client copy**
This checkbox will indicate when the client is locked against logon. It's used during a client copy to prevent data changes during the copy. It's not a selectable box because it only indicates status.
 - **Protection against SAP Upgrade**
This checkbox will prevent an upgrade from taking place on this client when the system itself is being upgraded. It's only used in exceptional cases.

4.1.2 Suggested Client Settings

Table 4.1 through Table 4.4 list the suggested client settings for typical use cases. To summarize, production and test clients shouldn't be open to changes. However, development clients should be because their purpose is to implement changes. As always, client 000 should also be protected from changes because it's the SAP-delivered reference client.

Settings	Client 000, Any System
Client role	SAP reference
Changes to client-specific objects	No changes allowed

Table 4.1 Suggested Client Settings for Client 000 in All Systems

Changes to cross-client objects	No changes to SAP repository or Customizing
Client copy protection	Protection level 1: no overwriting

Table 4.1 Suggested Client Settings for Client 000 in All Systems (Cont.)

Settings	Productive Clients
Client role	Production
Changes to client-specific objects	No changes allowed
Changes to cross-client objects	No changes to SAP repository or Customizing
Client copy protection	Protection level 1: no overwriting

Table 4.2 Suggested Client Settings for Productive Clients

Settings	Testing Clients
Client role	Test
Changes to client-specific objects	No changes allowed
Changes to cross-client objects	No changes to SAP repository or Customizing
Client copy protection	Protection level 0: no restrictions

Table 4.3 Suggested Client Settings for Testing Clients

Settings	Development Clients
Client role	Customizing
Changes to client-specific objects	Changes are automatically recorded
Changes to cross-client objects	Changes allowed to SAP repository or Customizing
Client copy protection	Protection level 1: no overwriting

Table 4.4 Suggested Client Settings for Development Clients

4.1.3 Changing Client Settings

Now, let's walk through how to change client settings. Follow these steps:

1. Navigate to Transaction SCC4.
2. In the upper-left menu, click **Table View**, then select **Display • Change** (Figure 4.4).

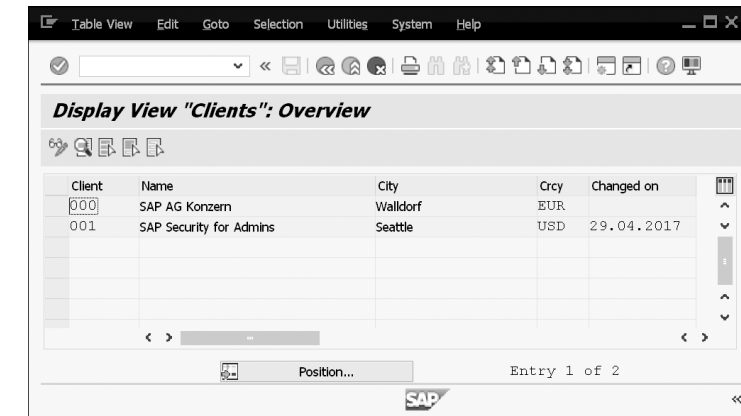


Figure 4.4 Change Table View

3. The system will prompt you with a warning about the table being cross-client (Figure 4.5). Click the check button to proceed.

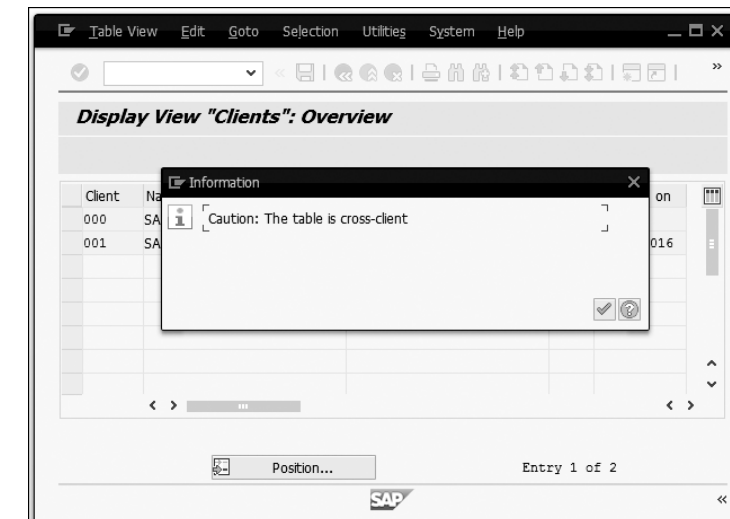


Figure 4.5 Cross-Client Warning

4. Double click on the row of the client you'd like to change settings for (Figure 4.6).

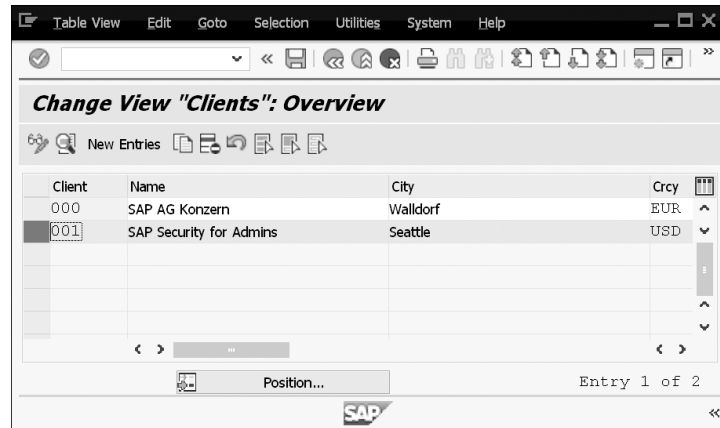


Figure 4.6 Select Client to Change Settings

5. The system will now display, in change mode, the settings for the client you have selected (Figure 4.7).

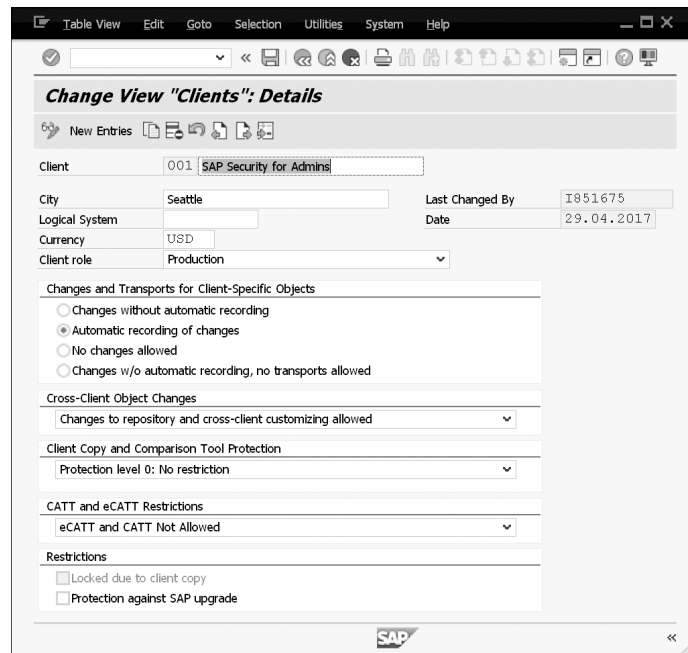



Figure 4.7 Change Mode in Transaction SCC4

6. Once you've made your changes, click the **Save** icon .

Depending on your chosen client settings, you may see a transport request. This is to ensure that your settings can be move to any other systems you choose. If you don't want to transport your client settings, delete the transport that you create to contain this change.


4.2 Client Logon Locking

Occasionally, you'll need to lock a client. This may be for an upgrade or a system maintenance activity. Locking the client will prevent users from logging into the client that is locked. A similar effect can be gained by locking all users in a client using Transaction SE10, but the method described in this section is more quickly implemented. Locking using Transaction SE10 will be covered in Chapter 6.

Remote Locking

This procedure can be done in any client, to any client, or with an RFC connection to a remote system with the proper authorizations.

To lock a client and prevent logon, follow these steps:

1. Navigate to Transaction SE37.
2. Enter the **Function Module** name "SCCR_LOCK_CLIENT" and click the **Test/Execute** button  in the toolbar (Figure 4.8).

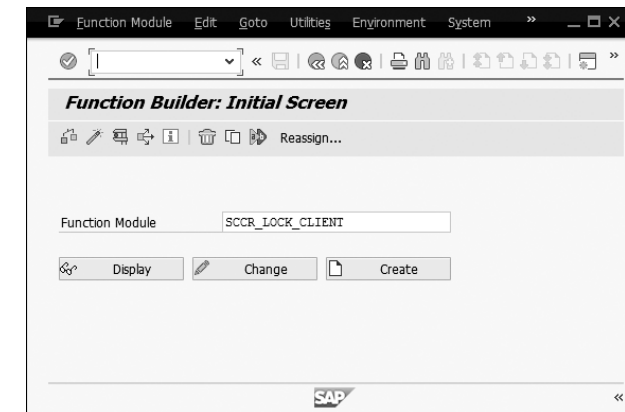



Figure 4.8 Enter Lock Client Function Module Name

- Enter the number of the client for which you'd like to prevent logon (Figure 4.9).
Click the **Execute** button  in the toolbar.

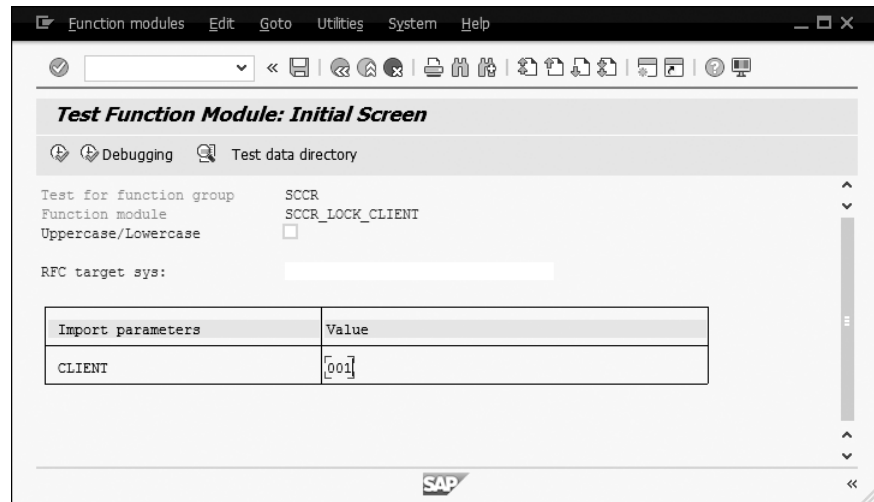


Figure 4.9 Enter Number of Client to Lock

Now, if a user attempts to access the locked client, he will receive the notification seen in Figure 4.10.

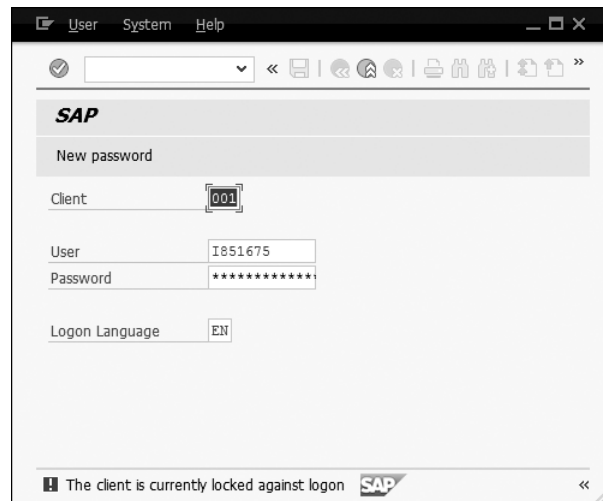



Figure 4.10 Client Locked against Logon Notification

To unlock a client, follow these steps:

- Navigate to Transaction SE37.
- Enter the **Function Module** name "SCCR_UNLOCK_CLIENT" and click the **Test/Execute** button  in the toolbar (Figure 4.11).

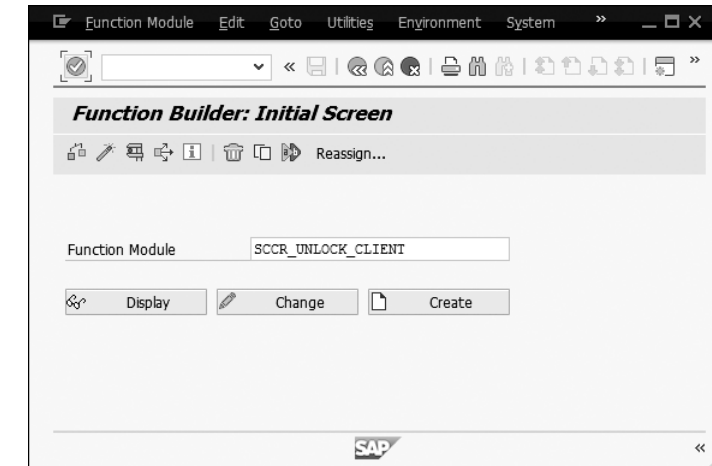



Figure 4.11 Enter Unlock Client Function Module Name

- Enter the number of the client you'd like to unlock for logon (Figure 4.12). Click the **Execute** button  in the toolbar.

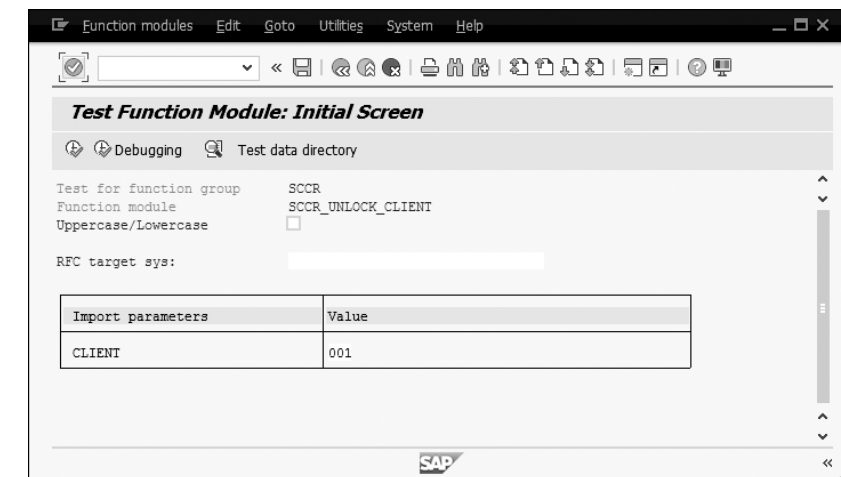


Figure 4.12 Enter Number of Client to Unlock

4.3 Summary

In this chapter, you learned about client settings and how they're used to control what's allowed in each client. We covered what settings are appropriate in specific client roles and what the production client should be set to. You also learned how to lock users out of a client and how to reverse that lock.

In the next chapter, you will learn about the set of executables that make up the SAP NetWeaver AS ABAP system, called the kernel. The kernel is an integral part of the system that administrators must keep up to date.

Chapter 11

Auditing and Logging

To keep a system secure, it's essential to have eyes on all parts of the system and the changes being made therein. Security audit logging records all security events for later analysis; table logging records changes made to tables, including when the changes were made and by whom. In this chapter, you'll learn to configure and enable security audit logging and table logging.

Certain activities in the SAP system are periodically checked and reviewed by an auditor. Therefore, you must ensure that those activities are recorded in the system. The security audit log provides a framework to record security-related events in the system—for example, Remote Function Calls (RFCs), logon attempts, changes to the audit configuration, and so on. The security audit log doesn't log changes to the data within the SAP system that are stored in the database. However, with the table-logging functionality, you can record changes to a table. It's not recommended to log all table changes—only the ones that are considered important and hence for which changes must be traceable. For example, important tables include table T000 (clients), table TCUR (exchange rates), and others.

To analyze the workload of the SAP system, you can use the Workload Monitor, which is also a neat tool to analyze a user's history. The Workload Monitor records historical usage data and allows you to drill down on a user level.

As data protection laws gain ground, protecting your data becomes more and more important. To protect the privacy of and personal information in your SAP system, along with sensitive and classified data, you can use Read Access Logging (RAL) to record read activity.

In this chapter, you'll learn how the different logging functionalities work, what makes them unique, and the impact on your system.

11.1 External Audits

Often, a security administrator will find herself being asked to help with an external audit. Before we tackle the task of assisting with an audit, first we'll cover what these audits do for a company.

External audits are typically financial; that is, they center on the financial records of the company. These audits typically focus on any customer running the SAP ERP or SAP S/4HANA finance functionality on SAP NetWeaver AS ABAP. Two common audits that organizations go through are to check compliance with the Sarbanes-Oxley Act (SOX) and the International Financial Reporting Standard (IFRS). Each of these audits is performed by an *external auditor*, an organization outside of your own that performs the audit. This organization will send one or several auditors who will be tasked with observing and recording proof that the practices of your organization comply with the controls required for your audit.

The Sarbanes-Oxley Act of 2002 set forth internal financial auditing controls in the United States that must be adhered to when preparing financial information for reporting purposes. US-based financial systems are routinely audited to SOX standards.

IFRS is an audit of accounting systems such that they can be compared between countries reliability. It's common to see IFRS audits performed for multinational companies.

Besides these two, there are many other audits that vary country by country. These auditing standards generally are prepared by a country's government-mandated accounting standards organizations and commonly follow Generally Accepted Auditing Standards (GAAS).

The external auditor will be working off a set of controls, in which the security administrator will most likely be the person that is running the queries in the SAP system to satisfy those queries. Most queries are run through the User Information System (UIS; Transaction SUIM). We'll cover the use of the AIS later in this chapter. Auditors may also ask for the output of some standard reports, among other things.

Often, auditors may also ask for access to your system to run reports on their own. Unless this is legally required, it's a good idea to deny this request. When given the choice, it's a more efficient practice for the SAP security administrator to run queries given to them by an auditor. This is done to keep the security administrator in control of the scope of the audit. If an audit is for financial compliance, the auditor should be looking at finance-related authorization objects. Too often, auditors are

given free access to a system, which tends to change the scope of the audit to whatever the auditor feels like digging into.

Often, external audits are focused into categories similar to the following:

- Internal controls
- Network activity
- Database activity
- Login activity (success and failures)
- Account or user activity
- Information access

For each such category, the auditor will require proof that the controls for that category are being applied. They may also ask for a random sample of users or transports, or even provide a time frame and ask to see logs or proof that controls were being adhered to for that time.

11.2 Internal Audits

Internal audits are performed by individuals within your own organization. Often, they focus on preparing for an external audit. However, this isn't always the case. Internal audits can be used to ensure that a specific control or policy is being followed by examining system activity, logs, or even user master records. This type of activity is usually mandated by either the security administrator or an internal audit department for the purposes of verification.

Quite often, when an internal audit is performed, the objective is to improve adherence to the controls that will be followed for an external audit. This will often leave the security administrator with a to-do list to satisfy the audit requirements. In addition, the security administrator may be consulted to help create controls that will help keep compliance such that it's not a major effort when an external audit is performed.

One of the common tasks for an internally led audit is to manage the number of users that have powerful authorizations, like SAP_ALL, or access to perform business-critical tasks, like pay vendors or create accounts. This is done by evaluating the roles and authorization objects that each user master record contains.

The internal audit is also a good time to determine the effectiveness of your general security operations and process. Defining a set of controls and evaluating your

system and users based on those controls can help enforce a strong, consistent level of security.

11.3 Auditing Tools

SAP systems are equipped with a set of tools that can be used for auditing. Such tools include the security audit log, the system log, table logging, the Workload Monitor, as well as Read Access Logging and the User Information System. All these tools can be utilized to extract and analyze data about certain activities in the system, such as who logged on to a system, who changed a certain table, who accessed certain data, and more. We'll explore each of these tools in more detail in the next sections.

11.3.1 Security Audit Log

The security audit log (SAL) records security-related activities in the system, such as changes to user master records, logon attempts, RFCs, and so on. This tool is designed for auditors to log and review the activities in the system. With the SAL, an auditor can reestablish a series of events that happened in the system.

The SAL offers wide flexibility in its usage. You can activate and deactivate it, as well as change the filters as necessary. For example, you can activate the SAL before an audit takes place and deactivate it once the audit has been performed. Also, you can change the filters and, for example, monitor a user if you've detected suspicious activity in the system.

The audit log must be activated before it can be used. To activate the audit log, you have to specify which activities you want to record in the security audit log. The following activities are available:

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

In addition to these events, the security audit log also logs certain activities that aren't categorizable, such as the following:

- Activation and deactivation of the HTTP security session management or instances in which HTTP security sessions were hard-exited
- File downloads
- Access to the file system that coincides with the valid logical paths and file names specified in the system (particularly helpful in an analysis phase to determine where access to files takes place before activating the actual validation)
- ICF recorder entries or changes to the administration settings
- The use of digital signatures performed by the system
- Viruses found by the Virus Scan Interface
- Errors that occur in the Virus Scan Interface
- Unsuccessful password checks for a specific user in a specific client

Once activated, the system will record the activities into a log file on the application server.

Warning

Be cautious when activating the security audit log because it contains personal information that may be protected by data protection regulations—especially with the new GDPR regulation from the European Union but also other protection laws in other regions. Make sure that you adhere to the regulations in your area.

Versions

Your SAP_BASIS component affects your version of the security audit log. With SAP NetWeaver 7.5 SP 03 for SAP_BASIS, SAP has introduced new functionality in the security audit log.

In the old version, the main transactions for the security audit log were Transactions SM18, SM19, and SM20. In the new version, SAP introduced several new transactions:

- **Transaction RSAU_CONFIG**
Maintenance of the kernel parameters and selection profiles relevant for the security audit log

- **Transaction RSAU_CONFIG_SHOW**
Printable display version of Transaction RSAU_CONFIG
- **Transaction RSAU_READ_LOG**
Audit log evaluation
- **Transaction RSAU_READ_ARC**
Audit log evaluation in archive data
- **Transaction RSAU_ADMIN**
Administration of integrity protection for files; reorganization of log data
- **Transaction RSAU_TRANSFER**
File-based transfer of an audit profile

With the enhanced functionality and the new transaction codes, SAP delivers new features as well:

- Save the audit log into the database, either in full or in part.
- Filter by user groups with the user attribute **User Group for Authorization Check** from the **Logon Data** tab in Transaction SU01.
- Increase the number of filters from 10 to 90.
- Check the file integrity.
- Use an enhanced authorization concept with authorization object S_SAL.
- An API for evaluating log data is provided with the class CL_SAL_ALERT_API.

Tip

If you use the new security audit log, we recommend locking the old transactions with Transaction SM01_CUS in client 000. Parallel usage of the old and new functionality is possible but not recommended.

Usage Scenarios

Depending on your requirements, you can define usage scenarios differently. With the new security audit logging capability, you can define how and where you want to store the audit log, as well as how to access it. With the old security audit log, you could only save data on the file system of the application server; with the new functionality, you can either save on the file system of the application server or in its database. Also, shared scenarios are possible in which some parts will be stored in the database and the some in the file system.

Classical Approach

In the classical approach, similar to the old version, the audit log is only stored on the file system of the application server. You can read the data from the file system, as well as archive and delete old audit log files.

Database Logging

With the new functionality, it's possible to save the audit log into the database. However, system events are stored in the file system as well. Storing the audit log in the database might result in a quick growth of table RSAU_BUF_DATA, which holds the data. With the archiving object BC_SAL you can, however, archive the data in that table. With the database, you have an improved experience when accessing the data because it's quicker and the requirements for data privacy are met.

Mixed Scenarios

With the enhanced functionality, you can also activate mixed scenarios in which you generally save the logs on the file system but selective events in the database. When saving selective events in the database, you can access the data faster, which results in a significantly increased performance. That makes sense especially when using statistical data or if you run large evaluations against the log data.

In a second scenario, you can use APIs to transfer data from the security audit log to a central monitoring system (e.g., SAP Solution Manager). In that scenario, the SAL saves the data in the file system of the application server. Certain events that are relevant for the central monitoring systems, such as those to create alerts, are stored in the file system and in database table RSAU_BUF_DATA. The API that transfers the data will read the data from the table and then automatically delete it. Your logs are still available in the file system but will be removed from the database table and hence don't require archiving activities in the database.

Configuration

The new security audit log offers an enhanced configuration via Transaction RSAU_CONFIG. Let's explore configuration in detail now.

In general, the security audit log requires some parameters and the definition of filters that define which events will be logged.

To define the parameters, enter Transaction RSAU_CONFIG and open the **Parameter** folder (Figure 11.1).

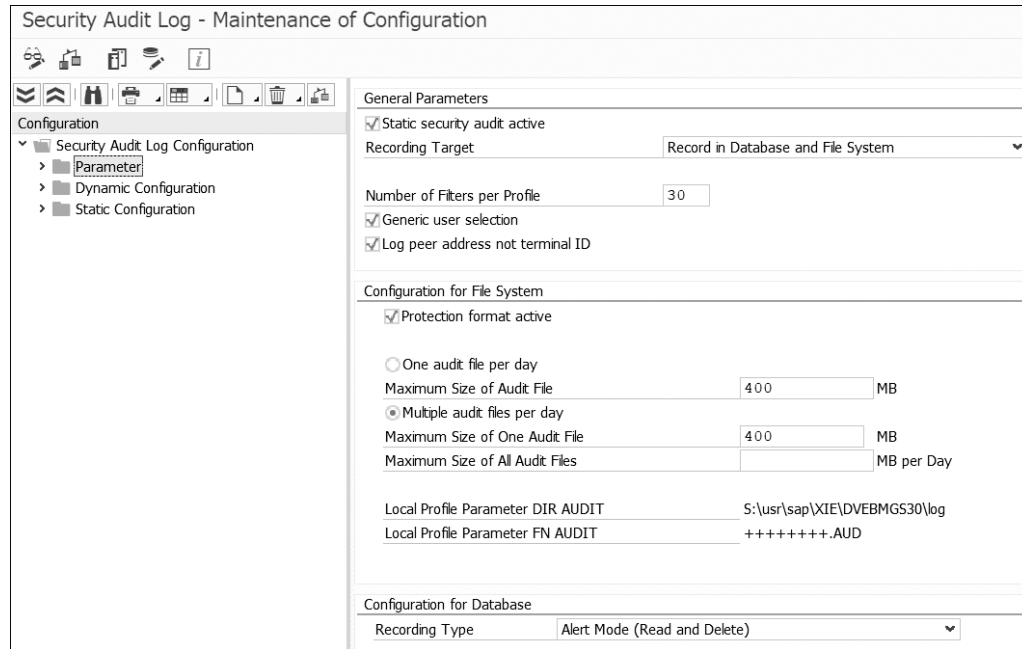


Figure 11.1 Parameter Maintenance in Security Audit Log Configuration in Transaction RSAU_CONFIG

The following can be configured:

- Activate or deactivate logging.
- Define the recording target, whether it's on the file system, in the database, or a combined recording in both the file system and database.
- Define the number of filters per profile, up to 90.
- Define if you'll allow generic user selection with an asterisk (*) character in the filters.
- Define if you log the IP address of the originator and not the terminal ID.
- Activate or deactivate integrity protection format for log files in the file system.
- Define the memory space usage when file system storage is used.
- Define the recording type in the database, whether it's temporary data or permanent data.

In the profiles, you define which events will be logged. To create a new profile or an additional profile, simply right-click the **Static Configuration** folder and choose

Create New Profile. Once the profile is created, you can go ahead and define the settings. Remember that each profile must have at least one filter. To add additional filters, you can simply right-click the **Profile** folder and choose **Create Filter**.

Regardless of the filter you create and specify, it's important to activate the filter once defined by clicking the **Activate** button (Figure 11.2). Only active filters will be selected at the next system start. You can define as many filters as you have defined in the parameter maintenance for each profile.

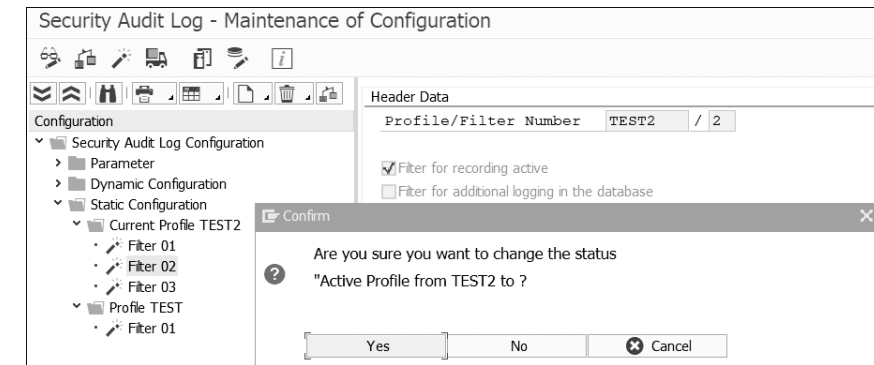


Figure 11.2 Activation of Filters in Transaction RSAU_CONFIG

Each filter that you add to a profile is linked via an OR connector. So, for example, if you have two filters, and the first filter logs everything for user group SUPER and the second filter everything for users starting with RFC*, then those two filters are *OR linked*. That means that all users that belong to user group SUPER and all users starting with RFC* will be logged. Note that user groups only allow for a specific value and that you can't use wildcards as you can for the user name.

In the **Standard Selection** screen, shown in Figure 11.3, where you define the client and whether you want to restrict the logging of a user name or user group, you can select the user group either positively or negatively. **Select by User Group (Positive)** means that you will log all users that are part of that user group. If you use the negative selection, the system logs the events for all users who aren't part of the user group. Possible scenarios for a negative selection can include wanting to log RFC function calls for all users who aren't technical and hence aren't part of a certain user group because those users shouldn't perform RFCs.

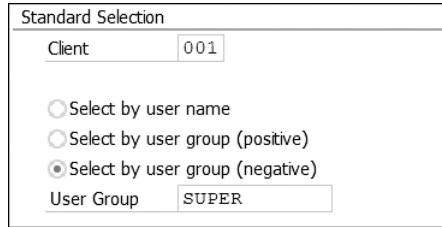


Figure 11.3 Standard Selection in Security Audit Log Configuration

In the **Event Selection** screen (Figure 11.4), you can define which events you want to log. In the **Classic event selection**, you get the same options as in the old security audit log.

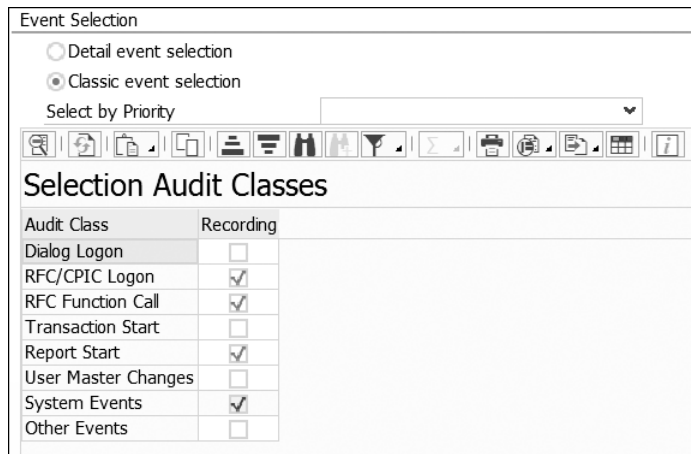


Figure 11.4 Classical Event Selection in Security Audit Log Configuration

In the **Detail event selection** (Figure 11.5), you can slice and dice on a more granular level and pick and choose events more specifically. For example, in the classical selection, you choose **Dialog Logon**, whereas in the detailed selection you can decide whether you want successful logons or failed logons.

If you defined the selection in the classic event selection, the underlying detailed events will be selected.

To start the logging of a filter, it's important that the switch **Filter for Recording Active** is selected. You can have active and inactive filters. Therefore, it's important to keep an eye on the **Active** checkbox, as well as if the filter has been activated.

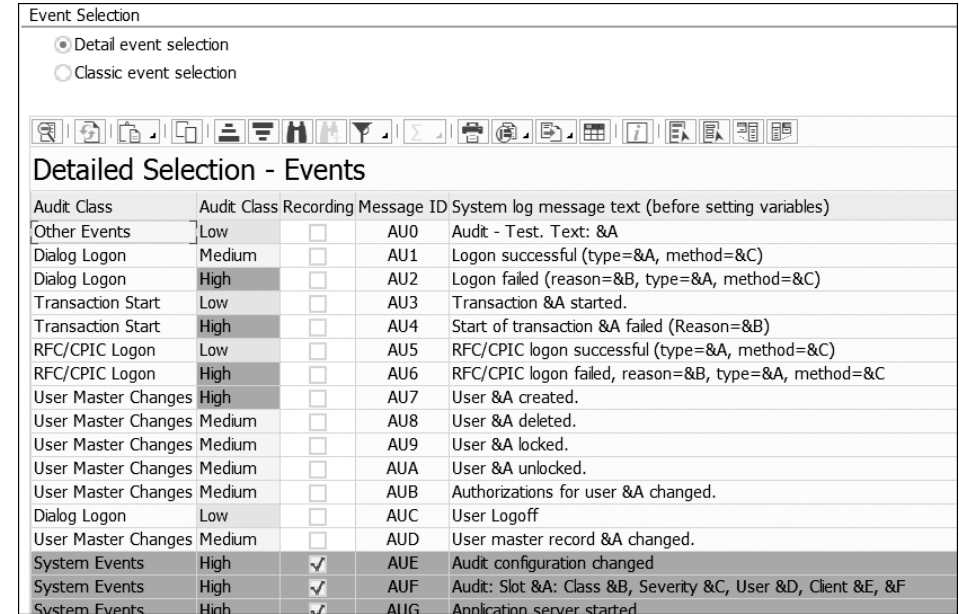


Figure 11.5 Detailed Event Selection Options in Security Audit Log Configuration

Administration of Log Data

The administration of log data takes place in Transaction RSAU_ADMIN (Figure 11.6). In the administration cockpit, you can check the integrity of the file-based log data and reorganize obsolete files. For the database tables, you can use this cockpit to reorganize table RSAU_BUF_DATA by means of deletion or archiving.

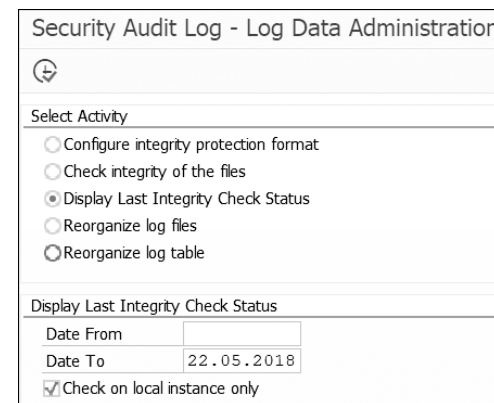


Figure 11.6 Log Data Administration Initial Screen

Integrity Protection

With the integrity protection setting of the SAL, you can protect the security audit log from manipulation of its log files on the file system. However, it doesn't prevent the manipulation of the file but it will tell you if it was manipulated.

To protect the integrity of your files, you can create one hash-based message authentication code (HMAC) per system. To create the HMAC key, choose **Configure Integrity Protection Format** from the initial screen (Figure 11.7) and define your secret **Passphrase**.

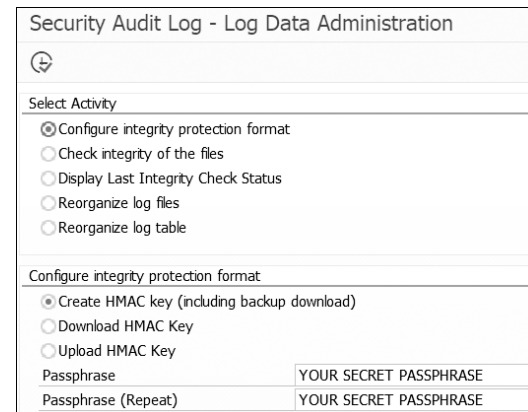


Figure 11.7 Configure Integrity Protection Format

If you wish to restore the key, a local backup file is generated that can be used in combination with the passphrase. Make sure to store the backup file and passphrase so that you can check the integrity of the system later.

If you decide not to create an individual system HMAC key, your integrity is at risk because the integrated key must be considered to be known, as it is set to a default value. That means that you can check the files only against unintentional corruption or change and not against malicious manipulation.

Once configured, all log files written forward will be checked by the integrity protection format. To check the integrity of the files, you can choose **Check Integrity of the Files** on the initial screen (Figure 11.8).

Shorter time frames can be analyzed in the foreground. However, larger periods will be run in the background. Once the check has been performed, you'll see an overview of all the files and their attributes (Figure 11.9). Also, you'll see the status, which indicates whether the file has integrity issues or not.

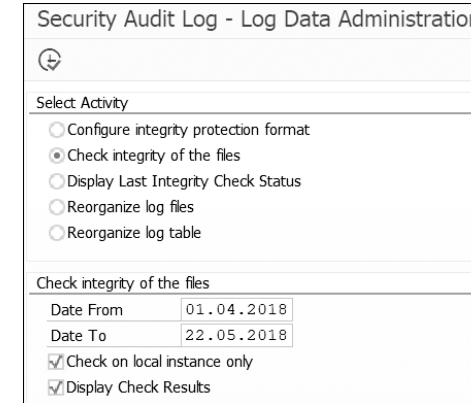


Figure 11.8 Check Integrity of Files

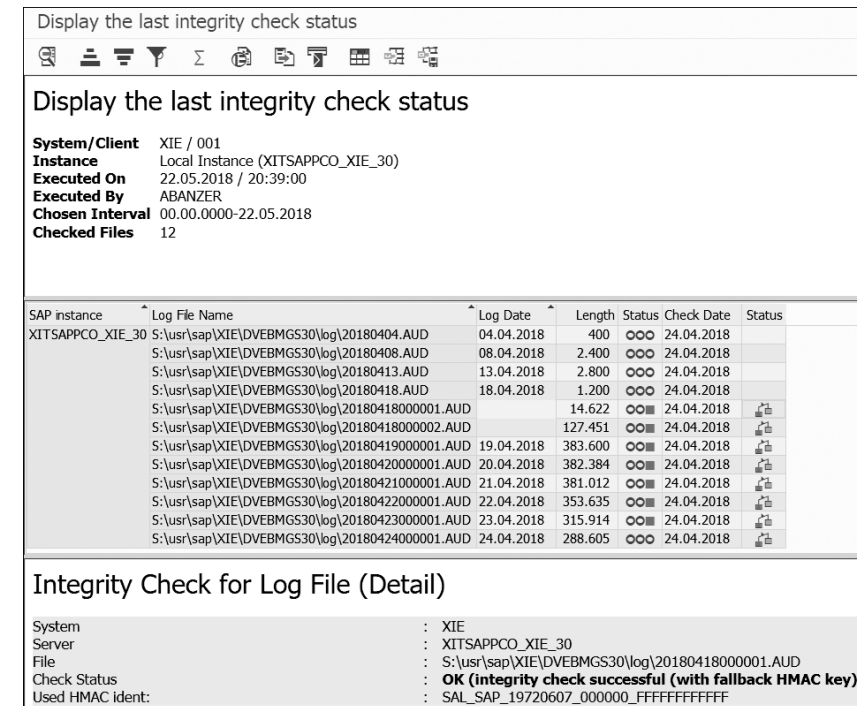


Figure 11.9 Display the Last Integrity Check Status

To quickly navigate back to the last integrity check, you can choose the **Display Last Integrity Check Status** option in the selection screen.

Reorganize Log Files

To reorganize log files by means of deleting the physical file from the file system, you can choose **Reorganize log files** from the initial screen (Figure 11.10). You can delete or display the data to be reorganized, as well as run a simulation mode first. The simulation mode lets you see what will happen if you deselect the checkbox.

Figure 11.10 Reorganize Log Files

The minimum age decides which files will be deleted. Once executed, you'll see a results screen (Figure 11.11) indicating which old files will be deleted (if run without simulation).

RFC Destination	Directory	File name	Length	Date
XITSAPPCO_XIE_30	S:\usr\sap\XIE\DVBMGS30\log	20150807.AUD	54.000	15.08.2015
	S:\usr\sap\XIE\DVBMGS30\log	20150818.AUD	3.600	19.08.2015
	S:\usr\sap\XIE\DVBMGS30\log	20151012.AUD	13.600	13.10.2015
	S:\usr\sap\XIE\DVBMGS30\log	20160407.AUD	4.800	19.04.2016
	S:\usr\sap\XIE\DVBMGS30\log	20160418.AUD	4.000	20.04.2016
	S:\usr\sap\XIE\DVBMGS30\log	20160419.AUD	800	

Figure 11.11 Delete Log Files

Remember, the deletion of log files should be carried out through this transaction because it performs an authorization check and follows the deletion process for files in the integrity protection format. Deleting files manually from the file system is considered a manipulation.

Reorganize Log Table

Reorganization of the database table is important when logging is activated to be stored exclusively in the database table. For all other scenarios, reorganization is not necessary; for example, APIs will delete the data after the transfer.

To delete data from the table, choose the **Reorganize log table** selection (Figure 11.12) and enter the date before which you want data to be deleted.

Figure 11.12 Reorganize Log Table in Database

Evaluation of Log Data

You can evaluate the log data in Transaction RSAU_READ_LOG (Figure 11.13). You can either evaluate the logs online in the foreground or send the report into the background. In the selection screen, you can set the time restrictions along with multiple other options.

Selection of Audit Events from the Audit Files (Background Variant)

Time Restrictions

From Date/Time: 22.05.2018 00:00:00
To Date/Time: 22.05.2018 23:59:59

Standard Selections

Selection Type: Dynamic selection (general selection)

Instance Name:

Client:

User:

Terminal:

Transaction Code:

Program:

Text in the Message:

Audit Classes

- Dialog Logon
- RFC/CPIC Logon
- RFC Function Call
- Transaction Start
- Report Start
- User Master Changes
- Other Events
- System Events

Events

Only Critical
 Severe and Critical
 All

Data source selection

Loading data from audit log files
Name of Audit Directory:
Name of Audit File:

Loading data from audit log table

Figure 11.13 Evaluate Log Data Initial Screen

In the **Standard Selections** (Figure 11.14), you can set the selection type and, for example, search based on a specific user, client, terminal, or audit class or based on the criticality of the event. Also, you can reuse your filters and search for specific filters only.

The **Instance Name** field lets you input the instance that you want to evaluate. If you have multiple application servers and want to only include the current application instance, you can use the value <LOCAL>.

Standard Selections

Selection Type: Selection by profile/filter
Profile/Filter: Selection by profile TEST2/filter 0003

Instance Name:

Client:

User:

Terminal:

Transaction Code:

Program:

Text in the Message:

Figure 11.14 Standard Selection in Evaluation of Log Data

In the **Data source selection** (Figure 11.15), you can define if you want to read all your files, a specific file or directory, or your database tables.

Data source selection

Loading data from audit log files
Name of Audit Directory:
Name of Audit File:

Loading data from audit log table

Figure 11.15 Data Source Selection in Evaluation of Log Data

The result screen shows the logged events in detail. For example, in Figure 11.16, you can see successful logons by user WF-BATCH.

Security Audit Log - Evaluation

Navigation: Evaluation | File List | Statistics | SAL Configuration

Evaluation of Security Audit Log

Period Requested 24.04.2018 00:00:00 - 22.05.2018 23:59:59
Period Selected 24.04.2018 00:00:16 - 03.05.2018 10:57:29
Server XITSAPPCO

Events Read

- Critical 0
- Severe 18.899
- Other 29

SAP System	AS Instance	Date	Time	Cl.	Message ID	User	Terminal	Peer	TCode	Program	Audit Log Msg. Text
XIE	XITSAPPCO_XIE_30	24.04.2018	00:00:16	001	AU1	WF-BATCH				RSBTCRTE	Logon successful (type=B, method=A)
XIE	XITSAPPCO_XIE_30	24.04.2018	00:00:17	001	AU1	WF-BATCH				RSBTCRTE	Logon successful (type=B, method=A)
XIE	XITSAPPCO_XIE_30	24.04.2018	00:02:48	001	AU1	WF-BATCH				RSBTCRTE	Logon successful (type=B, method=A)
XIE	XITSAPPCO_XIE_30	24.04.2018	00:02:58	001	AU1	WF-BATCH				RSBTCRTE	Logon successful (type=B, method=A)
XIE	XITSAPPCO_XIE_30	24.04.2018	00:02:58	001	AU1	WF-BATCH				RSBTCRTE	Logon successful (type=B, method=A)

Figure 11.16 Evaluation of Log Data Result Screen

Evaluate Archived Log Data

To evaluate archived log data, you can use Transaction RSAU_READ_ARC (Figure 11.17). In the selection screen, you can set the period, as well as other selections like the client, user, terminal, and so on.

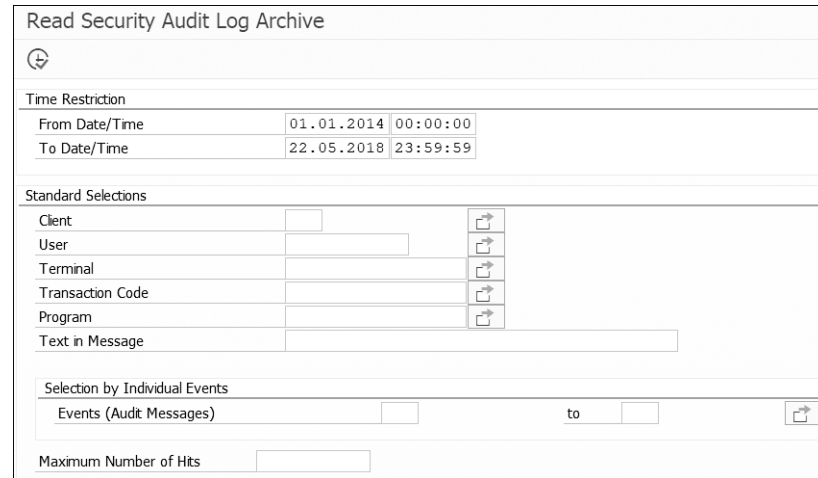


Figure 11.17 Read Security Audit Log Archive Data

11.3.2 System Log

Whereas the security audit log records security-related information about the system, the system log records information that may signal system problems. As an administrator, the system log is an important tool to maintain the healthiness of your system and keep the system up and running with good performance. The system log records warnings, error messages, database read errors, rollbacks, and so on.

The system log offers different types of logging depending on the host. On an UNIX host, you have local and central logging available. If you run on a Microsoft Windows NT host, you'll only have local logging. In the local scenario, the log is stored locally on the application server in a ring buffer. The ring buffer is overwritten once full. Therefore, the system log is only available for a certain time frame as the size is limited. In the central log, each individual application server sends its local log to a central server. Similar to the local log, the size of the central log is limited and hence it doesn't hold the information indefinitely.

In either scenario, we recommend analyzing the system log on a regular basis. Most administrators check the system log daily to avoid any disruption to the SAP system.

The local log is always up to date, whereas the central log might have a slight delay as the data must be written from the local application server to the central server.

The main transaction to analyze the system log is Transaction SM21 (Figure 11.18), in which you can read the system log and its messages. In the selection screen, you can define basic and extended attributes to get to the messages that are most important to you.

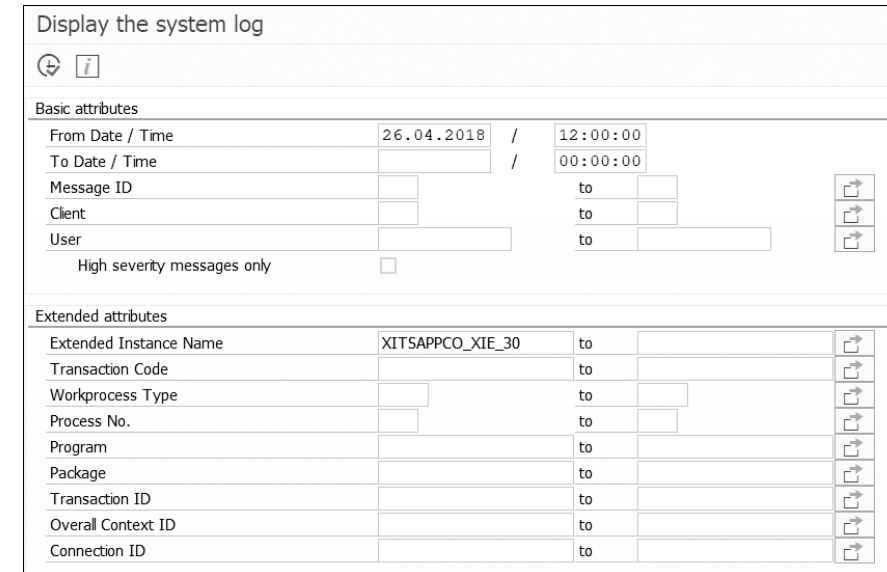


Figure 11.18 Initial Screen in Transaction SM21 to Display System Log

In the result screen (Figure 11.19), you get an overview of all messages that have been logged by the SAP system. For each entry, you see the time stamp, instance, client, user, and the priority of and information about the message. You can double-click any line item.

Syslog messages									
Syslog of instance XITSAPPCO_XIE_30									
Date	TIME	Instance	Type	Process No.	Cl.	User	Priority	Message ID	Message Text
01.04.2018	15:14:51	XITSAPPCO_XIE_30	WRK	000			Q00	Q00	Start Workp. 12, Pid 14276
01.04.2018	15:19:57	XITSAPPCO_XIE_30	DIA	012	000		Q02	Q02	Stop Workp. 12, PID 14276
01.04.2018	15:57:25	XITSAPPCO_XIE_30	DP	000			Q01	Q01	Operating system call recv failed (error no. 10054)
01.04.2018	15:57:30	XITSAPPCO_XIE_30	DP	000			Q04	Q04	Connection to user 6118 (ABANZER), terminal 65 (DESKTOP-1CFU) lost
01.04.2018	15:57:30	XITSAPPCO_XIE_30	DIA	003	001	ABANZER	R47	R47	Delete session T65_U6118_M0 after error Execution was canceled (Softcancel) [Warning/Session]
01.04.2018	15:57:54	XITSAPPCO_XIE_30	WRK	000			Q00	Q00	Start Workp. 15, Pid 13756
01.04.2018	16:02:57	XITSAPPCO_XIE_30	DIA	015	000		Q02	Q02	Stop Workp. 15, PID 13756

Figure 11.19 System Log Result Screen

After you double-click an item, you'll see to the details of the message (Figure 11.20) to dive further into the error. In addition to details about the message and the session, as well as technical and parameter details, you can also navigate to the trace from the menu bar.

Figure 11.20 System Log Detail View

In the trace, you can see all the steps that the system performed for the message that you selected. Analyzing traces requires a deep understanding of the SAP system and is definitely an expert-tool only.

11.3.3 Table Logging

To enable table logging in general, you have to activate the table logging in the profile parameter `rec/client`. Once activated, you can define tables to be logged in the table properties. The profile parameter `rec/client` knows four different values:

- **OFF**
Logging is deactivated.
- **nnn**
Logging takes place for client-specific tables only in the client listed (001, 100, etc.).
- **nnn,nnn,nnn**
Logging takes place for client-specific tables for the clients listed (a maximum of 10 clients possible, comma-separated).

- **ALL**
Logging always takes place; for client-specific tables, it takes place for all clients. *Caution:* This setting makes sense only in special cases. Note that in the case of ALL, changes are recorded in the log file for all test clients (including SAP client 000).

Once the table logging has been activated, you can define which tables will be logged. To activate logging for a particular table, you have to define the properties in the table itself. You can do that from Transaction SE13. SAP pre-delivers customizing tables with the table change logging activated.

For the example shown in Figure 11.21 for table RFCDES (RFC Destinations), the table change log is activated.

Figure 11.21 Log Data Changes in Technical Settings of Table in Transaction SE13

To check all tables that have the logging activated and to review the changes, you can use Transaction SCU3 (Figure 11.22). In Transaction SCU3, click **List of Logged Tables** to see an overview of all tables that have table change logging activated.

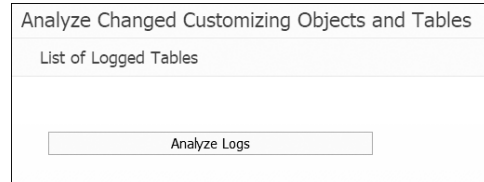


Figure 11.22 Initial Screen of Transaction SCU3

Warning

In an SAP NetWeaver 7.50 system with SAP ERP installed, SAP defined close to 30,000 tables with the table change log. Most of the tables are customizing tables and hence do not contain master data that changes regularly.

Analyze Logs

To analyze the changes that have been logged, you again can use Transaction SCU3. In Transaction SCU3, go to **Analyze Logs** and make your selections. In the selection screen (Figure 11.23), you must select one specific table or customizing object for analysis. This is enforced because the amount of data can be huge. For reporting purposes, we suggest using the ALV Grid Display, which lets you sort and filter the output.

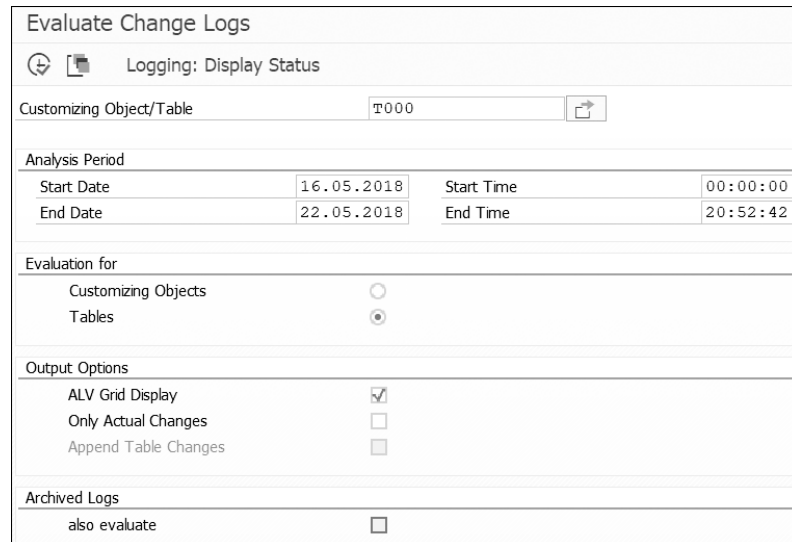


Figure 11.23 Evaluate Table Change Log in Transaction SCU3

In the output view, you can get the details of what’s been changed in the table. In Figure 11.24, you can see changes to table T000 (clients). You can see the type of change, as well as which transaction and program were used to perform the change.

Date	User Name	Time	TCode	Program	Type	Cl.	Name	City	Crcy	Role	CorrSys
01.02.2018	DKINDERMANN	09:13:54	SM30	SAPMSVMA	Created	200	SecArch Test	Schöffisdorf		T	1
		10:34:21	SM30	SAPMSVMA	Created	300	Earlywatch	Walldorf		T	1
		11:06:14	SM30	SAPMSVMA	Created	066	e	Walldorf		S	1
		11:06:20	SM30	SAPMSVMA	Old	066	e	Walldorf		S	1
			SM30	SAPMSVMA	new	066	Earlywatch	Walldorf		S	1
		13:27:04		RSLXCOP	Unchanged	200	SecArch Test	Schöffisdorf		T	1
	SAP*	09:17:40		RSLXCOP	Unchanged	200	SecArch Test	Schöffisdorf		T	1
		09:34:27	SM30	SAPMSVMA	Old	066	EarlyWatch	Walldorf	EUR	S	1

Figure 11.24 Display Table Change Logs

The data being analyzed in Transaction SCU3 is stored in table DBTABLOG. Transaction SCU3 offers a fully functional cockpit to analyze the data efficiently.

SAP Note 1916

For more information about table logging, see SAP Note 1916 (Logging of Table Changes in R/3).

Performance Impact

Table change logging shouldn’t have a performance impact if you only log customizing tables. Although SAP delivers many tables with table logging activated, those tables usually contain little data that rarely changes. Avoid logging for master data and transaction data tables because those tables are subject to mass changes and hence would have a negative impact on the system performance. For custom tables, you can define whether you want to activate table logging or not.

If you experience negative performance after activating table logging, you can find out which tables log the most amount of data. In Transaction SCU3, you can validate the table logging via the menu path **Administration • Number of Logs (Selection)**. In the selection screen (Figure 11.25), leave the **Table Name** field empty and analyze the last month (or extend the time if required).

Number of Table Change Logs (System-Wide)

Table Name to

Starting Point

End

Hide Table Without Logs

Figure 11.25 Number of Table Change Logs in Transaction SCU3

In the results screen, you can see the number of entries per table logged. For the example in Figure 11.25, table RFCDES logged 36 changes in the last 30 days, as shown in Figure 11.26. You can sort the number of logs in descending order to quickly get an indication of which tables might cause a performance issue.

Table Name	Short Description	No. of Logs
<input type="checkbox"/> RFCDES	Destination table for Remote Function Call	36
<input type="checkbox"/> RFCDOC	Description of Possible RFC Connections (->RFCDES)	24
<input type="checkbox"/> RSADMIN	Data import administration settings	3
<input type="checkbox"/> RSADMINC	Customizing Table General BW	4
<input type="checkbox"/> RSAUPROF	Audit: Audit configuration parameters (audit profile)	87
<input type="checkbox"/> RSAUPROFEX	SAL: Extended Audit Configuration Parameters (Audit Profile)	13
<input type="checkbox"/> RSDATRNAVT	Navigation Attributes	136
<input type="checkbox"/> SACF_ALERT	Collector for Failed Calls	31
<input type="checkbox"/> SFOBUEV000	FoBuEv: Header Data of a Formula	335
<input type="checkbox"/> SFOBUEV001	FoBuEv: Rows (Token) of a Formula	1.780
<input type="checkbox"/> SSF_PSE_H	SSF: Personal Security Environment	2
<input type="checkbox"/> SWD_EXPR	WF Definition: Expressions	411
<input type="checkbox"/> SWD_HEADER	WF Definition/Runtime: Basic Data	15
<input type="checkbox"/> T77ARRAYTP	Column Framework: Definition of Column Groups	2
<input type="checkbox"/> T77ARRAYTT	Text Table for t77arraytp	2
<input type="checkbox"/> TADIR	Directory of Repository Objects	1.284
<input type="checkbox"/> TBDLS	Logical system	1
<input type="checkbox"/> TBDLST	Text for logical system	2
<input type="checkbox"/> TDDAT	Maintenance Areas for Tables	809

Figure 11.26 Result Screen of Number of Table Change Logs

Table logging shouldn't have an impact on your overall system performance and hence is a helpful feature to ensure the traceability of changes to customizing and other important tables in your SAP system.

11.3.4 Workload Monitor

The Workload Monitor lets you analyze system statistics in the SAP system. You can report on different task types like background processing, dialog processing, update processing, ALE, RFC, and so on. You will also see detailed information on CPU time, number of changes to the database, number of users that use the system, and so on. You can start the Workload Monitor in Transaction STO3N.

Apart from all the analysis capabilities to check the workload of your system, the Transaction STO3N trace contains information that might be helpful for auditing purposes. In Transaction STO3N, you can analyze the activity of a user and reproduce the actions a user has executed in the system. In the user profile, you can see all the users in a certain time frame and details of the actions they performed. In Figure 11.27, you can see that user ABANZER executed several transactions (e.g., Transactions RSAU_ADMIN, RSAU_READ_LOG, and so on). You can also see how many dialog steps were executed along with the details of average response times.

Workload in System XIE

Instance: TOTAL | First record: 22.05.2018 00:00:01 | Last record: 22.05.2018 19:59:59 | Time period: 0 Day(s) 19:59:59

Task type: DIALOG

Task type: Single Records

User Profile: Times; T Total Time (s), Ø Time/Step (ms)

User	# Steps	T Response Time	Ø Time	T CPU~	Ø CPU~	T DB Time	Ø DB Time	T Time	Ø Time	Ø WaitTime	# Trps	Ø Time	Ø GUI Time	KB
ABANZER	428	1.464	3.420,9	975	2.279,1	413	965,3	0,0	0,0	0,0	924	350,4	363,4	3.063.824
EPERALTA	224	304	1.358,5	114	509,8	45	200,2	0,0	0,0	0,1	687	348,6	537,9	224.271

Instances Utilized by User ABANZER

ABAP Instance	# Steps	T Response Time	Ø Time	T CPU~	Ø CPU~	T DB Time	Ø DB Time	T Time	Ø Time	Ø WaitTime	# Trps	Ø Time	Ø GUI Time
PF04	258	90	349,8	8	30,3	12	48,4	0,0	0,0	0,0	512	344,4	272,0
SU24	33	42	1.276,9	5	157,7	4	116,2	0,0	0,0	0,0	131	281,7	1.009,9
SU25	33	1.205	36.529,7	942	28.549,7	319	9.669,5	0,0	0,0	0,1	83	369,5	592,3
SUPC	31	88	2.847,6	17	559,0	63	2.029,4	0,0	0,0	0,0	66	334,3	435,9
RSABAPPROGRAM	25	13	532,0	1	31,2	5	202,3	0,0	0,0	0,0	49	346,8	287,8
PF04MASSVAL	16	6	374,4	1	82,1	2	112,5	0,0	0,0	0,1	21	458,4	175,6
SE93	13	6	485,1	0	22,8	4	299,5	0,0	0,0	0,0	18	448,0	97,8
SU1M	10	5	467,9	0	25,0	1	101,5	0,0	0,0	0,0	20	313,5	342,0
ROLE_CMP	4	5	1.149,8	0	27,3	1	340,8	0,0	0,0	0,0	16	296,0	764,5
SESSION_MANAGER	3	2	666,0	0	52,0	1	213,3	0,0	0,0	0,0	6	810,7	401,0
PFUD	2	1	558,0	0	31,5	1	521,0	0,0	0,0	0,0	2	339,0	0,0

Figure 11.27 Workload Monitor for Specific User Profile in Transaction STO3N

The workload is deactivated by default as it increases the chances for performance implications. Therefore, we recommend activating it temporarily for specific analysis. Before activation, make sure that you adhere to the laws and regulations in your territory.

Warning

Analyzing user activities may not be permitted based on your area of operation. Also, personal data protection regulations like GDPR may prohibit the use of such information.

11.3.5 Read Access Logging

Read access logging (RAL) is a tool to monitor and record the read access to sensitive and classified data in your SAP system. The type of data that you want to monitor can be categorized as sensitive by law or by internal or external company policies. In the context of the GDPR, companies must comply with the regulations and adhere to standards about data privacy.

With the RAL framework, you can comply with the regulations because you always know who accessed which data from where and when. Also, in case of a security breach or a leak of information, you can report not only who had access to the data from an authorization standpoint but also who accessed the data through the logging.

The RAL framework works with different types of channels when a user is accessing the data. *Channels* are the way the data leaves or enters the system (e.g., through SAP GUI). On the UI side, the RAL framework works with Dynpro (logging of Dynpro UI elements and ALV grids) and Web Dynpro (logging of context-bound UI elements).

It also works with APIs such as the following:

- **Remote Function Calls (sRFC, aRFC, tRFC, qRFC, bgRFC)**
Logging of server- and client-side RFC-based communication
- **Web services**
Logging of consumer- and provider-side web service communications
- **OData channels**
Logging of data consumed by SAP Fiori applications through OData services

Further Information

For more information about the OData channels for SAP Fiori applications, you can check SAP Note 2182094 (Read Access Logging in SAP Gateway).

The configuration and monitoring of the RAL is done in Transaction SRALMANAGER (Figure 11.28).

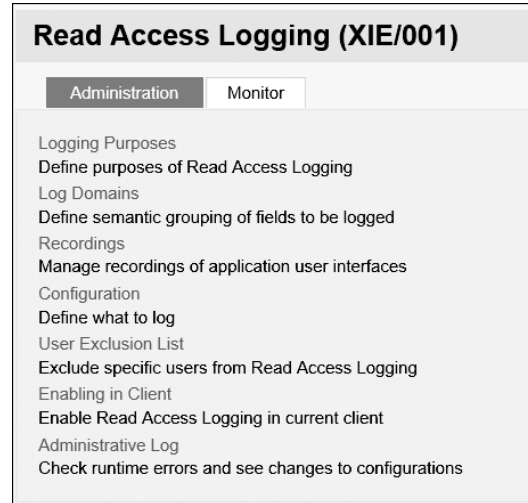


Figure 11.28 Read Access Logging Initial Screen

The configuration of RAL requires five steps, which are represented in the Web Dynpro application that starts with Transaction SRALMANAGER:

1. You have to identify and determine under what circumstances the RAL will log what type of data. For example, in view of GDPR, you have to protect personal information of your employees. Therefore, you have to monitor and protect transactions and tables that contain personal information, like Transaction SU01 (User Master Records), table USR02 (User Master Records), and so on.
2. In the second step, you have to define the purpose of the logging, which allows you to group certain requirements. You can freely define a name for the logging purpose. The logging purpose is used to organize the data in the context of a specific use case, such as for GDPR.
3. In the third step, you have to define the channels that you want to monitor. Common channels are Web Dynpro, RFCs, and so on.
4. Once you have the channels defined, you define the log domains. The log domains group semantically similar or related fields. For example, in the Basis area, an “account” is different than the “account” in the banking application. Therefore, you want to classify similar content into log domains.
5. Finally, you define the conditions that must be met for the application to log the data—for example, which fields are being recorded and whether the access is recorded only or the content of the data is recorded as well.

For simplified operation of the RAL, you can define an exclusion list of users that won't be logged. A common scenario is to exclude batch job users that perform multiple reads, which would lead to a significant number of logs.

Once the configuration has been activated successfully, you can start to monitor the log entries in the Web Dynpro application. To review the logs, you can go to **Read Access Log** in the **Monitor** tab. You can search channel-specific, date-specific, or user name-specific logs.

11.3.6 User Information System

The User Information System is one of the main tools required for both internal and external audits. This tool is a directory for several programs that facilitate the retrieval of information required for an audit. Most of the tools focus on users and authorizations. However, the AIS also contains a powerful change document feature. Each function is organized by its type in the menu tree and can be launched by double-clicking the **Execute** button to the left of the function name.

As an example, let's look up users with critical authorization combinations. This is a common report used by auditors to satisfy audit controls. Proceed as follows:

1. Navigate to Transaction SUIM.

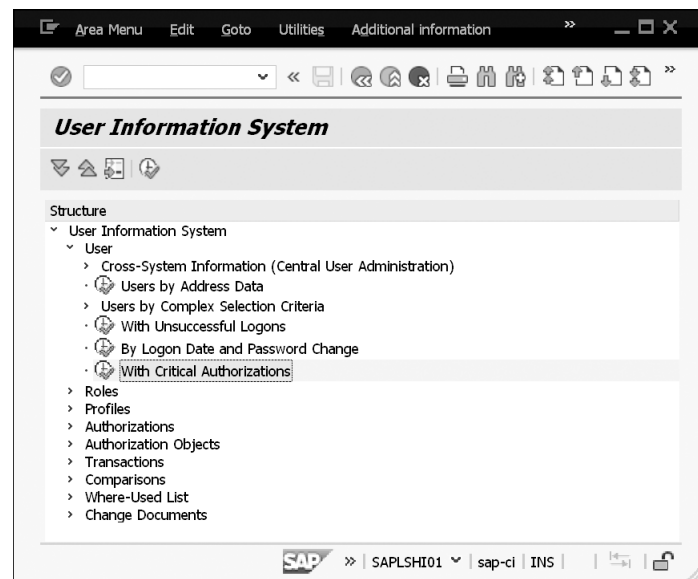


Figure 11.29 Transaction SUIM Main Screen

2. In the menu, click the **User** drop-down, then select **With Critical Authorizations** and click the **Execute** icon (Figure 11.29).

Direct Access

Alternatively, you can run report RSUSR008_009_NEW in Transaction SA38.

3. Next, choose the **For Critical Authorizations** radio button in the **Variant Name** box. For the variant name, choose the predelivered SAP_RSUSR009 variant (Figure 11.30).

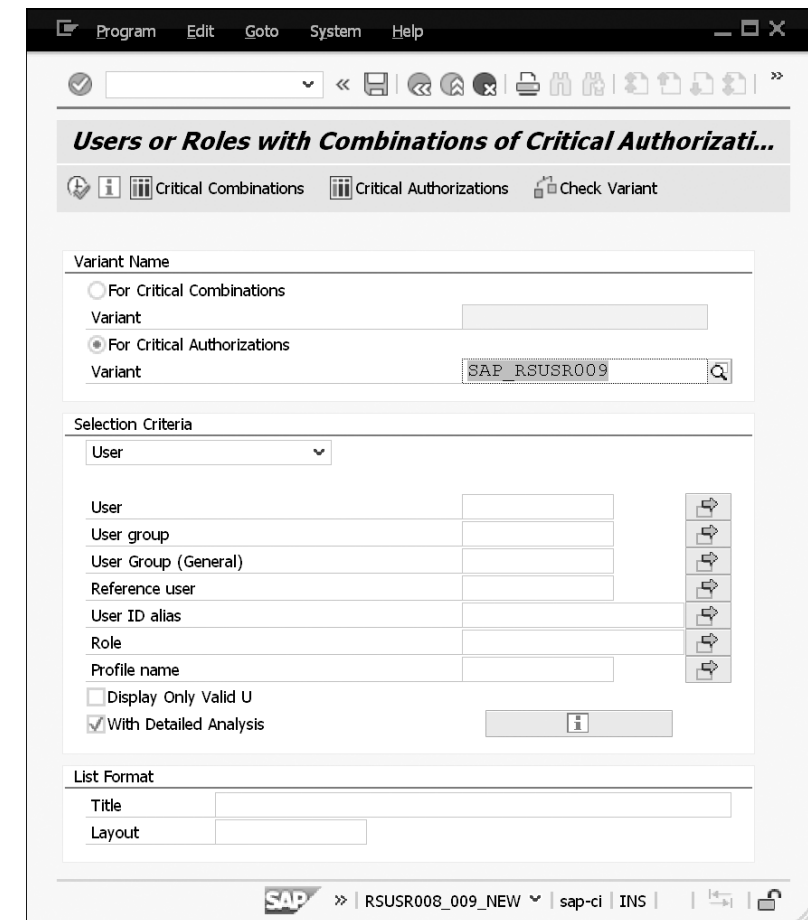


Figure 11.30 Critical Authorizations Selection Screen

Define Your Own Critical Authorizations

You can also define a list of critical authorizations. You may receive a list of critical authorizations or transaction codes from your internal auditor, external auditor, or functional business analysts. You may need to come up with this list on your own. A good starting point is to use the SAP delivered variant, SAP_RSUSR009, but be sure to adjust it for your auditing use.

4. Click the **Execute** button.

The screenshot shows the SAP report interface for 'Users or Roles with Combinations of Critical Authorizations'. The report title is 'Users or Roles with Combinations of Critical Authorizations'. Below the title, it indicates 'Number of Hits for Critical Authorizations: 105'. The system information shows 'System JDM Client 001 Checked by I851675 14.05.2018 17:11:41'. The selection criteria are listed as follows:

ID of CA	Text of Critical Authorization (CA)	User	Long name	Group	Valid from	Valid to	Account	no User
SAP_ABAA	Administration: All Rights for Background Jobs	DDIC		SUPER				A Di
		I851675	Markgraf Joe	SUPER				A Di
		P000001	P000001	SUPER				A Di
		SAP*		SUPER				A Di
		SSOTEST	Markgraf Joe	SUPER				A Di
SAP_ABJA	Administration: Release Background Jobs	DDIC		SUPER				A Di
		I851675	Markgraf Joe	SUPER				A Di
		P000001	P000001	SUPER				A Di
		SAP*		SUPER				A Di
		SSOTEST	Markgraf Joe	SUPER				A Di
SAP_ABNA	Administration: Start Background Jobs with Any User	DDIC		SUPER				A Di
		I851675	Markgraf Joe	SUPER				A Di
		P000001	P000001	SUPER				A Di
		SAP*		SUPER				A Di
		SSOTEST	Markgraf Joe	SUPER				A Di
SAP_ABNN	Use Background Jobs	DDIC		SUPER				A Di
		I851675	Markgraf Joe	SUPER				A Di
		P000001	P000001	SUPER				A Di
		SAP*		SUPER				A Di
		SSOTEST	Markgraf Joe	SUPER				A Di
SAP_ADMI	Administration: Network, Processes, Update Admin., and so on	DDIC		SUPER				A Di
		I851675	Markgraf Joe	SUPER				A Di
		P000001	P000001	SUPER				A Di
		SAP*		SUPER				A Di
		SSOTEST	Markgraf Joe	SUPER				A Di
SAP_ALOC	Execute Logical Operations System Commands	DDIC		SUPER				A Di

Figure 11.31 Report Generated with Critical Authorizations

The system will return a list of critical authorizations (Figure 11.31) that each user has in your system. If you have many super users, or administrators, this list could be in the thousands or tens of thousands. A review of this list and its users is done often, with the appropriateness of each user’s access reviewed by either internal or external auditors.

11.4 Summary

In this chapter, you learned about internal and external audits and their purpose in an organization. You learned about auditing tools like security audit logging, the system log, table logging, the Workload Monitor, and Read Access Logging. Finally, you learned about the User Information System and how to use it to find users with critical authorizations.

In the next chapter, you’ll learn about how to secure network communications to and from your SAP NetWeaver AS ABAP system. This is an important subject for a security administrator because most attacks against an SAP system use the network as an attack vector.

Contents

Preface	19
1 Introduction	25
1.1 Potential Threats	26
1.1.1 Data Breach	27
1.1.2 Privacy Violations	27
1.1.3 Phishing	27
1.1.4 Theft	28
1.1.5 Fraud	28
1.1.6 Brute Force Attacks	29
1.1.7 Disruption	29
1.1.8 Who Represents a Threat?	30
1.1.9 Understanding Modern-Day Vulnerabilities	31
1.2 The Onion Concept	34
1.2.1 Perimeter	35
1.2.2 Operations	35
1.2.3 Patching	35
1.2.4 Human Factor	36
1.2.5 Physical Security	36
1.2.6 Security Awareness	36
1.3 Risk and True Cost of Security	37
1.4 The Administrator's Role in Security	40
1.4.1 Planning	40
1.4.2 Execution	41
1.4.3 Segregation of Duties	42
1.4.4 Audit Support	42
1.4.5 Basis versus Security	43
1.5 Summary	43

2	Configuring Profiles and Parameters	45
2.1	Understanding System Parameters	46
2.2	System Profiles	47
2.2.1	Instance Profile	47
2.2.2	Default Profile	48
2.2.3	Other Profiles	49
2.3	Profile and Parameter Structure	49
2.3.1	Profiles on the Operating System Level	51
2.3.2	Profiles on the Database Level	52
2.4	Static and Dynamic Parameters	53
2.5	Viewing and Setting Parameters	55
2.5.1	Viewing Parameters with ABAP Report RSPARAM	56
2.5.2	Viewing the Documentation with Transaction RZ11	58
2.5.3	Changing Parameters with Transaction RZ10	59
2.6	Key Security-Related Parameters	64
2.7	Controlling Access to Change Parameters	66
2.8	Summary	67
3	Restricting Transactional Access	69
3.1	Clients	71
3.2	Who Should Be Able to Lock and Unlock Transactions?	71
3.3	Which Transactions to Lock	71
3.4	Locking Transactions	73
3.5	Viewing Locked Transactions	76
3.6	Summary	78

4	Securing Clients	79
4.1	Client Settings	81
4.1.1	Client Setting Fields	83
4.1.2	Suggested Client Settings	85
4.1.3	Changing Client Settings	87
4.2	Client Logon Locking	89
4.3	Summary	92
5	Securing the Kernel	93
5.1	Understanding the Kernel	94
5.1.1	Kernel Patching	96
5.1.2	Kernel Versioning	97
5.1.3	Checking the Kernel Version	100
5.1.4	Checking the Kernel Version from the Operating System Level	101
5.2	Common Cryptographic Library	102
5.2.1	Checking the CommonCryptoLib in SAP GUI	102
5.2.2	Checking the CommonCryptoLib on the OS Level	103
5.3	Kernel Update	104
5.3.1	Overall Kernel Update Process	105
5.3.2	Downloading the Kernel	107
5.3.3	Installing the Kernel	110
5.4	Summary	114
6	Managing Users	115
6.1	What Is a User ID in SAP?	115
6.2	Different User Types	115
6.2.1	Dialog User: Type A	116
6.2.2	System User: Type B	116
6.2.3	Service User: Type S	117

6.2.4	Communication User: Type C	117
6.2.5	Reference User: Type L	117
6.3	The User Buffer	117
6.4	Creating and Maintaining a User	118
6.4.1	Documentation	119
6.4.2	Address	120
6.4.3	Logon Data	121
6.4.4	Secure Network Communication	122
6.4.5	Defaults	123
6.4.6	Parameters	124
6.4.7	Roles	125
6.4.8	Profiles	125
6.4.9	Groups	126
6.4.10	Personalization	126
6.4.11	License Data	127
6.4.12	DBMS	127
6.5	Copy a User	128
6.6	Change Documents for Users	129
6.7	Mass User Changes with Transaction SU10	131
6.8	User Naming Convention	139
6.9	Security Policies	140
6.10	Maintain User Groups	145
6.11	Central User Administration	147
6.11.1	Distribution Parameters for Fields (Transaction SCUM)	149
6.11.2	Background Jobs	150
6.11.3	CUA-Related Tables	151
6.12	User Lock Status	151
6.13	User Classification	152
6.14	User-Related Tables	153
6.15	Securing Default Accounts	154
6.16	User Access Reviews	156
6.17	Inactive Users	157

6.18	Password and Logon Security	158
6.18.1	Where Does SAP Store Passwords?	158
6.18.2	What Is the Code Version?	159
6.18.3	Why Do I Have to Protect These Tables?	159
6.18.4	Logon Procedure	160
6.18.5	Password Change Policy	161
6.19	Segregation of Duties	163
6.20	Summary	165
7	Configuring Authorizations	167
7.1	Authorization Fundamentals	168
7.1.1	What is a Role?	168
7.1.2	What is a Profile?	168
7.1.3	Authorization Objects	169
7.1.4	The Profile Generator	169
7.1.5	Authorization Checks	169
7.1.6	Display Authorization Data	171
7.1.7	The User Buffer	173
7.1.8	Maintain Check Indicators: Transaction SU24	173
7.1.9	System Trace	175
7.2	SAP Role Design Concepts	180
7.2.1	Single Roles	181
7.2.2	Derived Roles	181
7.2.3	Composite Roles	182
7.2.4	Enabler Roles	182
7.2.5	Comparison of the Role Design Concepts	183
7.2.6	Why Not Use Enabler Roles?	184
7.2.7	What Impact Does a System Upgrade Have on Roles and Authorizations?	188
7.2.8	Role-Naming Conventions	188
7.3	The Profile Generator	192
7.3.1	Create a Single Role	192
7.3.2	Create a Composite Role	204

7.3.3	Create a Master and Derived Role	207
7.3.4	Overview Status	213
7.3.5	Mass Generation of Profiles	214
7.3.6	Mass Comparison	215
7.3.7	Role Menu Comparison	216
7.3.8	Role Versioning	217
7.4	Assign and Remove Roles	219
7.5	Lock and Unlock Transactions	221
7.6	Transaction SUIM: User Information System	221
7.6.1	User	222
7.6.2	Roles	223
7.6.3	Profiles	223
7.6.4	Authorizations	223
7.6.5	Authorization Objects	224
7.6.6	Transactions	224
7.6.7	Comparisons	224
7.6.8	Where-Used Lists	225
7.6.9	Change Documents	225
7.7	Role Transport	226
7.8	Common Standard Profiles	228
7.9	Types of Transactions	229
7.9.1	Dialog Transactions	230
7.9.2	Report Transactions	230
7.9.3	Object-Oriented Transactions	231
7.9.4	Variant Transactions	231
7.9.5	Parameter Transaction	234
7.9.6	Call Transaction in Transaction SE97	237
7.10	Table Authorizations	239
7.10.1	Table Group Authorizations via S_TABU_DIS	240
7.10.2	Table Authorizations via S_TABU_NAM	241
7.10.3	Cross-Client Table Authorizations via S_TABU_CLI	241
7.10.4	Line-Oriented Table Authorizations via S_TABU_LIN	241
7.10.5	Table Authorizations and Auditors	245
7.10.6	Table Views for Database Tables	245
7.11	Printer Authorizations	249

7.12	Other Important Authorization Objects	249
7.12.1	Upload and Download Authorizations	249
7.12.2	Report Authorizations	250
7.12.3	Background Jobs	251
7.12.4	ABAP Workbench	251
7.12.5	Batch Sessions	251
7.12.6	Query Authorizations	251
7.12.7	Remote Function Call Authorizations	252
7.13	Transaction SACF: Switchable Authorizations	253
7.14	Customizing Entries in Tables PRGN_CUST and SSM_CUST	255
7.15	Mass Maintenance of Values within Roles	257
7.16	Upgrading to a New Release	260
7.17	ABAP Debugger	267
7.18	Authorization Redesign and Cleanup	269
7.18.1	Business Impact of Security Redesign	270
7.18.2	Reducing the Business Impact of a Role Redesign Project	270
7.18.3	Gathering Authorization Data	271
7.18.4	Testing Role Changes in Production	272
7.18.5	Automate Role Creation and Testing	273
7.19	Introduction to SAP GRC Access Control	273
7.19.1	Access Risk Analysis	273
7.19.2	Access Request Management	274
7.19.3	Business Role Management	274
7.19.4	Emergency Access Management	275
7.19.5	Segregation of Duties Management Process	275
7.20	Summary	277
8	Authentication	279
8.1	What Is Single Sign-On?	279
8.1.1	Common Components of SSO	281
8.1.2	Establishing a Plan for SSO Adoption	283
8.2	Single Sign-On Technologies	284

8.2.1	X.509 Digital Certificates	284
8.2.2	Kerberos	285
8.2.3	SPNEGO	285
8.2.4	SAP Logon Tickets	285
8.2.5	SAML	286
8.3	SAP GUI Single Sign-On Setup	286
8.3.1	Setting up Secure Network Communications in Transaction SCNWIZARD	287
8.3.2	Setting Up Kerberos Single Sign-on with SAP GUI	296
8.4	SAML	309
8.4.1	Principals	310
8.4.2	Identity Providers	310
8.4.3	Service Providers	310
8.4.4	SAML Assertions	311
8.4.5	Overall SAML Process	311
8.4.6	SAP NetWeaver AS ABAP Service Provider Setup	312
8.4.7	ICF Service Authentication and SAP Fiori	338
8.5	Summary	339
9	Patching	341
9.1	Patching Concepts: SAP's Approach to Patching	341
9.1.1	SAP Notes	342
9.1.2	SAP Note Severity	343
9.1.3	Other Patching	344
9.1.4	SAP Security Patch Day	344
9.2	Application of Security SAP Notes	347
9.3	Implications of Upgrades and Support Packages	354
9.4	Evaluating Security with SAP Solution Manager	354
9.4.1	SAP EarlyWatch Alert Reporting	355
9.4.2	System Recommendations	356
9.4.3	Other Functionality	357
9.5	Summary	358

10	Securing Transports	359
10.1	Transport System Concepts	360
10.1.1	Operating System-Level Components	361
10.1.2	Controlling System Changes: Setting System/ Client Change Options	363
10.1.3	Transport Management System Users	367
10.1.4	TMS RFC connections	370
10.2	Transport Authorizations	373
10.3	Operating System-Level Considerations	376
10.4	Landscape Considerations	377
10.5	Summary	378
11	Auditing and Logging	379
11.1	External Audits	380
11.2	Internal Audits	381
11.3	Auditing Tools	382
11.3.1	Security Audit Log	382
11.3.2	System Log	396
11.3.3	Table Logging	398
11.3.4	Workload Monitor	403
11.3.5	Read Access Logging	404
11.3.6	User Information System	406
11.4	Summary	409
12	Securing Network Communications	411
12.1	Choosing a Network Security Strategy	411
12.2	Securing Using Access Controls	412
12.2.1	Firewalls	412

12.2.2	Application-Level Gateways	414
12.2.3	Business Secure Cell	415
12.2.4	Securing Common Ports	416
12.2.5	Securing Services	417
12.2.6	Access Control Lists	418
12.2.7	Tuning Network Access Control	422
12.3	Securing the Transport Layer	422
12.4	Connecting to the Internet and Other Networks	424
12.5	Summary	431
13	Configuring Encryption	433
<hr/>		
13.1	Introduction to Cryptography	433
13.1.1	Encryption in Depth	434
13.1.2	Secure Communication in SAP NetWeaver	448
13.2	Enabling SSL/TLS	451
13.2.1	Setting System Parameters	451
13.2.2	Creating the TLS/SSL PSE	454
13.2.3	Testing TLS/SSL	460
13.2.4	Requesting and Installing Certificates	464
13.3	The Internet Connection Manager	468
13.3.1	ICM Concepts	468
13.3.2	Important ICM Security Parameters	469
13.3.3	Controlling Access Using Access Control List	469
13.3.4	Security Log	473
13.3.5	Controlling Access Using a Permission File	475
13.4	SAP Web Dispatcher	481
13.4.1	Initial Configuration of SAP Web Dispatcher	483
13.4.2	SSL with SAP Web Dispatcher	486
13.5	Summary	487

14	Database Security	489
<hr/>		
14.1	Platform-Independent Database Considerations	490
14.1.1	Database Patching	490
14.1.2	Networking	491
14.1.3	User Accounts	492
14.1.4	Database Backups	493
14.1.5	Additional DB Functionality	494
14.2	Securing the Database Connection	495
14.2.1	Understanding the Database Connect Sequence	495
14.2.2	SAP HANA Database: HDB User Store	498
14.2.3	Oracle Database: Secure Storage in File System	500
14.2.4	Microsoft SQL Server: Authentication	504
14.3	Logging and Encrypting Your Database	507
14.3.1	SAP HANA Data Volume Encryption	508
14.3.2	Oracle Transparent Data Encryption	511
14.3.3	MSSQL Server	511
14.4	Summary	511
15	Infrastructure Security	513
<hr/>		
15.1	Business Secure Cell Concept	514
15.2	Secure Landscape	515
15.3	Policy	519
15.3.1	Establishing Security Policy	521
15.3.2	Starting Points for Your Policy	523
15.3.3	Further Policies	525
15.3.4	Adopting Policy	525
15.3.5	Auditing and Reviewing Policy	526
15.4	Operating System Considerations	527
15.4.1	General Linux Recommendations	528
15.4.2	Microsoft Windows	530
15.4.3	Operating System Users	531

15.4.4	Viruses and Malware	531
15.4.5	Application Server File System	539
15.5	Monitoring	540
15.5.1	OS Logs	540
15.5.2	Application Logs	540
15.5.3	Certificate Revocation Lists	541
15.6	Virtualization Security Considerations	553
15.7	Network Security Considerations	555
15.7.1	Auditing Using Vulnerability Scanners	556
15.7.2	Network Intrusion Detection	558
15.7.3	Firewall	559
15.7.4	Load Balancing	559
15.8	Physical Security	560
15.9	Summary	561
The Authors		563
Index		565

Index

2FA	280	Authorization (Cont.)	
		<i>redesign</i>	269
		<i>trace</i>	180
		Authorization checks	169
		<i>exceptions</i>	171
		<i>maintain</i>	173
		<i>TSTCA check</i>	169
		Authorization object	169
		<i>maintenance</i>	197
		<i>status</i>	198
		Authorizations	71, 115, 167
<hr/>			
A			
<hr/>			
ABAP debugger	267		
ABAP Program Editor	70		
ABAP support packages	99		
ABAP system identifier	300		
ABAP Workbench	251		
Access control	433, 523		
Access Control List (ACL)	411, 469		
Access Request Management	274		
ACL	376, 418, 473		
<i>file syntax</i>	419		
<i>syntax</i>	419		
<i>trace files</i>	422		
Active Directory Domain Services	297		
Adversaries	30		
ALG logs	422		
ALV Grid Display	400		
ALV list	130		
Application logs	540		
Application-level gateways	414		
Application-level proxies	414		
ASCS profile	49		
Assertions	282		
Asymmetric communication	442		
Asymmetric encryption	439, 442		
Attack surface	26, 41, 489		
Attack vector	41, 513		
Audit logs	540		
Audit regulations	522		
Auditing	379, 524		
Audits	42		
Authentication	523		
Authentication servers	282		
authfile	477		
Authorization			
<i>cleanup</i>	269		
<i>data</i>	171, 271		
<i>download</i>	249		
<i>profiles</i>	115, 125		
		Background jobs	251
		Basis	43
		Basis administrator	21
		Botnets	29
		BR*Tools	502
		Brute force attack	29, 159
		Business Process Change Analyzer	357
		Business Role Management	274
		Business secure cell	415, 514
<hr/>			
B			
<hr/>			
C			
<hr/>			
		CA	445
		Call transaction	237
		CA-signed certificates	371
		Central User Administration (CUA)	147, 275
		Certificate Authority	444
		Certificate revocation list	541
		Certificate signing request	290, 429
		Certificates	282
		<i>block</i>	551
		Change documents	129
		Change management	524
		Change Request Management	
		(ChaRM)	357, 519
		Channels	404
		ChaRM	357, 519
		Child role	207

Cipher	435	CVSS	345
<i>recommendation</i>	453	<i>score</i>	346
Cipher suite	436		
ClamAV scanner	532	D	
Client settings	81		
<i>changing</i>	87	Data breach	27
<i>check</i>	81	Data security	523
<i>fields</i>	83	Database	489
<i>locking</i>	89	<i>backup</i>	493
<i>restrictions</i>	85	<i>client</i>	491
<i>transport request</i>	89	<i>data manipulation</i>	492
Client-dependent	80	<i>default password</i>	492
Client-independent	80	<i>hardening</i>	490
Clients	79	<i>management consoles</i>	494
000	80, 85	<i>network</i>	491
001	80	<i>password</i>	500
066	80	<i>patching</i>	490
<i>locking</i>	89	<i>user</i>	127
<i>remote locking</i>	89	<i>user accounts</i>	492
<i>settings</i>	81	Database encryption	507
<i>table T000</i>	80	MSSQL	511
Clock skew tolerance	317	Oracle	511
CN	429	SAP HANA	508
Common Cryptographic Library	95, 434	Database table, reorganize	393
Common name	443	DDIC	155
Common Vulnerability Scoring System	344	DDIC user	367
CommonCryptoLib	95, 102, 286, 354, 434, 449	DDoS	29
<i>upgrading</i>	103	Default users	154
<i>versions</i>	102	Demilitarized zone	414
Communications security	523	Derived role	181, 207
Composite role	182, 204	Dialog transactions	229
Configuration validation	357	Dialog user	116, 139
Corporate espionage	489	Digital certificate	443
Cost of security	37	<i>public key</i>	444
CPIC	117	<i>signature</i>	444
CRL	542	Disaster recovery	517
<i>checks</i>	552	Disruption	490
<i>expirations</i>	548	Distinguished name	444
Cryptography	433	Distributed denial of service	29
CSR	290, 429	Distribution parameters	149
SAP Single Sign-On	291	DMZ	414
CUA	147	Domain controller	360
<i>background jobs</i>	150	DW package	94, 98
<i>master system</i>	149	DW.SAR	94, 98, 105
<i>tables</i>	151	Dynamic parameters	54

E		I	
Educating	525	IBM Tivoli Endpoint Manager	527
Emergency Access Management	275	ICF service authentication	338
Enabler role	182	ICM	418, 468, 473, 494
Encryption	411, 433	<i>permissions file syntax</i>	476
<i>asymmetric</i>	439	<i>security parameters</i>	469
<i>inverse relationship</i>	439	<i>service</i>	339
<i>key pairs</i>	439	<i>Web Administration Interface</i>	469
<i>protocols</i>	446	icmon	477
<i>symmetric</i>	437	IDocs	150
Encryption keys	436	IFRS	380
<i>private</i>	437	Infrastructure security	513
Enhancement packages	342	Integrity protection	390
Enqueue replication server	49	Interdatabase communications	491
Enterprise PKI tools	541	Intermediary CA	445
ERS profile	49	Intermediate certificate	542
EXT kernel	108	Internal audits	381
		Internal threat	31
F		International Telecommunications Union's Standardization sector	446
Firefighter ID	117, 275	Internet Connection Manager (ICM)	433
Firewall	412	Internet of Things	555
<i>configuration</i>	559	IP bans	556
<i>deny/accept logs</i>	422		
Fraud	28, 490	K	
Functional role	182		
		Kerberos	280, 285, 300
G		<i>authentication servers</i>	282
		<i>set up</i>	296
GAAS	380	SSO	296, 305
GDPR	167, 383, 404	SSO troubleshooting	306
		<i>token</i>	283
H		Kernel	94, 181
		<i>compatibility</i>	98
Hardening	41, 514	<i>components</i>	95
Hardware load balancers	483	<i>core</i>	94
HDB User Store	499	<i>download</i>	107
Heartbleed attack	434	DW package	94
HMAC	390	DW.SAR	94
<i>key</i>	390	<i>executable</i>	99
Host policy	525	EXT	108
HTTP protocol	424	<i>extended maintenance</i>	108
HTTPS	411	<i>location</i>	110
Hypervisor	554	<i>patch level</i>	98
		<i>patching</i>	96

Kernel (Cont.)	
<i>release level</i>	97
<i>release notes</i>	96
<i>selecting</i>	107
<i>three-tier approach</i>	106
<i>update</i>	97, 104
<i>upgrade</i>	97, 111
<i>utilities</i>	109, 362
<i>version check</i>	100
<i>versions</i>	99
Kernel upgrade	111
<i>testing</i>	111
Key distribution center	285
Message server	420
Message Server Monitor	420
Metasploit	31, 489
Microsoft Active Directory	281, 297, 302
<i>Federation Services</i>	282
<i>server</i>	285
Microsoft HyperV	553
Microsoft SQL Server	504
Microsoft Windows	503, 530
Microsoft WSUS	527
Monitoring	540
Mounted directories	361
MSSQL	504

L

LDAP	281, 424
Licensing classification	127
Lightweight Directory Access Protocol	281
Linux	503, 528
Load balancers	559
Locked transactions	
<i>export</i>	78
<i>print</i>	78
<i>view</i>	76
Locking transactions	73
Log data	
<i>administration</i>	389
<i>archived</i>	396
<i>evaluate</i>	393
Log files	422
<i>reorganize</i>	392
Logging	379
Login profile parameters	162
Logon language	123
Logs, analyze	400

M

Malware	531
Man-in-the-middle attack	33, 438
Mass user comparison	215
Master role	207
<i>maintenance</i>	211
MCOD	415

N

Naming convention	139
<i>roles</i>	188
Nessus scanner	557
Network access control	412
Network intrusion detection	558
Network security	555
<i>strategy</i>	411
Network Time Protocol	317
Network vulnerability scanner	556
Networking	491
NW-VSI	532

O

OASIS Security Services Technical Committee	309
Object-oriented transactions	229
Operational security	35
Operations	41
OR connector	387
OR linked	387
Oracle database	500
Oracle RDBMS	503
Oracle Transparent Data Encryption	511
Org levels	201
Org values	201
Organizational unit	297
Organizational values	201
OS logs	540

P

P4 protocol	424
Package	
<i>disp+work</i>	94, 98
PAM	98, 106, 527
Parameter	
<i>application area</i>	51
<i>name</i>	51
<i>transactions</i>	229
<i>value</i>	51
Parameters	124
Parent role	207
Password	158
<i>change policy</i>	161
<i>manager</i>	162
<i>policy</i>	29
<i>resets</i>	123
Patch Day Security Notes	344
Patching	35, 341
Perimeter security	35
Permissions file syntax	476
Personal security environment	291, 450
Personalization objects	126
Phishing	27, 36
<i>spear</i>	27, 36
Physical infrastructure	36
Physical security	36, 560
PKCS7 format certificate	293
POODLE attack	434
Positive authorization	115
Privacy violations	27
Product Availability Matrix	98
Profile Generator	169, 192
Profile parameters	45, 161
<i>database editing</i>	53
<i>key parameters</i>	64
<i>table TPFET</i>	52
Profiles	125, 168
<i>mass generation</i>	214
<i>standard</i>	228
PSE	291, 292, 450, 543
Public key	444

R

R/3	21
RAL	379, 404
RDBMS	507
Read Access Logging	379
Red Hat Satellite	527
Reference user	117
Regression testing	354
Report	
<i>authorizations</i>	250
<i>transactions</i>	229
Report PFCG_ORGFIELD_CREATE	203
Report RSPARAM	56
Report RSUSR_DELETE_USERDOCU	119
Report RSUSR0003	156
Report RSUSR008_009_NEW	164, 407
Report RSUSR300	305
Report S_TRUST_DOWNLOAD_CRL	547
Report SU24_AUTO_REPAIR	266
RFC	117, 252, 379
<i>hardening</i>	269
<i>redesign</i>	269
<i>users</i>	139
Risk	37
Role	
<i>assignments</i>	136
<i>derivation</i>	181
<i>design</i>	180
<i>maintenance</i>	197
<i>versioning</i>	217
Role menu	216
<i>comparison</i>	216
Roles	125, 168
<i>assign</i>	219
<i>composite role</i>	168
<i>derived role</i>	168
<i>mass assignment</i>	220
<i>naming convention</i>	188
<i>remove</i>	219
<i>single role</i>	168
Rolling kernel switch	114
Root CA	445

S	
S_A.DEVELOP	228
S_A.SYSTEM	228
SAL	382
<i>versions</i>	383
SAML	280, 286, 309
<i>assertion</i>	283, 311
<i>authentication</i>	518
<i>identity provider</i>	310, 319
<i>logon</i>	311
<i>service provider</i>	310
<i>setup</i>	312
<i>testing</i>	331
SAML 2.0	284, 286
<i>SAP Fiori</i>	286
SAML 2.0 authentication	
<i>disable</i>	336
SAP administrator	22
SAP Cloud Platform Identity	
Authentication	319, 331
SAP EarlyWatch Alert	355
<i>reporting</i>	355
SAP Easy Access	194
SAP Fiori	286, 339
SAP GRC	
<i>Action Usage Report</i>	271
SAP GRC Access Control	117, 152, 167, 188, 271, 273
SAP HANA	494, 501, 528
<i>HDB User Store</i>	498
SAP HANA Studio	498
SAP HANA XS	494
SAP Identity Management	152, 188
SAP landscape	359, 515
SAP Logon Tickets	284, 285
SAP MaxDB	501
SAP NetWeaver AS ABAP	25
SAP NetWeaver AS ABAP 7.5	22
SAP NetWeaver AS Java	22
SAP NetWeaver Virus Scan Interface	532
SAP NetWeaver, ports	417
SAP Note	341
<i>digitally signed</i>	349
<i>implementation</i>	350
<i>revert</i>	348
SAP Note (Cont.)	
<i>severity</i>	343
<i>transporting</i>	352
SAP packages	99
SAP Passport	284
SAP S/4HANA	127
SAP Secure Login Client	285, 305
SAP security	
<i>administrator</i>	22
<i>audit</i>	245
SAP Security Patch Day	344
SAP Single Sign-On	123, 283
SAP Solution Manager	347, 354, 519
7.2	356
SAP Support Portal	343
SAP Web Dispatcher	414, 479, 481, 559
<i>administration console</i>	484
<i>parameters</i>	484
SAP_ALL	118, 168, 228, 374, 518
SAP_NEW	228, 518
SAP*	154
sapcpe	110
SAPEXEDB.SAR	109
SAPLOGON client	305
sapmnt	51
SAPOSS RFC	349
SAProuter	414, 424
<i>all connections</i>	428
<i>documentation</i>	425
Sarbanes-Oxley Act	167
SCCR_LOCK_CLIENT	89
SCCR_UNLOCK_CLIENT	91
Screening rule	471
Secure landscape design	517
Secure Network Communication (SNC)	122
Secure Storage in File System	500
Security administrator	40
Security Assertion Markup Language	
(SAML)	286
Security audit log	379
Security parameters	140
Security planning	41
Security policy	521
Segregation of duties (SoD)	29
Service security	417

Service user	117
<i>firefighter ID</i>	117
SGEN	112
SID	79, 300
SIDADM	46, 102
Simple and Protected GSS-API	
Negotiation Mechanism	285
Single role	181, 192
SNC	122, 286, 371, 411, 423
<i>certificate signed</i>	429
<i>debug</i>	296
<i>encryption</i>	416, 424
<i>personal security environment</i>	291
PSE	450
SAPCryptolib	292
SAPCryptoLib PSE	293
Socket Secure Layer	446
SoD	29, 42, 163, 167
<i>auditing</i>	29
<i>management process</i>	275
Software Update Manager	341
SOX	380
SP stack kernel	99
<i>release</i>	99
Spear phishing	27, 36
SPNEGO	285
<i>set up</i>	296
SQL server	505
<i>Transparent Data Encryption</i>	511
SQL TDE	511
SSAE 16	561
SSCM	527
SSFS	500
SSL	
<i>audit</i>	462
<i>certificate</i>	445
<i>termination</i>	486
SSL certificate installation	465
<i>testing</i>	467
SSL/TLS	416, 423, 451
<i>enable</i>	451
SSO	279
<i>adoption project</i>	283
<i>components</i>	281
<i>directory services</i>	281
<i>identity provider systems</i>	282
SSO (Cont.)	
<i>implementation</i>	283
<i>service providing systems</i>	282
<i>service users</i>	283
<i>strategy</i>	280
Standard profiles	228
Standard users	154
Subnet	415
Suggested client settings	85
SUM	341
Support package	344, 360
<i>Security Notes</i>	344
<i>upgrade</i>	260
SUSE Linux	528
SUSE Manager	527
Sybase ASE	501
Symmetric encryption	437, 442
System	
<i>administrator</i>	22
<i>log</i>	396
<i>upgrade</i>	342
<i>user</i>	116
System parameters	45
<i>access</i>	66
<i>audits</i>	66
<i>setting</i>	59
<i>static and dynamic</i>	53
<i>viewing and setting</i>	55
System profiles	47
<i>comments</i>	50
<i>database level</i>	52
<i>default profile</i>	48
<i>instance profile</i>	47
<i>operating system level</i>	51
<i>other profiles</i>	49
<i>structure</i>	49
<i>viewing properties</i>	54
System trace	175
<i>authorizations</i>	176
<i>return codes</i>	177
T	
Table access	493
Table authorizations	239
<i>audits</i>	245

Table authorizations (Cont.)	Transaction (Cont.)
<i>cross-client</i> 241	MMRV 73
<i>groups</i> 240	<i>object-oriented</i> 229
<i>line-oriented</i> 241	OKP1 73
Table logging 398	PA20 73
Table T000 80	PA30 73
Table views 245	parameter 229
TDMS 518	PFCG 122, 164, 168, 192
Tenable Network Security 557	PFCGMASVAL 257
Test Data Migration Server 518	report 229
The Onion Concept 34	RSAU_ADMIN 389
Thierry Zoller 462	RSAU_CONFIG 385
Threat vector 26	RSAU_READ_LOG 393
Three-tier landscape 280, 516	RZ10 54, 56, 59, 453
Ticket-granting ticket 285	RZ11 56, 58
TLS 446	SA38 72
TLS/SSL	SAFC 254
PSE 455	SAML2 316
testing 460	SCC1 72
TMS 116, 359	SCC4 81, 234
authorizations 373	SCC5 72
configuration 363	SCOT 231
default passwords 367	SCU3 399
Linux 376	SCUM 149
RFC connections 370	SE01 72
route 359	SE10 89
SNC-protected RFC 371	SE11 72
user roles 374	SE16 153, 160, 240
users 367	SE16N 240
TMSADM user 367	SE17 160, 240
Tokens 282	SE37 89
Trace data 179	SE38 70, 72, 368
reuse 179	SE93 170
Transaction	SE97 237
access control 69	SECPOL 140
administrative 72	SGEN 112
AUTH_SWITCH_OBJECTS 264	SHDO 232
CAT6 73	SICF 460
CATS 73	SICK 111
CRCONFIG 545	SMO1 73
dialog 229	SMO1_CUS 73, 221, 384
FI10 73	SMO1_DEV 73, 221
FKO3 172, 184, 198	SM21 111, 397
locking 69, 221	SM30 72, 147, 160, 240
MIRO 73	SM31 240
MMPV 73	SM49 72

Transaction (Cont.)	Treble control 164
SM50 111	Trust chain 445
SM51 111	Trust Manager 290, 449
SM59 252, 349	TSTC check 169
SMICM 468	Two-factor authentication (2FA) 280
SMMS 420	U
SNCWIZARD 286, 287, 300	Upgrade management 524
SNOTE 348	Usage and procedure logging 357
SPAM 341	User
SQ00 252	access reviews 156
SQVI 251	change documents 129
SRALMANAGER 404	change role assignments 136
SSFA 541	classifications 152
SSM2 123	copy 128
STO1 179	default settings 123
STO3N 403	inactive 157
ST22 111	licensing 153
STAD 178	log on verification 160
STAUTHTRACE 176	mass comparison 215
STMS 69, 72, 361, 372	mass processing 131
STRUST 102, 289, 449, 543	naming conventions 139
STUSOBTRACE 180	operations 135
SU01 118, 122, 171	search by logon 133
SU03 169	tables 153
SU10 72, 122, 131	User administration 145
SU21 72, 169	User buffer 118, 173
SU22 260	User classification 127
SU24 72, 173, 192, 198	User directory 281
SU3 124	User groups 145
SU53 172	User ID 115
SU56 118, 173	cryptic 139
SUGR 145	User information system 217, 382, 406
SUIM 221, 354, 380, 406	User master record 115, 118, 145
SUPC 214	User master table 151
SW37 72	User types 115
variant 229	default 154
VSCAN 535	dialog users 139
Transport 360	RFC users 139
administrator 375	V
domain 360	Value role 182
layer 423	Variant transactions 229
operator 375	
viewer 375	
Transport Layer Security 446	
Transport Management System	
(TMS) 69, 116, 359	

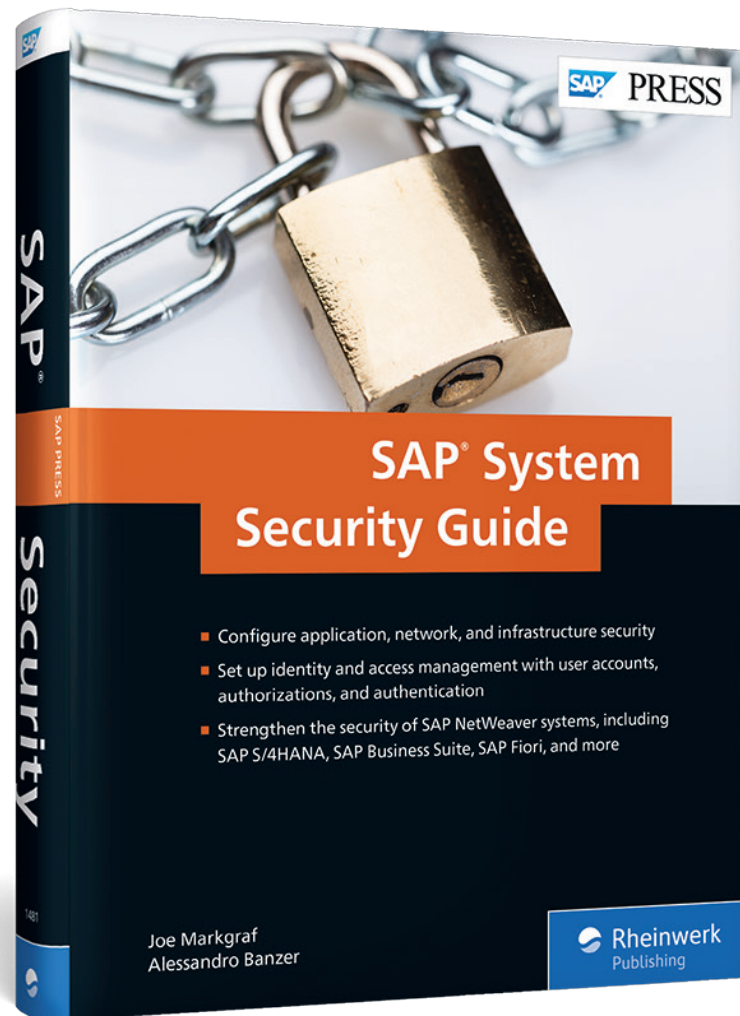
Viewing and setting parameters,
 Report RSPARAM 56
 Virtual LAN 556
 Virtual machine escape 554
 Virtual machines 554
 Virtualization 553
 Virus scan definitions 537
 Virus Scan Interface 532
 Viruses 531
 VMware ESX 553
 VMware Go 527
 Vulnerability scanner 557

W

wdispmon 477
 Web Dispatcher 433
 Windows authentication mode 505
 Windows domain controller 530
 Workload Monitor 382, 403

X

X.509 certificates 279, 280, 284, 446
 XAMS 272
 Xen hypervisor 553
 Xiting Authorizations Management
 Suite 272



Joe Markgraf and Alessandro Banzer

SAP System Security Guide

574 Pages, 2018, \$79.95

ISBN 978-1-4932-1481-5

 www.sap-press.com/4307



Joe Markgraf is a senior cloud architect and advisor for SAP HANA Enterprise Cloud at SAP. Before joining SAP he worked as a Basis and security administrator, contributing to both small- and large-scale SAP system implementations. He holds a business degree with a focus on information system management from Oregon State University. He enjoys playing vintage video games and shooting sports with his family in Washington State.



Alessandro Banzer is the Chief Executive Officer of Xiting, LLC. He has worked in information technology since 2004, specializing in SAP in 2009. Since then, Alessandro has been involved with global SAP projects in various roles. Alessandro is an active contributor and moderator in the Governance, Risk, and Compliance space on SAP Community, as well as a speaker at SAPP-HIRE, ASUG, SAPInsider, and other SAP-related events. He holds a degree in business information technology, as well as an executive master of business administration from Hult International Business School in London, UK.

We hope you have enjoyed this reading sample. You may recommend or pass it on to others, but only in its entirety, including all pages. This reading sample and all its parts are protected by copyright law. All usage and exploitation rights are reserved by the author and the publisher.