

ADM940

Exploring the Authorization Concept for SAP S/4HANA and SAP Business Suite

**PARTICIPANT HANDBOOK
INSTRUCTOR-LED TRAINING**

Course Version: 24
Course Duration: 3 Days

SAP Copyrights, Trademarks and Disclaimers

© 2025 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. Please see <https://www.sap.com/corporate/en/legal/copyright.html> for additional trademark information and notices.

Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors.

National product specifications may vary.

These materials may have been machine translated and may contain grammatical errors or inaccuracies.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP SE or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP SE or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platform directions and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.

Typographic Conventions

American English is the standard used in this handbook.

The following typographic conventions are also used.

This information is displayed in the instructor's presentation



Demonstration



Procedure



Warning or Caution



Hint



Related or Additional Information



Facilitated Discussion



User interface control

Example text

Window title

Example text

Contents

vii	Course Overview
1	Unit 1: Understanding Authorizations in General
3	Lesson: Describing Authorizations
11	Lesson: Creating and Implementing an Authorization Concept
31	Unit 2: Understanding Basic Terminology of Authorizations
32	Lesson: Explaining Elements and Terminology of the ABAP Authorization Concept
39	Exercise 1: Practice System Exercise: Display Authorization Information of the Authorization Concept(ABAP)
49	Lesson: Identifying Authorization Checks in the SAP System
55	Exercise 2: Practice System Exercise: Check Authorizations in the SAP System
65	Unit 3: Creating Users
66	Lesson: Maintaining and Evaluating User Data
83	Exercise 3: Practice System Exercise: Maintain and Evaluate User Data
93	Lesson: Understanding the Business User Concept
101	Exercise 4: Practice System Exercise: Create a user master record for a business user
107	Unit 4: Working with the Role Maintenance
108	Lesson: Creating Standard Roles
125	Exercise 5: Practice System Exercise: Maintain Standard Roles
141	Lesson: Creating Customizing Roles
143	Lesson: Implementing a Composite Role Strategy
147	Lesson: Implementing a Derived Role Strategy
151	Exercise 6: Practice System Exercise: Maintain Special ABAP Roles
168	Lesson: Outlining Subtleties of Authorization Maintenance
177	Exercise 7: Practice System Exercise: Understand the Subtleties of Authorization Maintenance

191 Unit 5: Performing Basic Settings

- | | |
|-----|--|
| 192 | Lesson: Investigating Installation and Upgrade Tasks |
| 203 | Exercise 8: Practice System Exercise: Maintain Authorization Default Values |
| 211 | Lesson: Maintaining Access Control and User Administration |
| 227 | Lesson: Implementing User and Authorization Management Strategies |
| 237 | Exercise 9: Practice System Exercise: Access Control and User Administration |

255 Unit 6: Using Traces

- | | |
|-----|---|
| 256 | Lesson: Troubleshooting Authorization Checks |
| 265 | Exercise 10: Practice System Exercise: Troubleshoot and Administer Aids |
| 269 | Lesson: Using Traces to Maintain Role Menus and Authorizations |
| 273 | Exercise 11: Practice System Exercise: Use Authorization Trace |

283 Unit 7: Transporting Authorizations

- | | |
|-----|---|
| 284 | Lesson: Transporting Authorization Components |
| 291 | Exercise 12: Practice System Exercise: Transport Authorization Components |

297 Unit 8: Administrating Users in the Company Landscape

- | | |
|-----|--|
| 299 | Lesson: Working with the Central User Administration |
|-----|--|

311 Unit 9: Course Glossary

- | | |
|-----|-------------------------|
| 313 | Lesson: Course Glossary |
|-----|-------------------------|

Course Overview

TARGET AUDIENCE

This course is intended for the following audiences:

UNIT 1

Understanding Authorizations in General

Lesson 1

Describing Authorizations

3

Lesson 2

Creating and Implementing an Authorization Concept

11

UNIT OBJECTIVES

- Describe the SAP authorization concept.
- Implement the SAP authorization concept.

Describing Authorizations

LESSON OVERVIEW

This lesson will introduce the contents of the ADM940 course. It will also provide an introduction to the topic of authorizations and the *role-based authorization concept*, using a number of overview figures.

Business Example

Authorizations are used to control access at the application level. At this level, the term **role** is at the center of the SAP authorization concept. SAP course ADM940 describes the individual steps, from setup, through the implementation of a role concept with **PFCG**, to its use in a production environment. The system must also be protected at the operating system, database, network, and front end levels in order to implement a comprehensive security concept. SAP courses ADM950 and ADM960, for example, consider these issues.



LESSON OBJECTIVES

After completing this lesson, you will be able to:

- Describe the SAP authorization concept.

Why and for What Do We Require Authorizations?

Table 1: Security Expectation Overview

Security Expectations	
	<ul style="list-style-type: none">• Protection of sensitive business data on the basis of:<ul style="list-style-type: none">- Laws- Agreements- Regulations• Advantageous cost-benefit relation• No obstruction of business processes

Security Expectations

Requirements for protecting sensitive data:

- A company must meet certain legal requirements based on their country of operation. These include, for example, data protection laws (personal data, family status, illnesses, and so on), or employee protection.

- A company must be able to adhere to agreements with and requirements of partners and vendors, and to ensure their implementation.
- A company must publish and enforce security policies, so that a secure environment can be established and maintained. This applies both to data used externally and to data used internally.

Cost-Benefit Relation

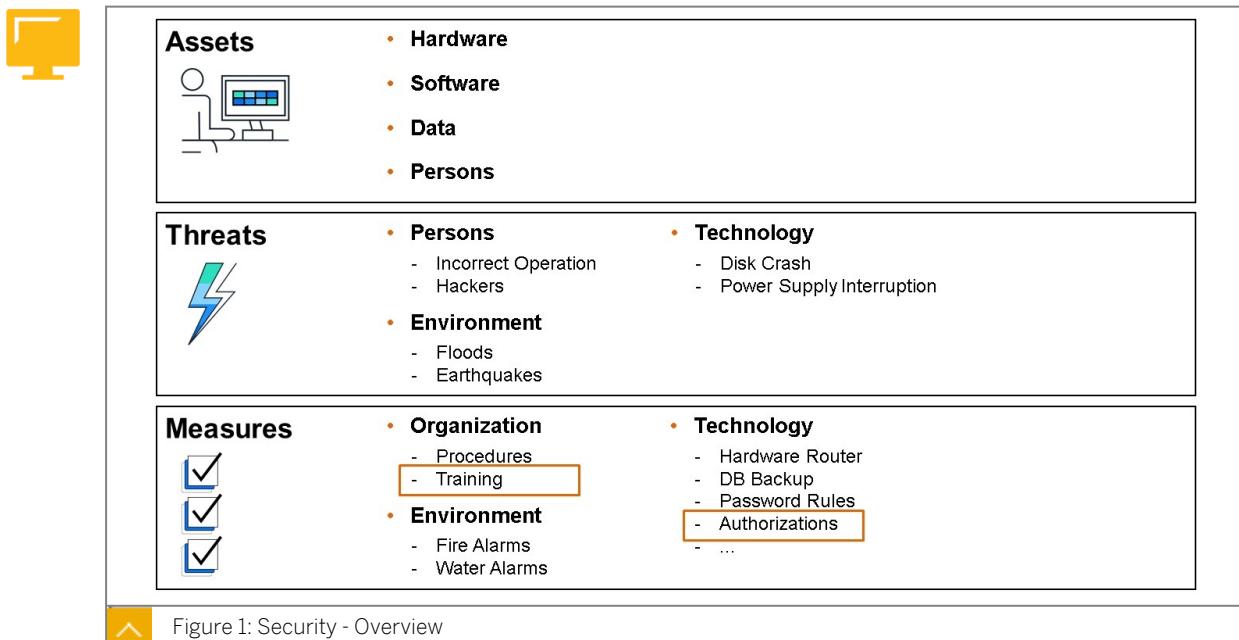
- There are a large number of different possible threats. Perfect security could only be achieved with cross-dimensional assignment of authorizations. However, the benefits achieved in this way are often not relative to the costs incurred.

With some values, it is cheaper to replace a loss than to protect the data at great expense. A company should therefore concentrate on areas in which a clear benefit can be realized through this expenditure. This saves unnecessary investments of time and money.

- It is impossible to ensure complete security against all potential threats. Therefore, a company must be able to weigh up the extraordinary risks of a threat against the costs of a security system.

Obstruction of Business Processes

- It is disadvantageous if business processes are controlled with authorizations to such an extent that almost every call leads to an error message. A situation of this type is not favorable for the processes in a company.
- The assignment of authorizations should be structured in a way that is clear for the administrator, by using a smaller number of roles. If this is not done, it is often difficult to remove undesired obstructions to business processes in complex, nested authorizations. Only with a transparent structure can this be avoided. If problems occur nevertheless, it is only in this way that the places to be maintained can be found.



When developing a security concept, you must first determine **what** you want to make safe. Which **assets** must be protected? To which categories do these assets belong (for example: hardware, software, data, persons)? When assigning assets to categories, consider the

consequences of losing these assets. When calculating the value of fixed assets, for example, you should take into account the loss of value due to depreciation, damage, or theft.

You must also determine **against what** you want to protect your assets. What are potential **dangers**? Sources of danger could be, for example, technology, the environment, or persons.

- Persons: Important employees leaving the company, dissatisfied or inexperienced employees. Hackers with criminal intent.
- Technology: Processing errors (caused by applications or operating systems), viruses, power supply interruption, hardware failure.
- Environment: Fire, flood, dust, earthquakes.

Once you have identified your assets and the potential sources of danger, you can develop security mechanisms. You must determine an appropriate protective measure for each source of danger. These **measures** should also be assigned to different categories (for example: organizational, technical, environmental).

- Organizational measures; Training, internal security policy, procedures, roles, responsibilities.
- Technical measures: Inclusion of electronics for checks (routers). Access authorizations for systems and data.
- Environmental measures protect physical system components against natural sources of danger.



Layer	Components	Security Aspects	SAP Course
Presentation	GUI, browser PC	Access control, virus scanners, encryption	ADM960
Communication	SAProuter, network, SNC	Access control, packet filtering, encryption	ADM960
Web Connection	ICM, SAP Web Dispatcher	Encryption, certificates, Single Sign-On	ADM960
Application	Application modules, work processes, interfaces	SAP users, password rules, authorizations	ADM940
Database	Relational database	Access to SAP tables, backup, consistency	HA200
Operating System	UNIX, Windows NT, OS/400, OS 390	Access to SAP files, OS services	???

Figure 2: SAP Security Levels

SAP systems are made safe at a variety of levels. Each level has its own protection mechanisms.

To avoid unauthorized system access, for example, system and data access control mechanisms are provided at the application level.

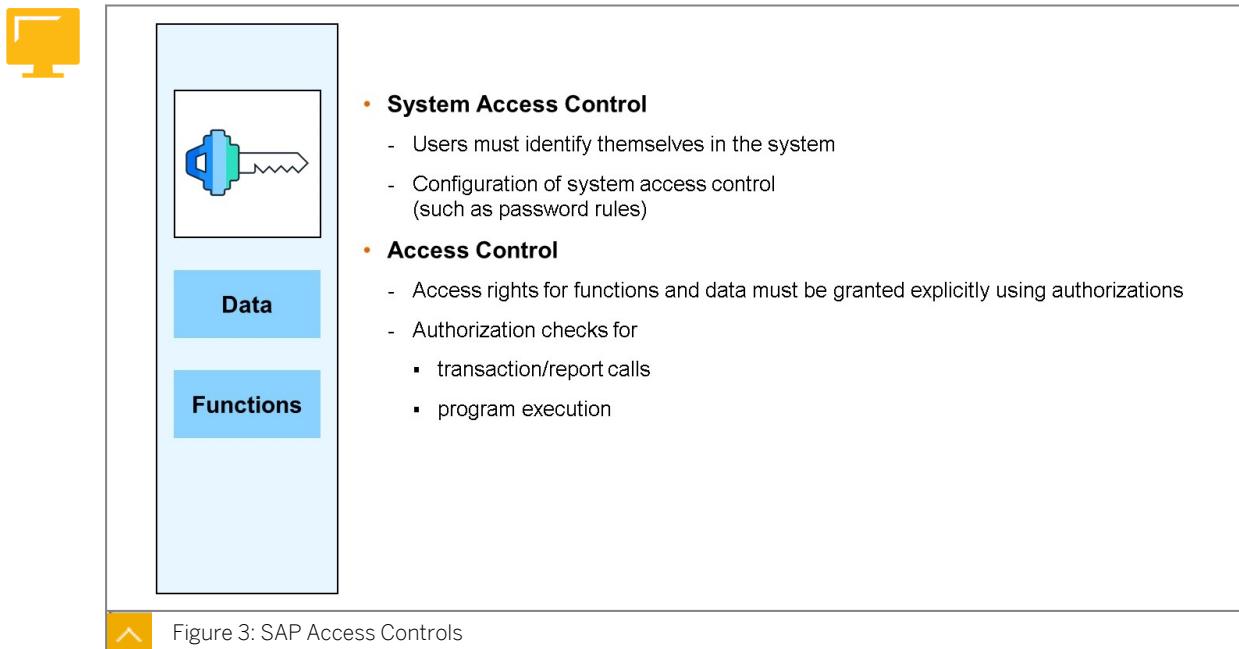
When protecting an SAP system, you must consider the following:

- Security must be implemented at all levels, since the overall security depends on the weakest part.

- A complex authorization concept is therefore only one aspect of an overall security concept.

This course deals only with the security mechanisms at application level. The other levels are covered in the SAP courses ADM950 and ADM960.

System Access Control and “Role-Based” Access Control



To work with an SAP system, users require unique user IDs. A user master record must be created in the system for each user. The user master record also stores the password that the system prompts the user to enter when logging on.

There are numerous mechanisms for preventing unauthorized access to an SAP system that can raise the security level of a system if configured appropriately. These configurable settings include, for example, the minimum length and the expiry date of passwords.

To protect business data and functions against unauthorized access, SAP programs utilize authorization checks. To pass an authorization check of this type, a user needs the appropriate authorization.

Authorizations are assigned using profiles in the form of roles that are entered in the user master record.

Users, Roles, and Authorizations

The SAP term *role-based authorization concept* is introduced on the following pages.

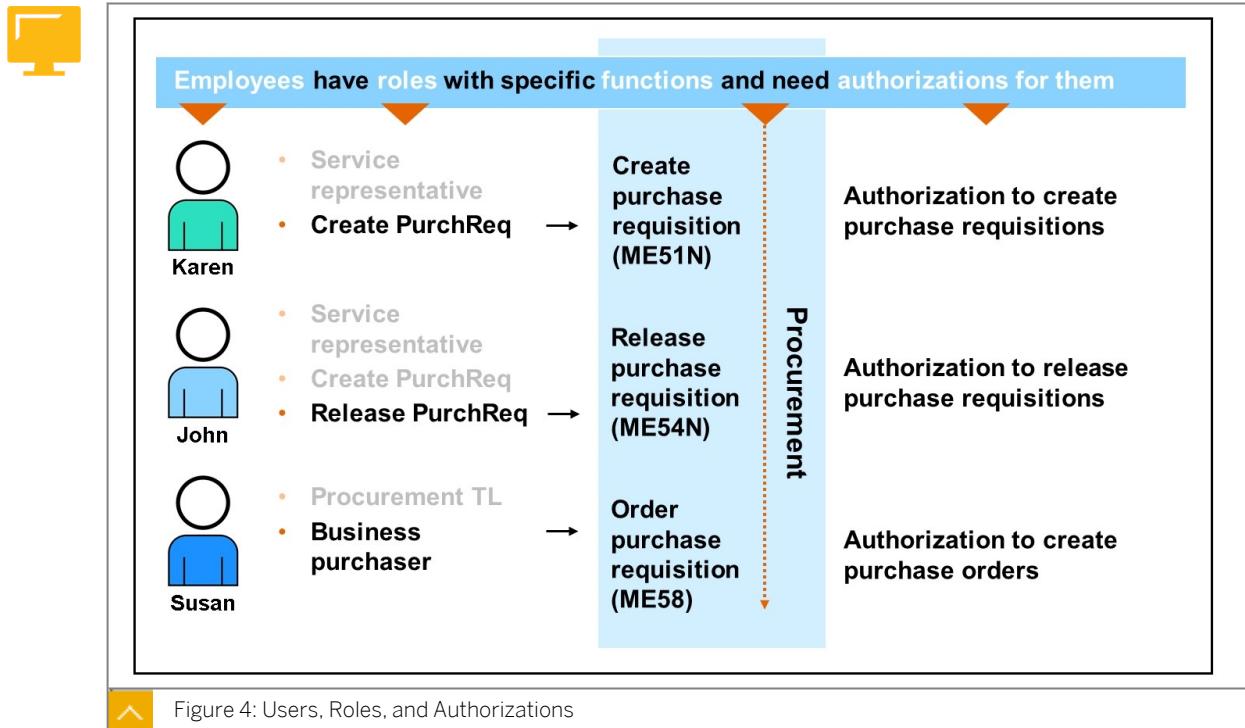


Figure 4: Users, Roles, and Authorizations

People perform **roles** that belong to **business scenarios**. In the example above, *Karen* performs the “Create Purchase Requisition” role in the PROCUREMENT business scenario.

A **person** can have multiple **roles**. *John*, for example, has been assigned the roles “Service Representative”, “Create Purchase Requisition”, and “Release Purchase Requisition”.

A **role** is a group of **activities** performed within business scenarios. For example, the activity CREATE PURCHASE REQUISITION belongs to the “Create Purchase Requisition” role.

A **role** generally includes all **activities** that may occur in the respective **scenario**.

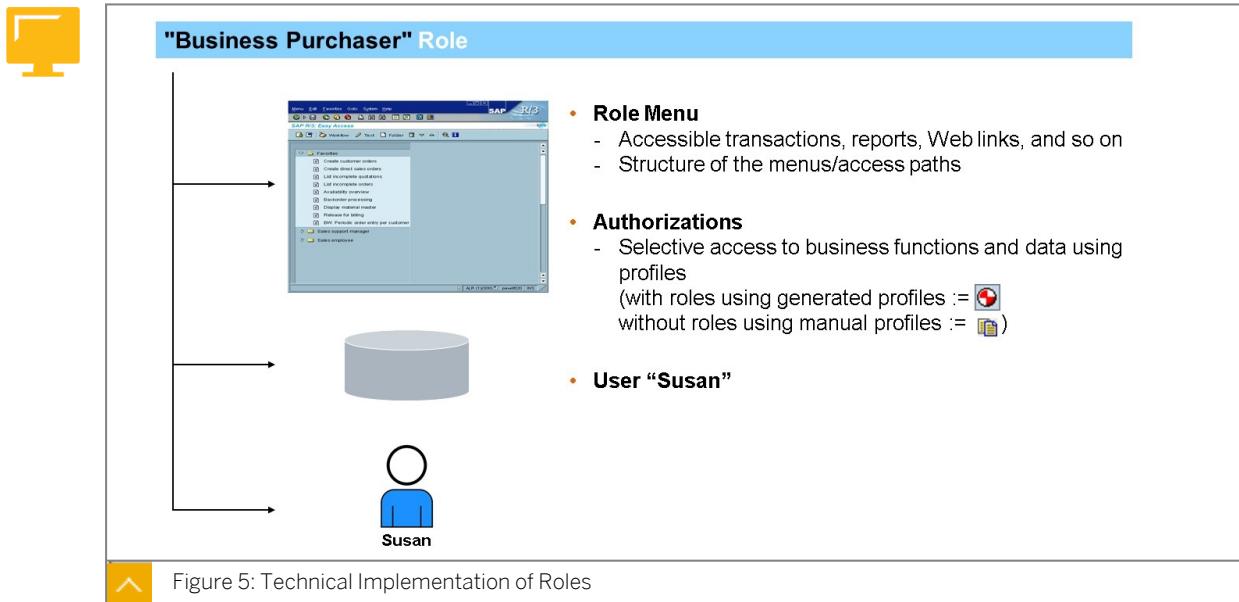
A single role can be involved in several **scenarios**. The EMPLOYEE, for example, participates in the SELF-SERVICES and the REPORTING scenarios, among others.

A single **scenario** may require the participation of multiple **roles**. In this way, the roles “Service Representative”, “Create Purchase Requisition”, “Release Purchase Requisition”, and, for the supervisor, the role “Business Purchaser” are all involved in the PROCUREMENT scenario.

Business scenarios are groups of **activities** performed by one or more **employees** in their respective **roles**. The PROCUREMENT scenario, for example, comprises the activities CREATE PURCHASE REQUISITION, RELEASE PURCHASE REQUISITION, and CREATE PURCHASE ORDER.

Activities are associated with specific system functions that can only be accessed with the proper authorization.

Technical Implementation of Roles



To implement roles technically, you must create roles (or composite roles) using the Role Maintenance.

A role consists of the following components:

- Role Menu

The **transactions**, reports, Web links, and so on, in a role are combined into a **menu**, to which the users of the role have access.

- Authorizations

The **authorizations** define the access rights for business functions and data.

- User

To grant the access rights of a role to a **user**, you must assign the user to the role. You can assign users using either the Role Maintenance or user administration.

SAP delivers a large number of predefined roles with SAP systems. Customers can use these roles as templates and customize them to meet their individual requirements. You can use the report RSUSR070 and the selection "SAP*" to display all the role templates that are supplied by SAP.

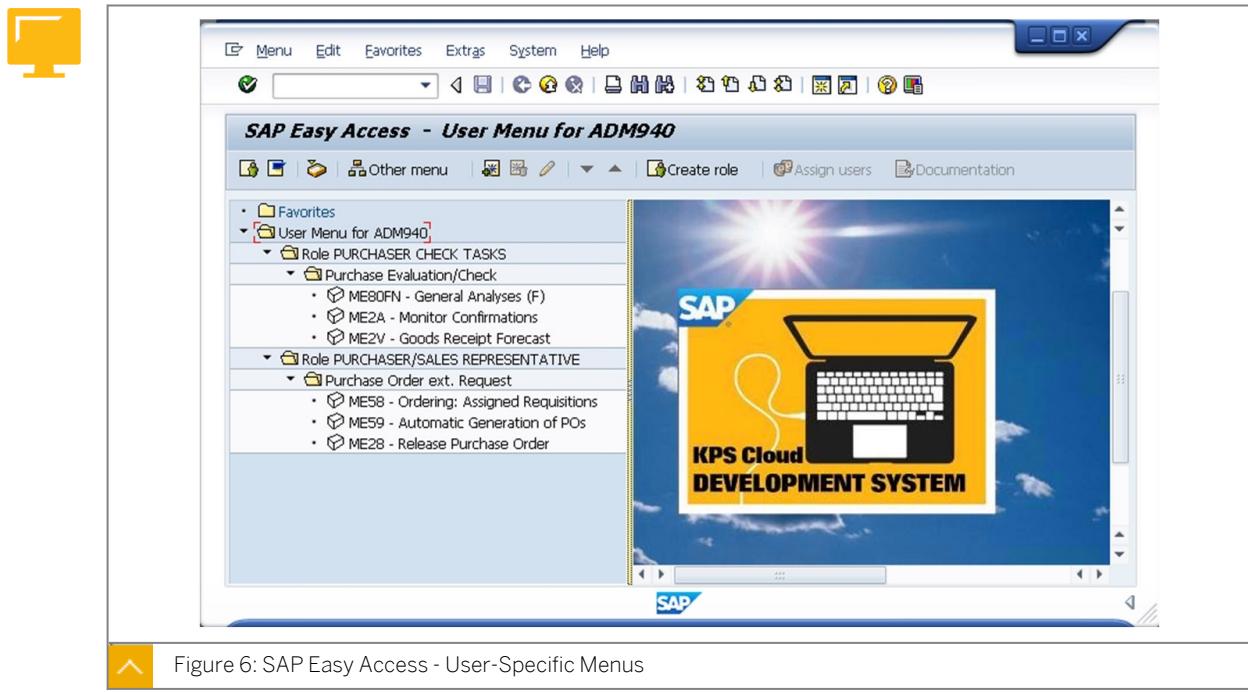


Figure 6: SAP Easy Access - User-Specific Menus

SAP systems support the setup of user-friendly personal user menus.

When creating the roles, the system administrator specifies the required functions including their descriptions. The descriptive text can be changed, and is therefore freely definable.

Once a user has been assigned a particular role (with menu), the appropriate personal user menu is automatically displayed when the user logs on to the system. The menu is based on the assigned activities.

In addition to the functions preset by the administrator, users can choose their own "Favorites". There are two ways to do this. Users can drag the desired function with the mouse into the relevant menu area, or they can select the transaction and then choose "Add to Favorites" to add the function to their list of favorites.

If the user calls a transaction, the personal menu is hidden so that the entire screen can be used for transaction processing. If the user quits the transaction or opens a new session, the menu is shown in the foreground again.

Facilitated Discussion

You should prompt the participants to become involved in discussion to avoid the course becoming a monologue over three days. This should relax the atmosphere between the instructor and the participants, which is usually reserved to begin with.

There is a round of introductions in most SAP courses. However, not all participants appreciate this, since it takes up a lot of important course time. You should decide yourself whether you think this is useful. We recommend that you do not do this with large groups. However, to obtain a general impression about the previous knowledge of the participants, you can use additional questions during the discussion to find out about the knowledge and wishes of the participants. Examples of questions are:

Who is familiar with transaction PFCG?- What are the experiences of participants familiar with the transaction?- In which area do you work (FI, CO, MM, HR, CRM, APO, BW, and so on)?- Are you familiar with CUA or portals? Do you use these?



LESSON SUMMARY

You should now be able to:

- Describe the SAP authorization concept.

Unit 1

Lesson 2

Creating and Implementing an Authorization Concept

LESSON OVERVIEW

This lesson will present a possible method for introducing an authorization concept in a company. The methodology used here to implement a role and authorization concept consists of five steps (preparation, analysis and conception, implementation, quality assurance and test, and cutover), which will be described in more detail in this lesson. User and authorization administration are defined, specified, and implemented in parallel to these five steps.

Business Example

Before going live, your company wants to implement an authorization concept. The steps required to realize the authorization concept must be planned in the context of the entire implementation process. During the planning phase you want to estimate the time and personnel resources needed.

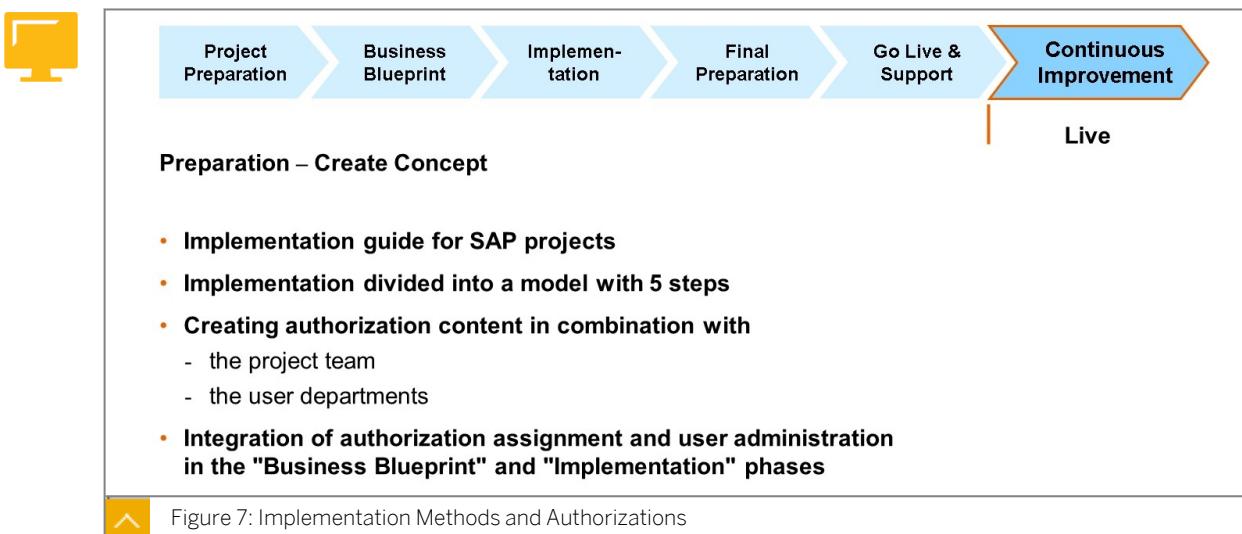


LESSON OBJECTIVES

After completing this lesson, you will be able to:

- Implement the SAP authorization concept.

Development of an Authorization Concept



The procedure used here is based on the principles of the SAP implementation method. Many consultancy companies use a similar model, usually with their own name. When combined, the individual steps of this method ensure quick and efficient implementation of the SAP system.

Setting up an authorization concept must be planned and implemented step-by-step using a project plan. In the example used here, the project was divided into five key points at the uppermost level (these are often also called phases):

- **Project Preparation**

Inclusion of all relevant decision-makers for the SAP implementation and selection of the internal and external members of the project team.

- **Business Blueprint**

The business requirements of the implementing company are determined. The Business Blueprint is a visual representation of the status of the company that is to be realized in the SAP implementation. All business processes are analyzed and described here. This is the basis for the later authorization concept.

- **Implementation**

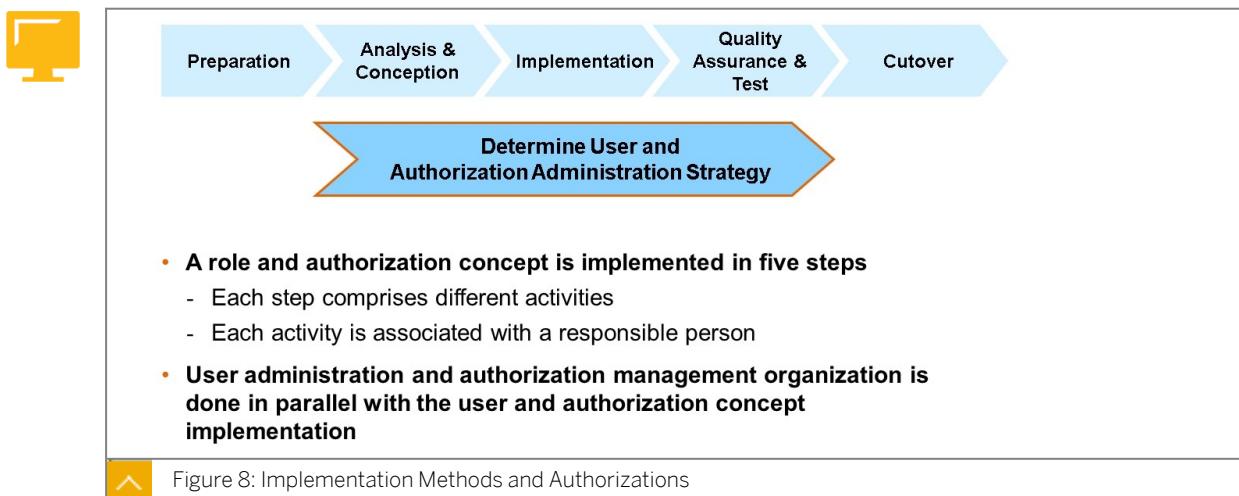
Configuration and fine tuning of the SAP system. The business processes created and described in the previous phase are the starting point for the implementation of the roles.

- **Final Preparation**

Testing of all interfaces, training of users, and migration of business data into the SAP system.

- **Go Live & Support**

Start of SAP production operation, specification of procedures, and measurement items for ongoing checking of the benefits of the investment in the SAP system.



To fulfill a certain task, the employee responsible must normally use several applications. The transactions and reports used for a business activity can be combined into roles.

It is important that users can only process those tasks that they are authorized to perform, and are prevented from making unintentional or incorrect changes in system areas that are outside their competence. Since all SAP components use authorizations to control access to their functions, administrators only assign those authorizations to each role that is necessary to perform the role-specific tasks.

Besides authorizations, a role comprises the user menu specifications. When a user logs on to an SAP system, the system displays a user-specific menu, with selected transactions, reports, and Internet links in the form of a tree structure. This menu is based on the assigned

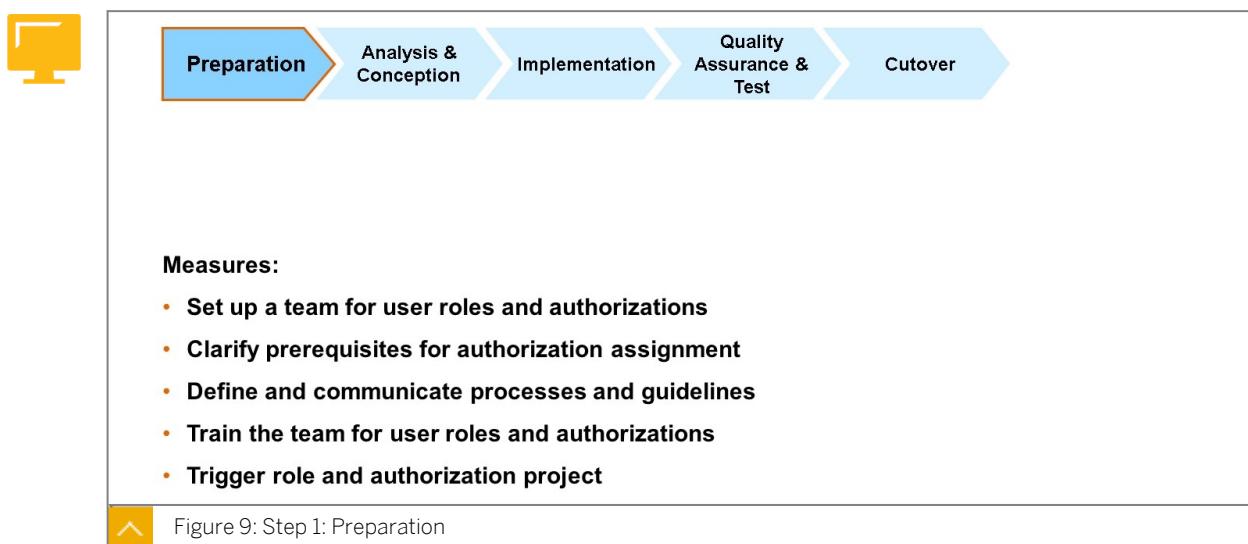
role. Users can only access transactions and reports that they are authorized to use. This eliminates unnecessary functions from the navigation structure.

When developing the role and authorization concept, the challenge is to coordinate business requirements at a cross-department level and protect sensitive data against potential dangers.

This is why we recommend that you develop the role and authorization concept as a separate project. You should follow the procedure explained in this training course and use the demonstrated method for orientation.

An Authorization Concept Is Developed Step-by-Step

Step 1: Preparation



Set up a team responsible for the specification and implementation of the user roles and the authorization concept.

Identify the business areas affected and their special security requirements. Like the control mechanisms selected, these can vary from area to area. Normally, the security requirements of the Human Resources department are more demanding than those of other departments. Therefore, you must first determine the desired security level.



Hint:

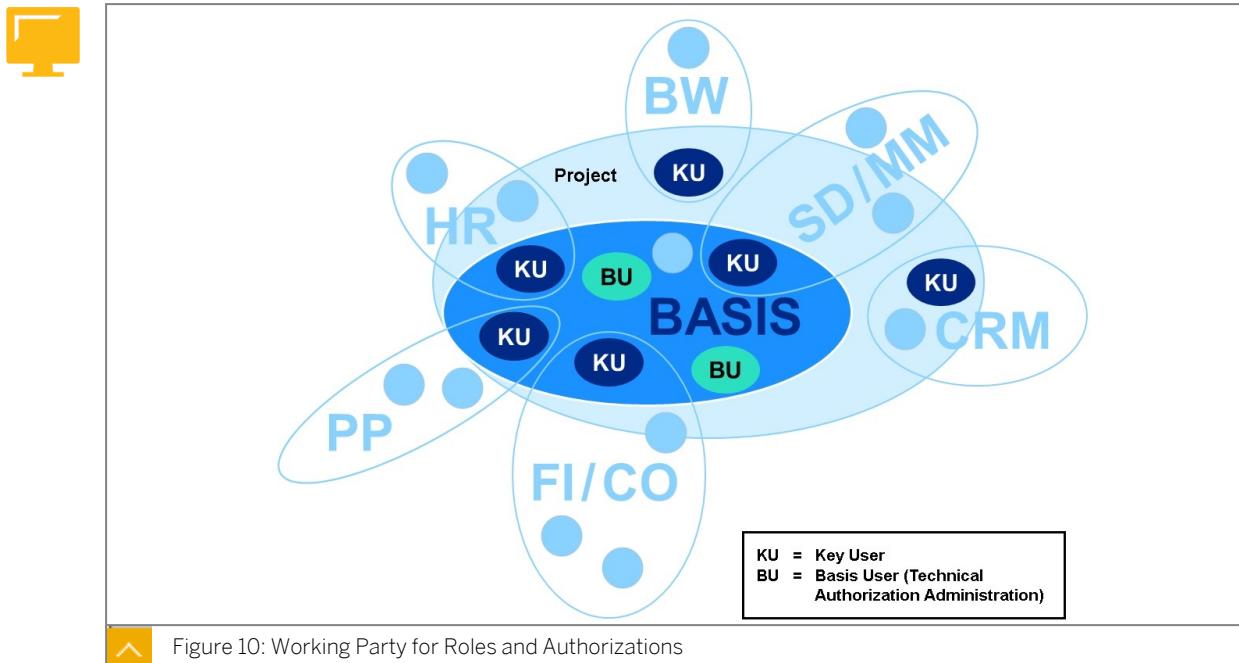
Consider the different security requirements for the production, test, and development environments. Bear in mind, too, that user roles often need to access a number of systems and may therefore require different functions and authorizations depending on the system.

Train the team for roles and authorizations with regard to specification and implementation topics.

The team members must be familiar with the basic principles of the SAP authorization concept and the available control and administration tools (such as central user administration). The members responsible for implementation must be able to use the Role Maintenance.

Since the role and authorization project requires the cooperation of various business areas and departments, SAP recommends that you inform the responsible employees of the project

targets set and establish communication channels at an early stage to ensure efficient handling.



When developing the role and authorization concept, the challenge is to coordinate business requirements at a cross-department level and protect sensitive data against potential dangers.

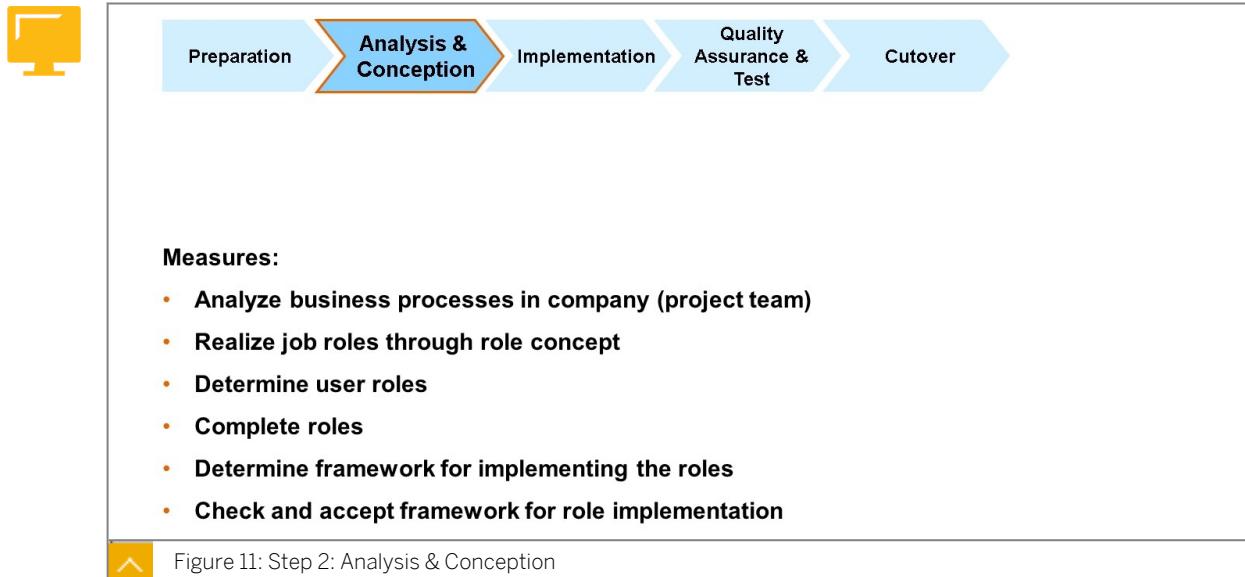
While user roles and the authorization concept are specified with the cooperation of the individual business areas, they are normally implemented by the IT department. This is why you must set up a cross-area and cross-department project team.

The team members have the following tasks:

- Create SAP-dependent role descriptions in the “Analysis & Conception” step.
- Cooperate with the IT department during implementation.
- Set up and run through test scenarios.

To ensure that both the authorization concept and the procedures for user administration and authorization management comply with the control regulations of the company, the internal invoice verification department must be involved in the authorization project at an early stage.

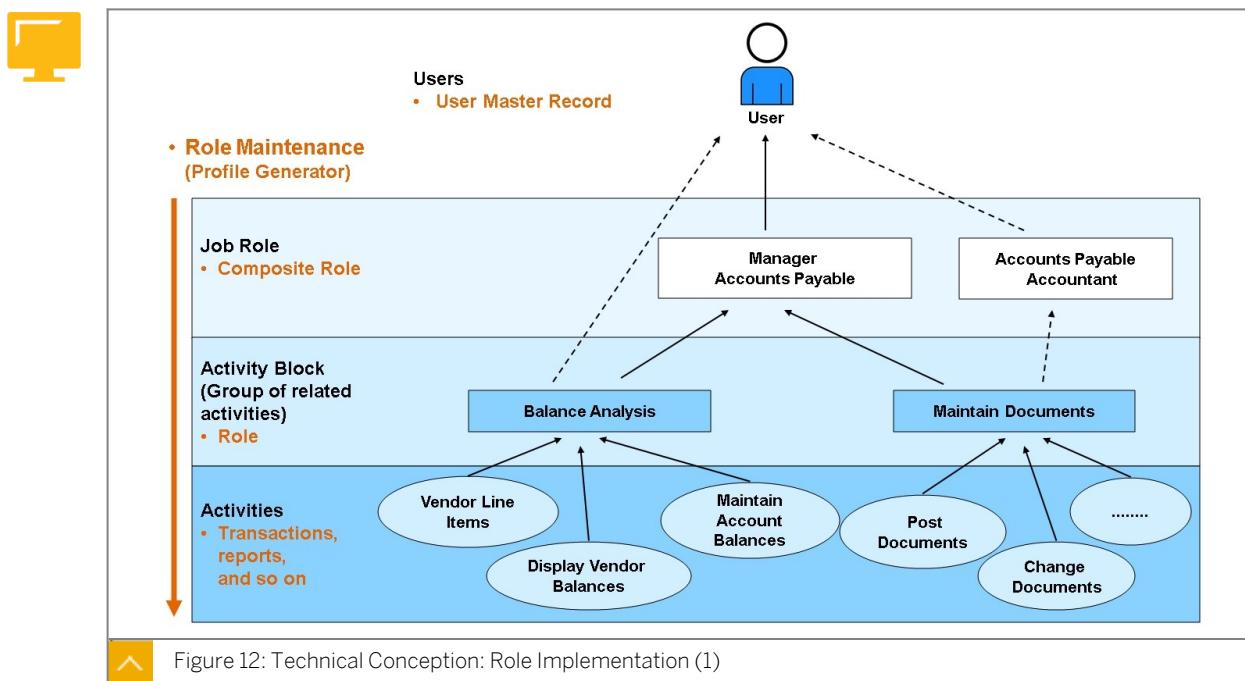
Step 2: Analysis & Conception



Specification of the role and authorization concept:

- Identify required roles. Determine task profiles based on the organization chart and a business process analysis. Check if SAP role templates can be used.
- Specify relevant applications functions (transactions, reports, Web links) to the roles. Make any required adjustments if role templates are used.
- Specify if the roles are higher-level roles or specific roles; that is, if they are subject to any restrictions resulting from organizational or application-specific control mechanisms.
- Identify required composite and individual roles for implementing the roles and the authorization concept.

Check the role and authorization concept. To detect any shortcomings in conception before actual implementation, SAP recommends that you create a prototype of the concept.



User roles are technically implemented using individual, composite, and derived roles. Based on the transactions and reports selected for each role, the Role Maintenance automatically determines all authorization objects required for performing the functions specified, and creates the corresponding authorization profile.

Using individual, composite, and derived roles, you can model the role structure in two ways:

- You can model each role as an individual role that contains all required functions. If some functions are used unchanged in multiple roles, the associated transactions and reports are contained in several individual roles. If general function modifications are required, this consequently affects several individual roles.
- Alternatively, you can model each role as a composite role consisting of individual and derived roles. In this case, the individual and derived roles represent activity blocks, that is, groups of interrelated functions (for example: all functions needed for a specific business scenario). Since individual and derived roles contain encapsulated functions, they can be used in multiple or composite roles. The advantage of this approach is that multiple access to transactions used in several individual roles is avoided. Therefore, organizational or process-related modifications that affect several user roles can be applied by adjusting a single role.



Authorization List - Role Design						Enterprise Area >>>	Job Role >>>	R/3-Links: T-Code	Scope	Scope	Scope
E 1	E 2	E 3	E 4	E 5	E 6						
Instruction...											
Business Processes											
External Accounting											
General Ledger Processing											
Closing Operations											
Profit and Loss Adjustment											
						General Ledger: Profit and Loss Adjustment	F0.50				
						General Ledger: Upd. Balance Sheet Adj.	F5D				
						General Ledger: Post Balance Sheet Readj.	F5E				
						General Ledger: Balance Sheet Readj., Log	F5F				
						General Ledger: Upd. Balance Sheet Spec.	F5G				
Accounts Payable											
Invoices and Credit Memos											
Parked Document Posting [Vendors]											
						Post Parked Document	FBV0				
						Changed Parked Document	FBV2				
						Display Parked Document	FBV3				
						Change Parked Doc. (Header)	FBV4				
						Document Changes: Parked Documents	FBV5				
						Reject Parked Document	FBV6				
Vendor Account Analysis											
Balance Analysis											
						Customer Account Analysis	FD11				
						Vendor Account Balance	FK10				
						Display Vendor Balances	FK10N				
						Vendor Line Items	FBL1N				
Correspondence with Vendors											
Correspondence with Vendors											
						Correspondence: Print Requests	F0.61				
						Correspondence: Print Internal Docs	F0.62				
						Correspondence: Delete Requests	F0.63				
						Correspondence: Maintain Requests	F0.64				

Figure 13: Analysis: Determining User Roles

Step 2 “Business Blueprint for the Implementation Project” is used to analyze and determine the scope of the implementation. When creating the Business Blueprint, you determine which processes are to be implemented in the context of the implementation.

The result of all the business processes that can be used and mapped in the SAP system is saved as a Microsoft Excel list in this example.

The user roles are created and completed in this authorization list. A similar list can also be generated in the SAP system. In this case, the list is component-oriented, and not process-oriented as in our example.

SAP systems are delivered with a number of role templates in which the associated application functions (transactions and reports), the user menu, and the authorization data are predefined. These templates can be used as a basis for analyzing and developing the company-specific roles and the authorization concept.



Hint:

These roles begin with SAP_* and the profiles for these roles have not yet been generated. They are only intended as templates with examples for the authorization setting.



Authorization List - Role Design						Enterprise Area >>>	FI	FI	FI
E 1	E 2	E 3	E 4	E 5	E 6	R/3-Links: T-Code	FI_Manag	AP_Manag	AP_Acc
Instruction...									
Business Processes									
External Accounting									
General Ledger Processing									
Closing Operations									
Profit and Loss Adjustment									
General Ledger: Profit and Loss Adjustment						F0.50		x	
General Ledger: Upd. Balance Sheet Adj.						F.5D		x	
General Ledger: Post Balance Sheet Readj.						F.5E		x	
General Ledger: Balance Sheet Readj., Log						F.5F		x	
General Ledger: Upd. Balance Sheet Spec.						F.5G		x	
Accounts Payable									
Invoices and Credit Memos									
Parked Document Posting [Vendors]									
Post Parked Document						FBV0	x	x	x
Changed Parked Document						FBV2	x	x	x
Display Parked Document						FBV3	x	x	x
Change Parked Doc. (Header)						FBV4	x	x	x
Document Changes: Parked Documents						FBV5	x	x	x
Reject Parked Document						FBV6	x	x	x
Vendor Account Analysis									
Balance Analysis									
Customer Account Analysis						FD11		x	
Vendor Account Balance						FK10		x	
Display Vendor Balances						FK10N		x	
Vendor Line Items						FBL1N		x	
Correspondence with Vendors									
Correspondence with Vendors									
Correspondence: Print Requests						F0.61			x
Correspondence: Print Internal Docs						F0.62		x	
Correspondence: Delete Requests						F0.63		x	
Correspondence: Maintain Requests						F0.64		x	



Figure 14: Conception: Completing User Roles (1)

The authorization list is a Microsoft Excel table that helps the project team to model the user roles before they are implemented in the SAP system. Using this list, the roles can be developed before the system is installed.

In the authorization list, you create user roles and specify the associated transactions. In this example, it consists of two worksheets:

- **Sheet 1: Process View (Roles Design - Scope)**

The structure shows the business processes that were selected during the analysis and conception of the enterprise. The job roles and user roles are specified and linked with the processes here.

- **Sheet 2: Transaction Overview for Each Role (T Code for Each Role)**

You can generate an overview of the transaction assignments for each role in the transaction overview (after the modeling on sheet 1).



Authorization List - Role Design						Enterprise Area	>>>	FI	FI	FI		
E 1	E 2	E 3	E 4	E 5	E 6	Job Role	>>>	FI_Manag	AP_Manag	AP_Acc		
						R/3-Links: T-Code		Scope	Scope	Scope		
Instruction...												
Business Processes												
External Accounting												
General Ledger Processing												
Closing Operations												
Profit and Loss Adjustment												
General Ledger: Profit and Loss Adjustment												
General Ledger: Upd. Balance Sheet Adj.												
General Ledger: Post Balance Sheet Readj.												
General Ledger: Balance Sheet Readj., Log												
General Ledger: Upd. Balance Sheet Spec.												
Accounts Payable												
Invoices and Credit Memos												
Parked Document Posting [Vendors]												
Post Parked Document												
Changed Parked Document												
Display Parked Document												
Change Parked Doc. (Header)												
Document Changes: Parked Documents												
Reject Parked Document												
Vendor Account Analysis												
Balance Analysis												
Customer Account Analysis												
Vendor Account Balance												
Display Vendor Balances												
Vendor Line Items												
Correspondence with Vendors												
Correspondence with Vendors												
Correspondence: Print Requests												
Correspondence: Print Internal Docs												
Correspondence: Delete Requests												
Correspondence: Maintain Requests												

Figure 15: Conception: Completing User Roles (2)

Modeling the role structure: Analyze the authorization list and determine the areas in which access to several transactions is needed. Activity blocks such as this can be created as roles.

To simplify implementation, you can subsequently modify roles during the technical conception phase, for example, by choosing additional transactions to use activity blocks that have already been created.



Hint:

Note that access to the same transactions and reports is not a sufficient criterion for the existence of an activity block. Since authorizations may vary even at field level, you must implement the different variants of individual activity blocks as separate or derived roles.

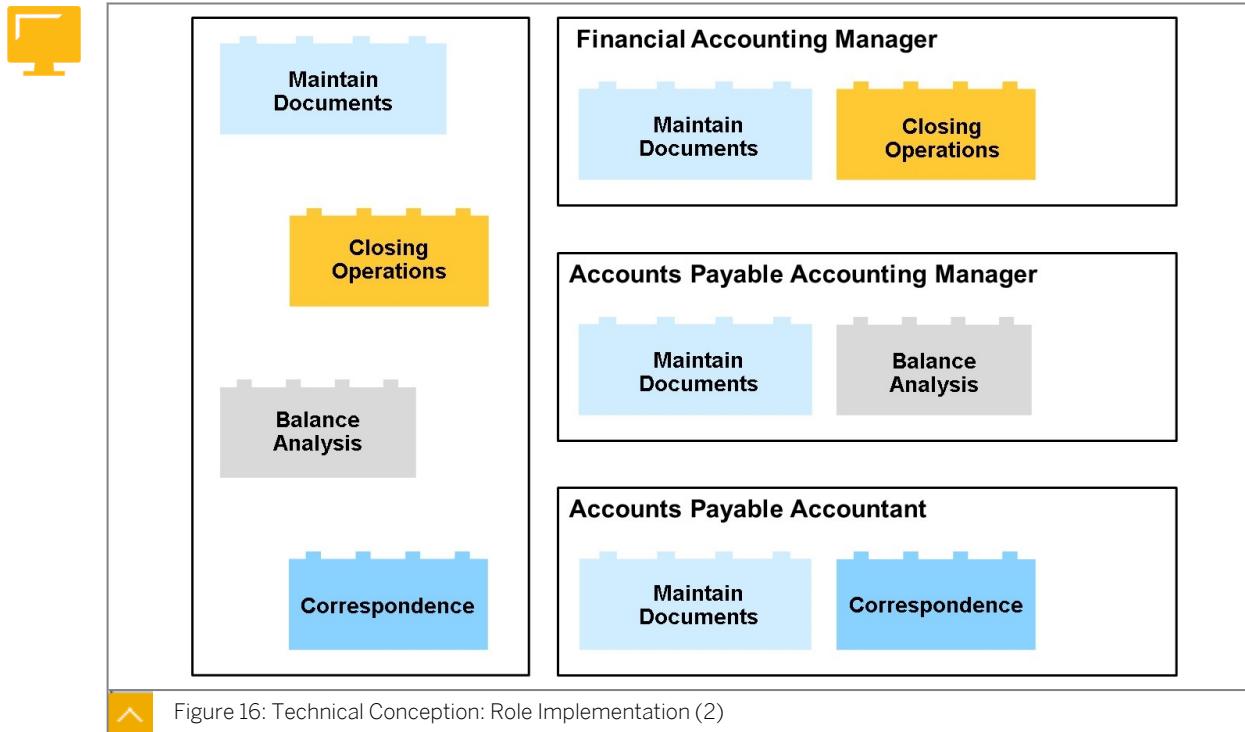


Figure 16: Technical Conception: Role Implementation (2)

During the first conception and implementation approach, individual functions are encapsulated in separate roles (for example, the Basis authorizations of the end-users).

From a technical point of view, all elements of the authorization concept must be assigned a unique identifier. This is why you must define individual naming conventions for all role types.

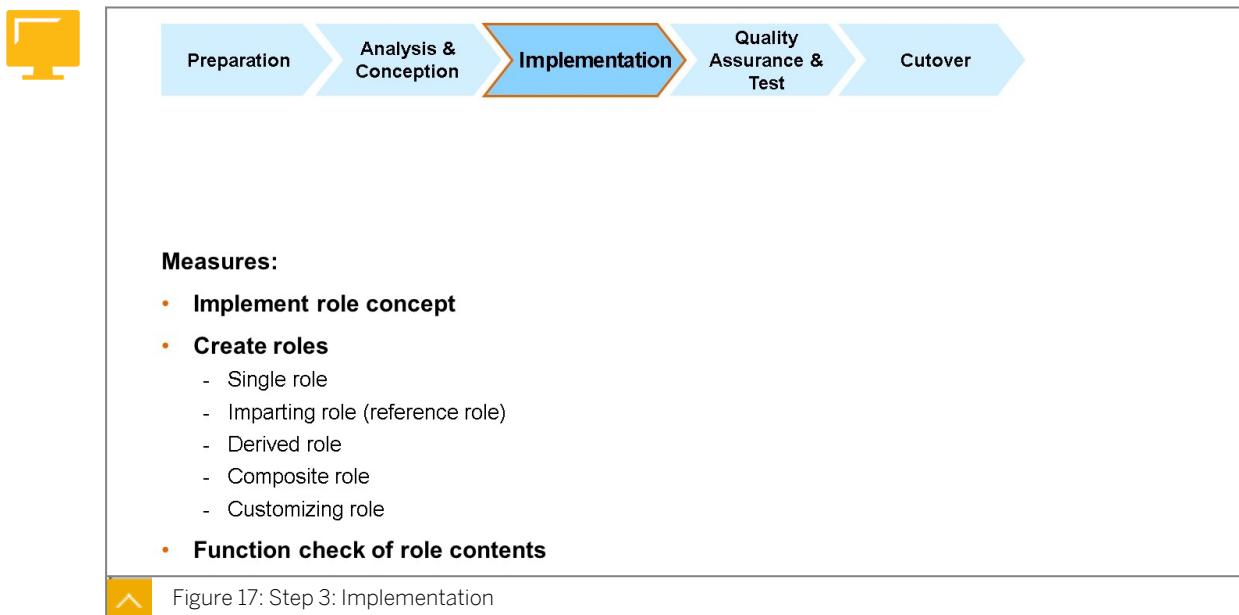
You can define naming conventions based on different criteria, for example, country, business area (FI, CO, and so on), or application component (FI-AP, CO-PA, and so on).

If you want to decentralize user and authorization management, the naming conventions are also required for administrative purposes. In this case, the access rights of the decentralized administrators should be limited to those (composite) roles that belong to a specific business area and thus apply only to a restricted namespace.

Since roles are divided into individual and derived roles, the user roles created in this step may be different from the original specification defined during the development phase. For example, the roles may contain more or fewer activities (transactions and reports). This is why you must check that the roles are properly defined before implementation.

SAP recommends that you carry out a test implementation of the user roles and authorization concept to check the technical conception.

Step 3: Implementation



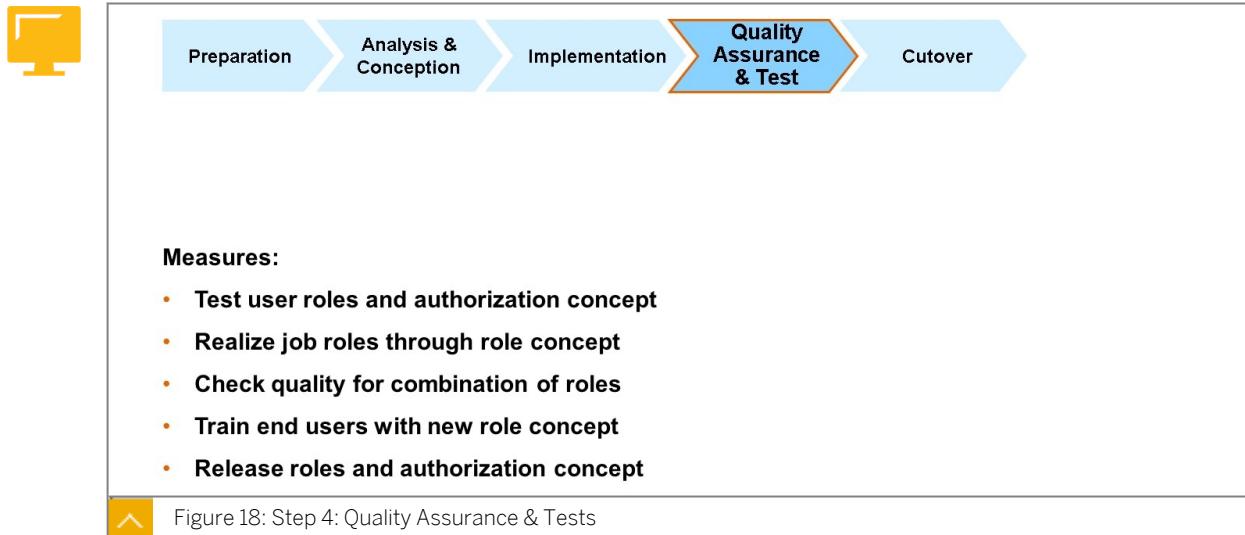
From a technical point of view, user roles (job roles) can be implemented as composite roles using the Role Maintenance. Composite roles consist of individual and composite roles that each contain the relevant authorizations and menu data. Authorizations specify the scope of access to data and functions. User menus use hierarchical structures to specify the access path to the transactions, reports, and Internet pages released for a specific user.

An example of how you create user roles:

- Create individual roles: Individual roles either describe higher-level functions that are independent of organizational or application-specific restrictions or are used as templates for creating derived roles that are not subject to any restrictions.
- Having checked the individual roles used as the derivation basis, you create the derived roles. These contain the desired organizational or application-specific restrictions. For each responsibility area, you create a derived role from an existing individual role.
- Finally, the composite roles are created from the implemented individual and derived roles as the technical counterparts of the user roles.

Step 4: Quality Assurance & Tests

To ensure that productive operation is not affected, it is important to thoroughly test the user roles in connection with the authorizations before you switch over to production. In addition, the responsible area manager must approve of the role and authorization concept implemented.



To standardize the tests, the relevant process flows must be determined and published. You should use predefined test scenarios that cover all business processes implemented.

The test scenarios should include both **positive checks** and **negative checks** of the authorizations of the individual roles. The positive checks must determine whether the functions are executed as desired, while the negative checks must confirm that all restrictions defined are observed. For example, a human resources administrator can display the users for a specific work center, but not the records for other work centers. The test scenarios must cover all functions that are to be performed by a user role.

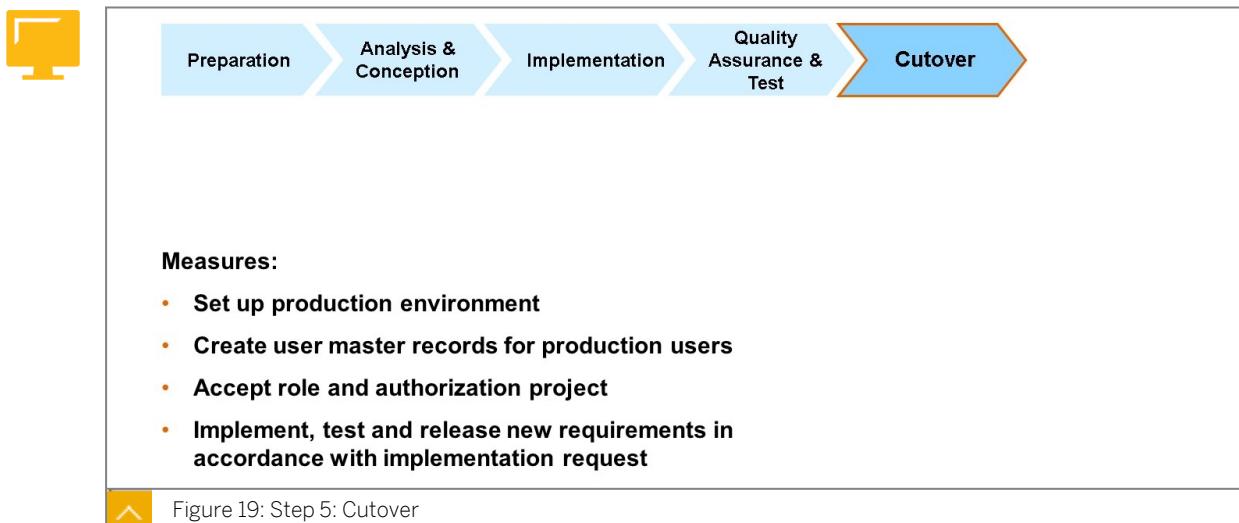
If a function cannot be called during the test, you must correct the user roles and the authorization concept. Note that changes may affect several (derived) roles. In extreme cases, you must revise the entire role and authorization concept.

You may also be required to modify the user menus to simplify access to the functions. To ensure that the system becomes more user-friendly, the project team responsible should closely cooperate with the representatives of the relevant business areas.

After fine-tuning the user roles, you must repeat the tests as often as necessary until the user roles implemented completely comply with the security and usability requirements.

Step 5: Cutover

Before you create the production users, you must create the master records for user management in your production environment, and possibly configure central user administration.



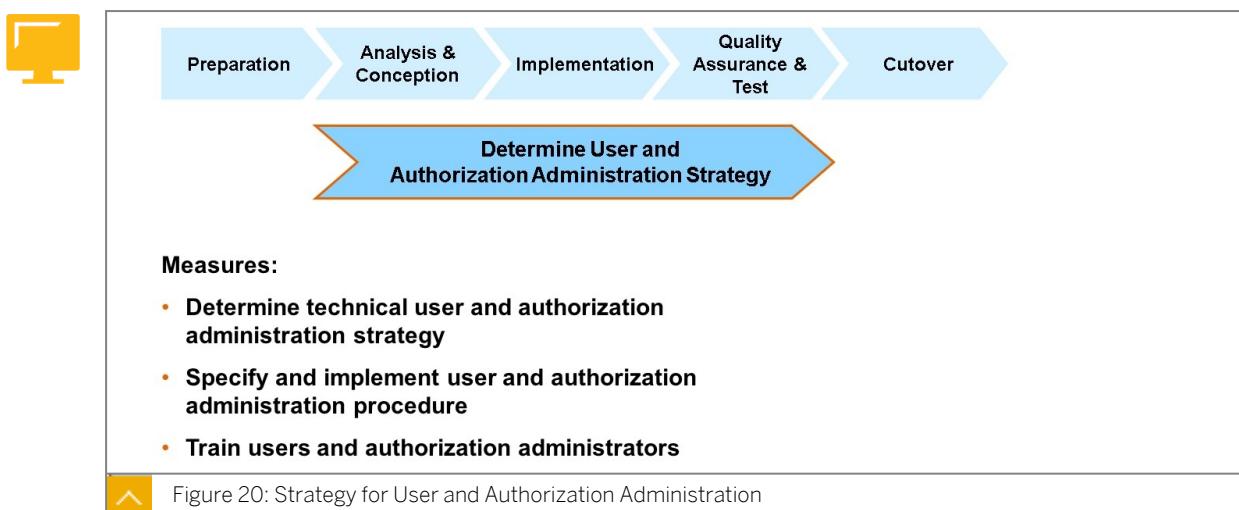
To simplify the creation of the individual user master records, you first create model records. These model records are used as copy templates for the records of the productive users. In the central system, create a user master record for each role specified in the company-wide role matrix (authorization list). If a role is subdivided into several responsibility areas that are subject to organizational restrictions (company code, cost center, plant, and so on) or application-specific control mechanisms (such as FI authorization groups), you must create a separate record for each responsibility area. Maintain the additional data (parameters, printers, and so on).

After consulting the area managers (data owners), define the roles for each user. Consider that some users may have several roles or different roles in various logical systems (clients). Enter the assignments in a user and role matrix.

To create a master record for a user, you copy the model record for the relevant role and customize this record as required.

Get the final approval of the area managers with regard to the users created and communicate all access-relevant data (system, client, ID, and password) to the end users.

Implementing User and Authorization Administration



The SAP environment offers various possibilities for managing users. Users distributed in a far-reaching system landscape can be managed from within a central system. All users are

initially created in a central logical system (client) and then distributed to the other clients in the entire installation.

Before you set up a central user management, you must determine which processes (for example, assigning or locking roles) can be run locally, and if modifications made in local systems (for example, address changes) should be passed on to the central system. Consistent central user management can be set up for such different SAP systems as SAP R/3, APO, and CRM.

After the role and authorization concept is implemented, the members of the project team are normally no longer responsible for managing users and authorizations. Depending on how the tasks are distributed in the company, the users are managed either centrally (for example, using a help desk) or on a decentralized basis (by local location or department administrators). You must assign and train employees for this purpose.

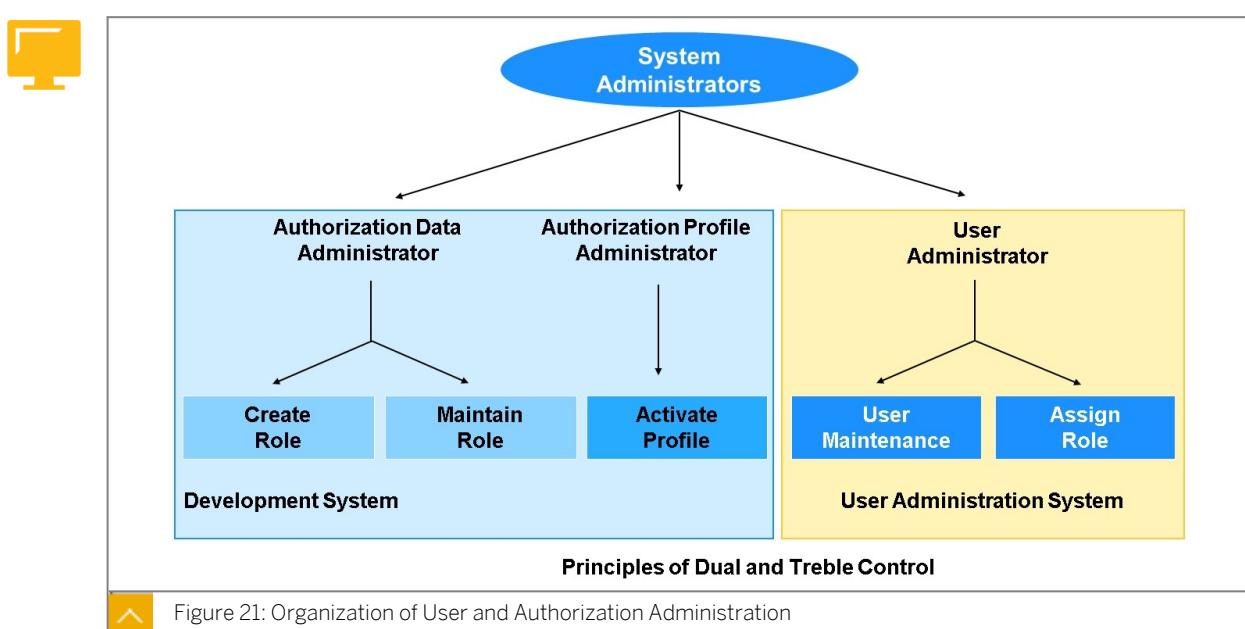


Figure 21: Organization of User and Authorization Administration

The tasks of the authorization administrators include creating, activating, changing, deleting, and transporting roles.

User administrators deal with setting up, changing, deleting, locking, and monitoring users, and assigning passwords and authorizations.

The user and authorization management tasks should be distributed among several administrators (for example, separate user, authorization data, and profile administrators). By dividing the tasks, you ensure that **no single administrator gets full control of user authorizations** (“dual control principle”).

By assigning the user maintenance tasks to local administrators that represent individual departments or locations, you can even further decentralize user and authorization management. Having an administrator on site can also be desirable since first-time users accessing the system often need to be introduced to their task-specific user role. In addition, decentralized administrators are useful for reporting since they know to whom the user IDs refer.

From a technical point of view, decentralization is achieved by subdividing the users into user groups and limiting the rights of the local administrators with regard to the assignment of authorizations. Decentralized administrators may only maintain the users of the group that has been assigned to them. In addition, decentralized administrators should only be allowed

to assign authorizations that are required in their department or at their site in accordance with the naming conventions of user roles.



LESSON SUMMARY

You should now be able to:

- Implement the SAP authorization concept.

Learning Assessment

1. What is the first step in developing a security concept?

Choose the correct answer.

- A Implementing technical protective measures
- B Identifying potential dangers to assets
- C Determining the assets that need to be protected
- D Assessing the skills of security personnel

2. What type of measure involves implementing access authorizations for systems and data?

Choose the correct answer.

- A Organizational measures
- B Technical measures
- C Environmental measures
- D Personal measures

3. When classifying assets, which of the following should be considered?

Choose the correct answer.

- A Cost of insurance for the assets
- B Number of people using the assets
- C Market demand for the assets
- D Consequences of losing the assets

4. What is the main focus during the Project Preparation phase of SAP implementation?

Choose the correct answer.

- A Testing all interfaces and training users
- B Inclusion of all relevant decision-makers and selection of the project team
- C Configuration and fine-tuning of the SAP system
- D Start of SAP production operation

5. Which phase involves configuring and fine-tuning the SAP system?

Choose the correct answer.

- A Project Preparation
- B Business Blueprint
- C Implementation
- D Final Preparation

6. What activities occur during the Final Preparation phase?

Choose the correct answer.

- A Testing interfaces, training users, and migrating business data
- B Determining business requirements and analyzing processes
- C Including decision-makers and selecting project team members
- D Starting SAP production operation

7. What happens during the Go Live & Support phase?

Choose the correct answer.

- A Selection of the internal and external project team members
- B Configuration of the SAP system
- C Start of SAP production operation and ongoing checks
- D Analysis of all business processes

Learning Assessment - Answers

1. What is the first step in developing a security concept?

Choose the correct answer.

- A Implementing technical protective measures
- B Identifying potential dangers to assets
- C Determining the assets that need to be protected
- D Assessing the skills of security personnel

The first step in developing a security concept is determining which assets need to be protected.

2. What type of measure involves implementing access authorizations for systems and data?

Choose the correct answer.

- A Organizational measures
- B Technical measures
- C Environmental measures
- D Personal measures

Access authorizations for systems and data are a form of technical measures.

3. When classifying assets, which of the following should be considered?

Choose the correct answer.

- A Cost of insurance for the assets
- B Number of people using the assets
- C Market demand for the assets
- D Consequences of losing the assets

It's important to consider the consequences of losing the assets when classifying them.

4. What is the main focus during the Project Preparation phase of SAP implementation?

Choose the correct answer.

- A Testing all interfaces and training users
- B Inclusion of all relevant decision-makers and selection of the project team
- C Configuration and fine-tuning of the SAP system
- D Start of SAP production operation

The Project Preparation phase involves the inclusion of all relevant decision-makers and the selection of both internal and external members of the project team.

5. Which phase involves configuring and fine-tuning the SAP system?

Choose the correct answer.

- A Project Preparation
- B Business Blueprint
- C Implementation
- D Final Preparation

The Implementation phase involves configuring and fine-tuning the SAP system.

6. What activities occur during the Final Preparation phase?

Choose the correct answer.

- A Testing interfaces, training users, and migrating business data
- B Determining business requirements and analyzing processes
- C Including decision-makers and selecting project team members
- D Starting SAP production operation

Final Preparation includes testing interfaces, training users, and migrating business data into the SAP system.

7. What happens during the Go Live & Support phase?

Choose the correct answer.

- A Selection of the internal and external project team members
- B Configuration of the SAP system
- C Start of SAP production operation and ongoing checks
- D Analysis of all business processes

The Go Live & Support phase includes the start of SAP production operation and ongoing checking of the benefits

UNIT 2

Understanding Basic Terminology of Authorizations

Lesson 1

Explaining Elements and Terminology of the ABAP Authorization Concept	32
Exercise 1: Practice System Exercise: Display Authorization Information of the Authorization Concept(ABAP)	39

Lesson 2

Identifying Authorization Checks in the SAP System	49
Exercise 2: Practice System Exercise: Check Authorizations in the SAP System	55

UNIT OBJECTIVES

- Understand SAP authorization elements and terminology.
- Identify authorization checks in the SAP System.

Unit 2

Lesson 1

Explaining Elements and Terminology of the ABAP Authorization Concept

LESSON OVERVIEW

This lesson will provide an overview of the terminology for the SAP authorization concept. The classical terms, such as authorization object, authorization field, authorization, and so on, are introduced first. Precisely these terms occur and are used if you use the Role Maintenance for authorization concepts using roles.

Business Example

The SAP authorization concept prevents unauthorized access to the system and to data and objects within the system. Users that are to perform specific functions in the SAP system need a user master record with the relevant authorizations.

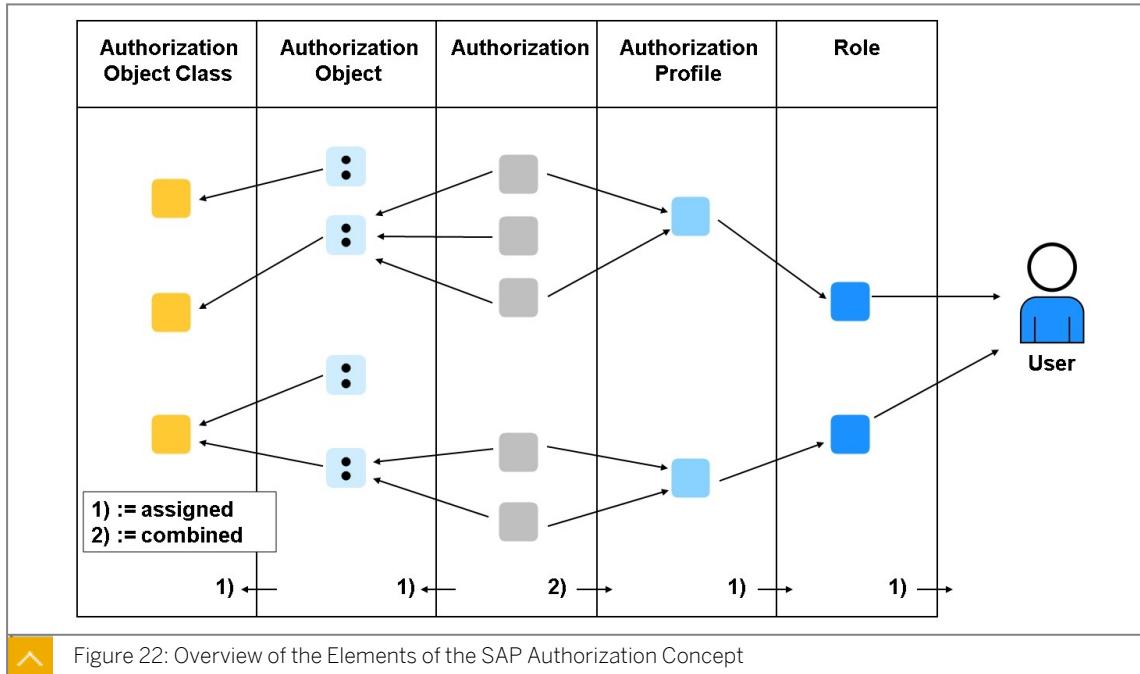


LESSON OBJECTIVES

After completing this lesson, you will be able to:

- Understand SAP authorization elements and terminology.

Overview of the Terms and Elements in the Authorization Concept



Authorization object class: A logical grouping of authorization objects (for example, all authorization objects for object class FI beginning with "F_").

Authorization object: Groups of 1 to 10 authorization fields together. These fields are then checked simultaneously (example: F_LFA1_APP, vendor: application authorization).

Authorization field: The smallest unit against which a check is to be run (ACTVT, APPKZ).

Authorization: An instance of an authorization object, that is, a combination of allowed values for each authorization field of an authorization object.

Authorization profile: Contains instances (authorizations) for different authorization objects.

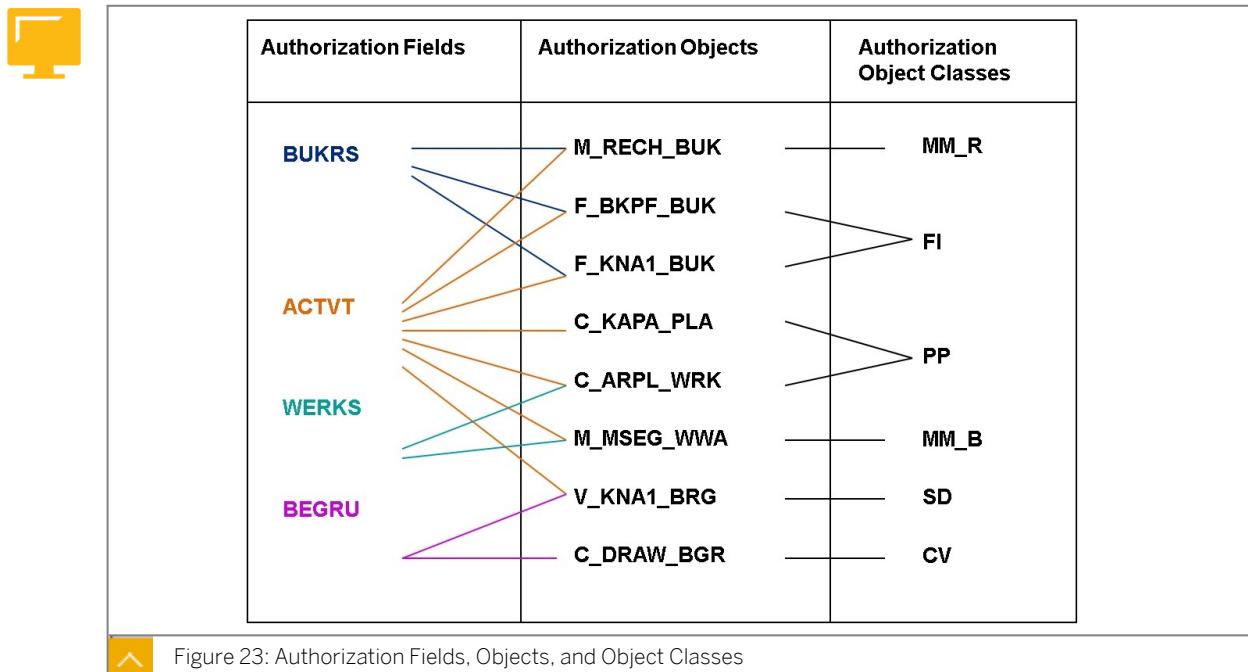
Role: Generated using Role Maintenance (transaction PFCG), and allows the automatic generation of an authorization profile. A role describes the activities of an SAP user.

User/user master record: Used for logging on to SAP systems and grants restricted access to functions and objects of the SAP system based on authorization profiles.

Naming conventions for customer developments (see SAP Notes 20643 and 16466):

- Authorizations and authorization profiles are Customizing objects and must therefore not be in the customer namespace (Y, Z). They must not include an underscore in the second position.
- Authorization classes, objects, and fields are development objects and must begin with Y or Z (customer namespace).

Authorization Fields, Objects, and Object Classes



Example:

The authorization fields **BUKRS** (company code) and **ACTVT** (activity) are used in the following authorization objects, among others:

- **M_RECH_BUK:** Authorization to release blocked invoices for specific company codes.
- **F_BKPF_BUK:** Authorization to edit documents for specific company codes.
- **F_KNA1_BUK:** Assignment of the activities allowed in the company code-specific area of the customer master record.

In the authorizations for each authorization object, you can specify which activities (such as create, change, display, and so on) may be performed in which company code. Each object has a specific number of allowed activities, which are described in the object documentation.

All possible activities (ACTVT) are stored in table **TACT** (transaction SM30).

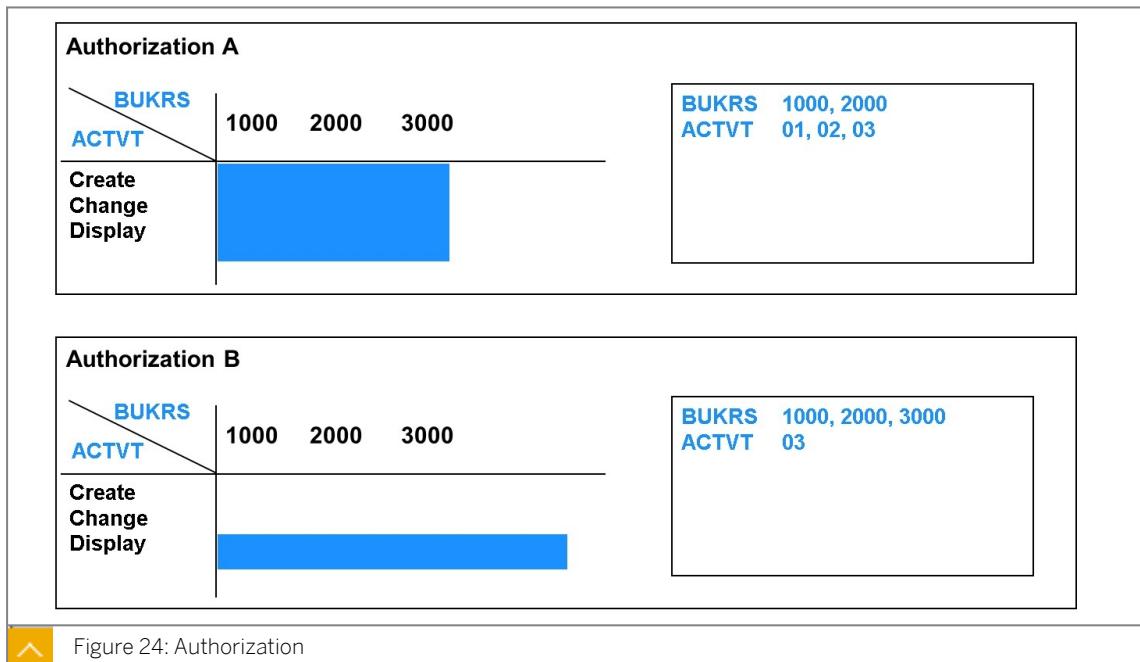
The valid activities for each authorization object can be found in table **TACTZ** (transaction SE16).



Hint:

Every customer can create their own authorization object classes, authorization objects, and authorization fields.

Authorization



Example:

- Authorization “A” allows the user to perform the activities create, change, and display in company codes 1000 and 2000.
- Authorization “B” allows the user to perform only the display activity in company codes 1000, 2000, and 3000.

If the user has authorization “A” and authorization “B”, they work together. This means that the user can perform the create, change, and display activities in company codes 1000 and 2000, but can only perform the display activity in company code 3000.

Authorizations and Authorization Profiles



Authorization Objects	Work Center 1	Work Center 2	Work Center 3
S_TCODE TCD	F-22, FB02	FB02, FB03	FB02, FB03
F_BKPF_BUK ACTVT BUKRS	01, 02, 03 2000	01, 02, 03 1000	03 1000
F_BKPF_GSP ACTVT GSBER	01, 02, 03 1000	01, 02, 03 2000	01, 02, 03 1000, 2000
F_BKPF_KOA ACTVT KOART	01, 02, 03 A, D, S	02, 03 D	01, 02, 03 K

Authorization Profile

Figure 25: Authorizations and Authorization Profiles

You can define several different authorizations for an authorization object. This means that an authorization object has various instances.

Example: Authorization object *F_BKPF_BUK* has the following authorizations:

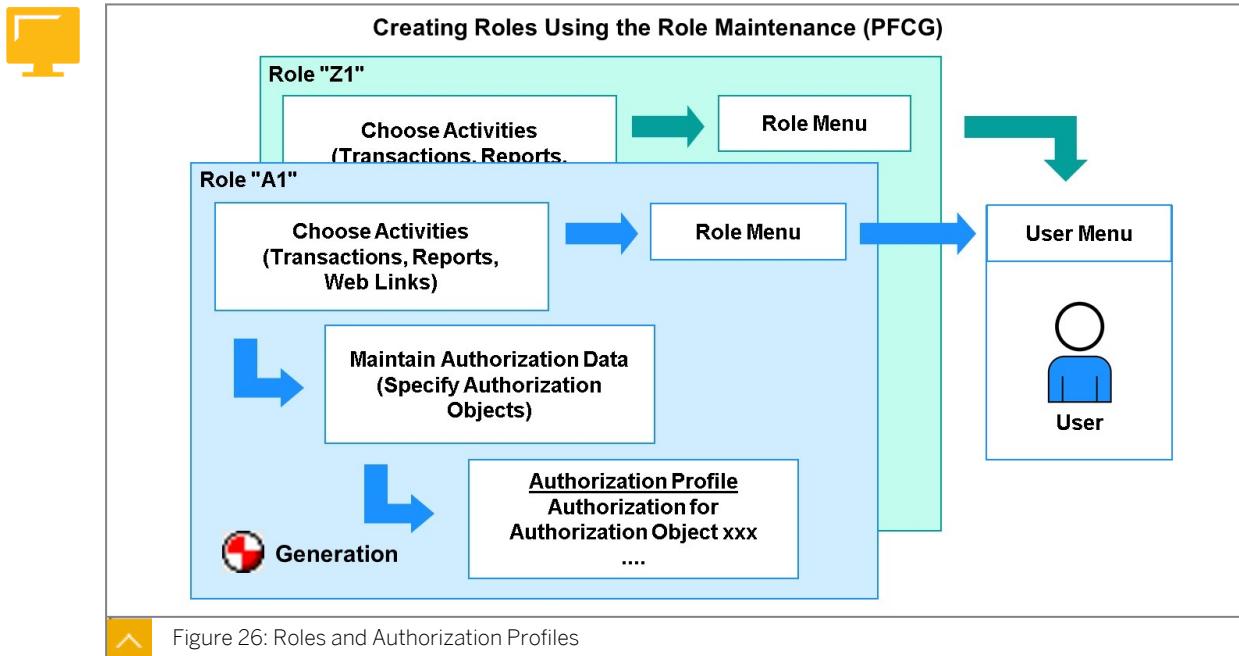
- Work center 1: Authorized to create, change and display documents in company code 2000.
- Work center 2: Authorized to create, change and display documents in company code 1000.
- Work center 3: Authorized to display documents in company code 1000.

You can assign multiple authorizations to a work center. Grouped together, these authorizations are called an authorization profile.

Example: Work center 2 has the following authorization profile:

- Authorization to execute transaction code FB02 and FB03.
- Authorization to create, change, and display documents in company code 1000.
- Authorization to create, change, and display documents in business area 2000.
- Authorization to change and display document items for the accounts receivable account type.

Roles and Authorization Profiles



To provide users with user-specific menus after they have logged on to an SAP system, you use roles. These are defined using Role Maintenance.

A role is a set of functions, also known as **activities**, describing a specific work area. The “Accounts Receivable Accountant” role, for example, contains transactions, reports, and/or Internet/Intranet links that an accountant needs for his or her daily work.

In the role, you organize transactions, reports, or Web addresses in a **role menu**.

A large number of roles (>1200) are delivered with the standard SAP R/3 System. Before you define your own roles, check if one of the user roles delivered as part of the standard SAP R/3 System can be used.



Hint:

Note that the predefined roles are delivered as templates, and begin with the prefix “SAP_”.

For a user to receive authorizations, you must first maintain **authorization data**.

You can then generate the **authorization profile**, and the role is complete.



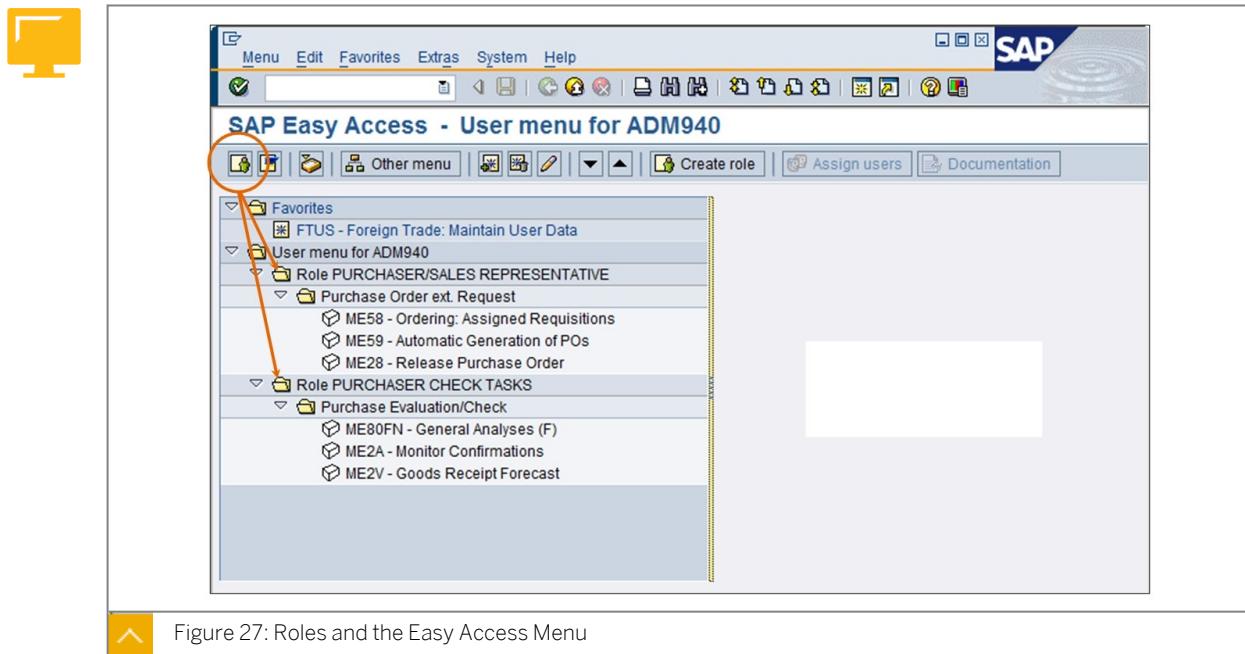
Hint:

SAP strongly recommends the automatic creation of authorization profiles in the form of roles using Role Maintenance. You should only use manual authorization profiles in exceptional cases.

A role can be assigned to any number of users. Through the role, you also assign the authorizations that users need to access the transactions, reports, and so on, contained in the menu.

This **user menu** appears when the user to which the authorization profile was assigned logs on to the SAP system. A user menu consists of the role menus of the assigned roles. It contains the activities that are required by a group of users for their work area.

Roles and the Easy Access Menu



The new **SAP Easy Access** menu provides a user-specific point of entry into the SAP system.

The user menu (created from multiple role menus) contains only those transactions, reports, and Web addresses needed by the users for their daily work processes.

The user menus can be and are often created with Role Maintenance using composite roles.

For users with system administrator authorization, the **SAP Easy Access** menu provides some additional functions for:

- Creating roles
- Calling menus for roles and assigning them to users

To use these extended functions, you need authorizations for the following authorization objects:

authorization object	Value
S_USER_TCD	PFCG
S_USER_PRO	*
S_USER_AUT	*
S_USER_GRP	*

Unit 2

Exercise 1

Practice System Exercise: Display Authorization Information of the Authorization Concept(ABAP)

Task 1: Access the Training System Landscape

Log in to your training landscape and log on to your training system.

1. Log in to your Training Landscape
Follow the guidance of your instructor.
2. Log on to the SAP GUI on the training system T41 as user ADM940-##.
 - a. Start SAP Logon.
 - b. Select system T41 and choose Log On.
 - c. Enter **ADM940-##** in the User field.
 - d. Enter the initial password **Welcome1** in the Password field.
 - e. Enter your log-on language (**EN** or **DE**) in the Language field.
 - f. Choose Enter.
 - g. Enter a password of your choice in the New Password and the Repeat Password fields.
 - h. Choose Transfer (Enter).
 - i. Choose Continue (Enter).

Task 2: Display the Master Record of User ADM940-##.

Display the master record of user ADM940-##.

1. Are roles assigned to the user? If yes, which ones?

_____ ,
_____ ,
_____ ,
_____ .

2. Is an authorization profile assigned to the user? If yes, which one/s?

_____ ,
_____ ,
_____ .

Task 3: Display the Details for an Authorization Profile

1. Display the details for the authorization profile for role ADM940_PLUS.



Hint:

Double-click the profile name to go to the detail screen of the authorization profile.

Expand the tree structure of the authorization profile.

Do you have authorizations for the following authorization objects?

- F_BKPF_BUK? _____
- PLOG? _____
- S_TCODE? _____
- S_USER_GRP? _____

From the detail screen of the authorization profile, go back to the display of the user master record.

Exit the transaction.

2. Which authorization fields does the object S_USER_GRP consist of?

3. Which authorization values do you have for the authorization object S_USER_GRP?

Authorization combination 1:

Field 1) _____ Field 2) _____

Authorization combination 2:

Field 1) _____ Field 2) _____

Task 4: Analyze Authorization Objects Using the User Information System

Display various authorization information in the User Information System.

1. Navigate to the User Information System in the SAP Menu.
2. Select the authorization object S_USER_GRP.
3. To which authorization object class is the authorization object S_USER_GRP assigned?
4. Display the documentation for this authorization object and find out in which transactions the authorization object is checked, and what activities are possible.

In which transactions is the authorization object checked?

; _____ ; _____ ;

; _____ ; _____ ; _____ ;

What activities are possible?

; _____ ; _____ ; _____ ;

; _____ ; _____ ; _____ ;

5. Search for authorization whose names begin with S_USER?

6. How many authorization objects have a name that begins with S_USER?

7. Find out about the authorization object S_USER_TCD by displaying the documentation.
What is controlled with this authorization object?

Which authorization field(s) does the object consist of?

Task 5: Analyze the Role ADM940_SD_SALES Using the User Information System

1. Navigate to the User Information System in the SAP Menu.
2. Use Report *Roles by Complex Selection Criteria node → By Role Name* with the role ADM940_SD_SALES.
3. Display the transaction assignment for the role.

Do these roles allow you to start transactions that start with "X"?

Does this role provide authorization to call transaction VA03?

Does this role provide authorization to call transaction MM03?

Practice System Exercise: Display Authorization Information of the Authorization Concept(ABAP)

Task 1: Access the Training System Landscape

Log in to your training landscape and log on to your training system.

1. Log in to your Training Landscape
Follow the guidance of your instructor.
2. Log on to the SAP GUI on the training system T41 as user ADM940-##.
 - a. Start SAP Logon.
 - b. Select system T41 and choose Log On.
 - c. Enter **ADM940-##** in the User field.
 - d. Enter the initial password **Welcome1** in the Password field.
 - e. Enter your log-on language (**EN** or **DE**) in the Language field.
 - f. Choose Enter.
 - g. Enter a password of your choice in the New Password and the Repeat Password fields.
 - h. Choose Transfer (Enter).
 - i. Choose Continue (Enter).

Task 2: Display the Master Record of User ADM940-##.

Display the master record of user ADM940-##.

1. Are roles assigned to the user? If yes, which ones?

- a) **SAP Menu:** Tools → Administration → User Maintenance → Users, “SU01”.

Enter ADM940-## and choose *Display (F7)*.

- b) Select the *Roles* tab page.

Yes:

ADM940_DEMO_MENU

ADM940_DISPLAY
ADM940_PLUS
ADM940_USER

2. Is an authorization profile assigned to the user? If yes, which one/s?

_____ ,
_____ ,
_____ ,

- a) Choose the *Profiles* tab page.

Yes:

Profile for role ADM940_DISPLAY (many)

Profile for role ADM94_PLUS

Profile for role ADM94_USER

Task 3: Display the Details for an Authorization Profile

1. Display the details for the authorization profile for role ADM940_PLUS.



Hint:

Double-click the profile name to go to the detail screen of the authorization profile.

Expand the tree structure of the authorization profile.

Do you have authorizations for the following authorization objects?

- F_BKPF_BUK? _____
- PLOG? _____
- S_TCODE? _____
- S_USER_GRP? _____

From the detail screen of the authorization profile, go back to the display of the user master record.

Exit the transaction.

- a) Double-click the profile name to go to the detail screen of the authorization profile.

Expand the tree structure of the authorization profile.

Authorization for authorization object:

- F_BKPF_BUK? No.
- PLOG? No.
- S_TCODE? Yes.
- S_USER_GRP? Yes.

2. Which authorization fields does the object S_USER_GRP consist of?

- a) Authorization fields for the authorization object S_USER_GRP:
ACTVT Activity
CLASS User group in user master maintenance

3. Which authorization values do you have for the authorization object S_USER_GRP?
Authorization combination 1:
Field 1) _____ Field 2) _____
Authorization combination 2:
Field 1) _____ Field 2) _____

a) Authorization values for the authorization object S_USER_GRP:
Authorization combination 1 :
Field 1: ACTVT: **05**, Field 2: CLASS: **Z***.
Authorization combination 2 :
Field 1: ACTVT: **03, 08**, Field 2: CLASS: *****.

b) From the detail screen of the authorization profile, go back to the display of the user master record.

c) Exit the transaction.

Task 4: Analyze Authorization Objects Using the User Information System

Display various authorization information in the User Information System.

1. Navigate to the User Information System in the SAP Menu.
 - a) SAP Menu: → *Tools* → *Administration* → *User Maintenance* → *Information System* folder.
 2. Select the authorization object S_USER_GRP.
 - a) Expand the structure for the *Authorization Objects* node, and select the report *Authorization Objects - By Object Name, Text* by double-clicking it.
 - b) Enter **S_USER_GRP** in the *Authorization Object* field.
 - c) Choose *Execute (F8)*.
 - d) Double click Object *S_USER_GRP*.
 3. To which authorization object class is the authorization object S_USER_GRP assigned?
 - a) You are in the pop up: *Display Authorization Object*. Which content has the field Class? The Authorization object class for authorization object S_USER_GRP is: **BC_A**, Basis Administration.
 4. Display the documentation for this authorization object and find out in which transactions the authorization object is checked, and what activities are possible.

What activities are possible?

_____ ; _____ ; _____ ; _____ ; _____ ; _____ ;

- a) Select the authorization object and choose the *Display Object Documentation* button.
- b) Transactions with integrated check of S_USER_GRP:
“SU01”, “SU10”, “SU12”, “PFCG”, “SUUM”, “SUUMD”.
- c) Possible values for the Activity field:
- 01: Create
 - 02: Change
 - 03: Display
 - 05: Lock, Unlock
 - 06: Delete
 - 08: Display Change Documents
 - 22: Add Users to Roles
 - 24: Archive
 - 36: Extended Maintenance
 - 50: Move
 - 78: Assign
 - 68: Model
 - PP: Set Productive Password
 - F4: Address data display in input help
- d) Exit the report *Authorization Objects by Object Name, Text* and go back to the SAP Easy Access menu.
5. Search for authorization whose names begin with S_USER?
- a) In the Information System, under the *Authorization Objects* node, double-click the report *Authorization Objects - By Object Class*.
 - b) Choose the *All Selections* icon (Shift+F7).
 - c) Enter **S_USER*** in the *Authorization Object* field.
 - d) Enter **BC_A** in the *Object class* field.
 - e) Choose *Execute (F8)*.
6. How many authorization objects have a name that begins with S_USER?
-
- a) Analyze the list of authorization objects.
Number of authorization objects that begin with S_USER:
17 Authorization objects
7. Find out about the authorization object S_USER_TCD by displaying the documentation.
What is controlled with this authorization object?
-
-
-

Which authorization field(s) does the object consist of?

-
- a) In line with the authorization object **S_USER_TCD**, double-click the *Information button* (*i*).
 - b) Read the displayed information.

Definition for authorization object **S_USER_TCD**:

Authorization objects control the transactions that system administrators can assign to a role, as well as the transactions for which they can assign transaction code authorization (object S_TCODE). Note that in the Profile Generator, you can only maintain intervals of transactions if you have full authorization S_USER_TCD for authorization object S_TCODE. Otherwise you can only maintain individual values for the object S_TCODE.

Defined fields:

TCD: Transactions that administrators may assign to roles and for which they may assign authorization to start a transaction in Role Maintenance.

- c) Exit the report and return to the SAP Easy Access menu.

Task 5: Analyze the Role ADM940_SD_SALES Using the User Information System

1. Navigate to the User Information System in the SAP Menu.
 - a) SAP Menu: → Tools → Administration → User Maintenance → Information System folder.
2. Use Report *Roles by Complex Selection Criteria node* → *By Role Name* with the role **ADM940_SD_SALES**.
 - a) Expand the structure for the *Roles* node, then expand the structure for the *Roles by Complex Selection Criteria node*, and choose the report *By Role Name* by double-clicking it.
 - b) Enter **ADM940_SD_SALES** in the *Role* field.
 - c) Choose *Execute (F8)*.
3. Display the transaction assignment for the role.

Do these roles allow you to start transactions that start with “X”?

Does this role provide authorization to call transaction **VA03**?

Does this role provide authorization to call transaction **MM03**?

-
- a) Display the transaction assignment of the role by selecting the line with the role name and choosing the button *Transaction Assignments* (Ctrl+Shift+F6).

Do these roles allow you to start transactions that start with “X”?

Yes.

There are three transactions (XD01; XD02; XD03).

Does this role provide authorization to call transaction VA03?

Yes.

Does this role provide authorization to call transaction MM03?

No.

- b) Exit the report and return to the initial Information System screen.



LESSON SUMMARY

You should now be able to:

- Understand SAP authorization elements and terminology.

Identifying Authorization Checks in the SAP System

LESSON OVERVIEW

This lesson will use an example to introduce the checking of authorizations in an SAP system. There are essentially two checks. The first check is performed by the system when transactions are called, and the second is then performed by checks in the program. The user buffer, which is also introduced, plays a vital role in the check.

Business Example

Authorization checks are performed under various conditions in the SAP system. In this way, there is, for example, a mandatory kernel check for each transaction start. The main task, however, in the company, is to control the checks in programs. To do this, it is very important to understand the relationship between the buffer and the authorization check.

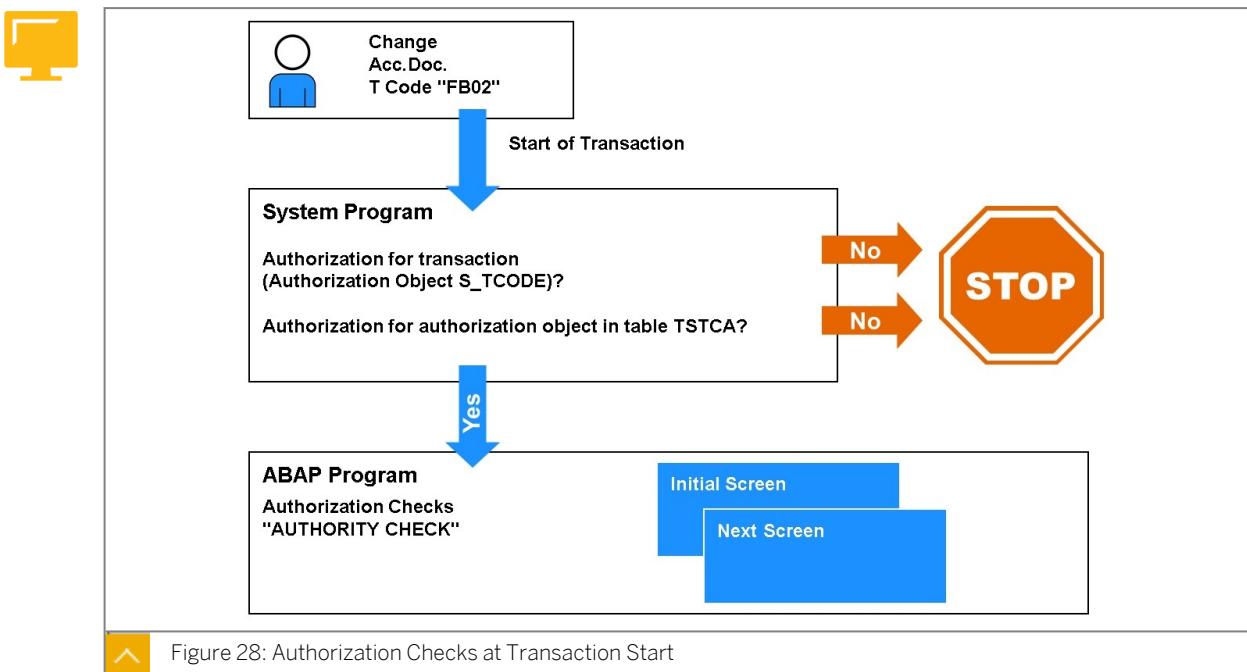


LESSON OBJECTIVES

After completing this lesson, you will be able to:

- Identify authorization checks in the SAP System.

Authorization Checks When Applications Are Started and in Programs



Authorization Checks When Applications Are Started

When starting applications (transaction, Web Dynpro application), authority checks are performed.

Start Authorization Checks

The start authorization checks are available for the following applications:



- SAP transactions (authorization object S_TCODE)
- Web Dynpro ABAP application (authorization object S_START)
- RFC function modules (authorization object S_RFC)
- SAP Fiori applications (authorization object S_SERVICE)

SAP Transactions (Authorization Object S_TCODE)

When starting a transaction, a system program executes a series of checks to ensure that the user has the appropriate authorizations.

Step 1: Check if the user is authorized to start the transaction. Authorization object *S_TCODE* (transaction start) contains the authorization field *TCD* (transaction code). The user must have the authorization for the transaction code that he or she wants to run (such as "FB02", Change Document).

Step 2: Check if an authorization object is assigned to the transaction code. If this is the case, the system checks if the user has an authorization for this authorization object. The transaction code / authorization object assignment is stored in table **TSTCA**.

If any of the above steps fail, the transaction does not begin, and the user receives a message.



Hint:

The ABAP statement *authority-check* is used to check the authorization object assigned to the transaction. The check is performed during transaction start by the ABAP program called by the transaction.

Web Dynpro ABAP Application (Authorization Object S_START)

Similar to the authorization object *S_TCODE* (for transactions), you use the authorization object *S_START* during the start authorization check of Web Dynpro ABAP applications. It has the three fields *AUTHPGMID*, *AUTHOBJTYP*, and *AUTHOBJNAM*, which correspond to the key fields *PGMID*, *OBJECT*, and *OBJ_NAME* of the object catalog (table *TADIR*). During the start authorization check, the key of the object catalog entry of the Web Dynpro ABAP application is therefore checked by the Web Dynpro ABAP runtime. For example: If you start the Web Dynpro ABAP application ABC, you require an authorization for the object *S_START* with the values *AUTHPGMID* = "R3TR", *AUTHOBJTYP* = "WDYA" and *AUTHOBJNAM* = "ABC".

This start authorization check is inactive when delivered and must be activated as described in SAP Note 1413011 - New start authorization check for Web Dynpro ABAP.

If you activate the start authorization check, you can use authorizations to control exactly which Web Dynpro ABAP applications that users can execute.

RFC Function Modules (Authorization Object S_RFC)

When starting RFC-enabled function modules, authorization object *S_RFC* is used to check the start authorization.

The authority object S_RFC has the key fields REC_TYPE, REC_NAME, and ACTVT. The authority object S_RFC can be maintained for function groups (REC_TYPE = FUGR) and function modules (REC_TYPE = FUNC).

At run time, the first check is for the function group executed. If this check fails, a second check for the function module is executed.



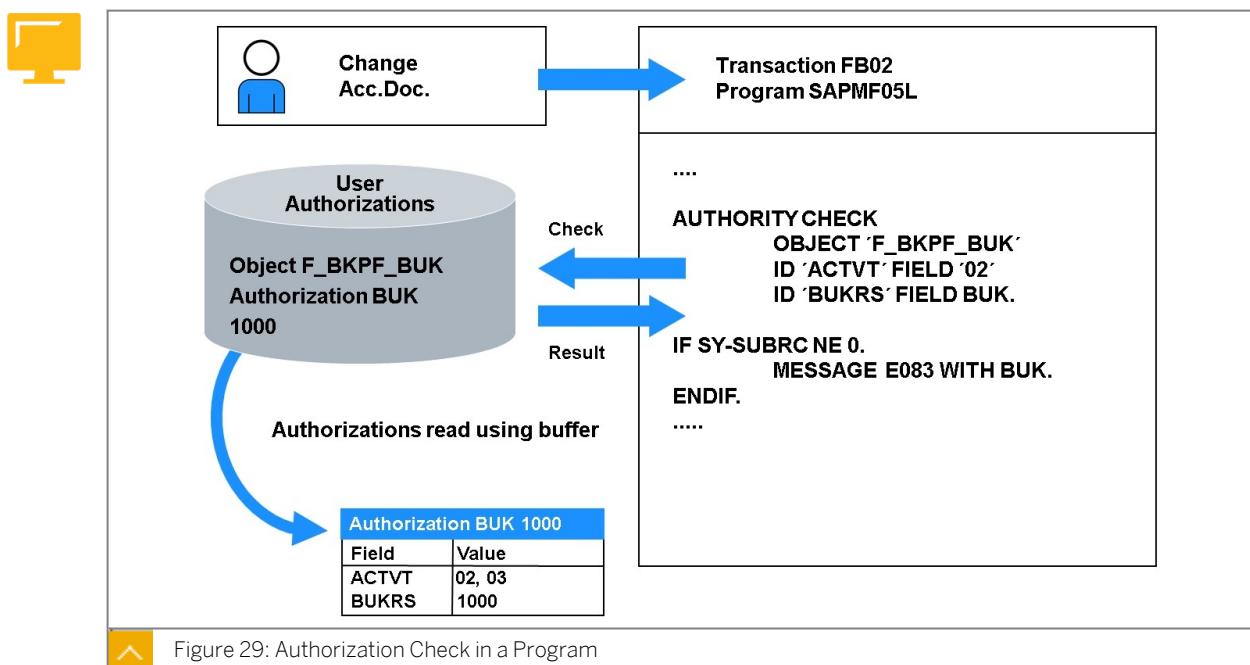
Note:

The authority check is performed only once with the first execution of the function module for the particular RFC session.

SAP Fiori Applications (Authorization Object S_SERVICE)

Start authorizations for the activated OData services to launch a certain SAP Fiori app. You find the service(s) used per app in the app-specific documentation in the section SAP Fiori Apps.

Authorization Checks in Programs



Authorization checks in programs are performed using the ABAP command *authority-check*.

A program may contain any number of authorization checks.

Example: The user wants to call transaction FB02. An *authority-check* is coded in the ABAP program SAPMF05L, which transaction FB02 calls. The following authorization is checked:

- Authorization object *F_BKPF_BUK*
- Authorization field *ACTVT* (activity) for the value “02” (change)
- Authorization field *BUKRS* (company code) for value “1000”

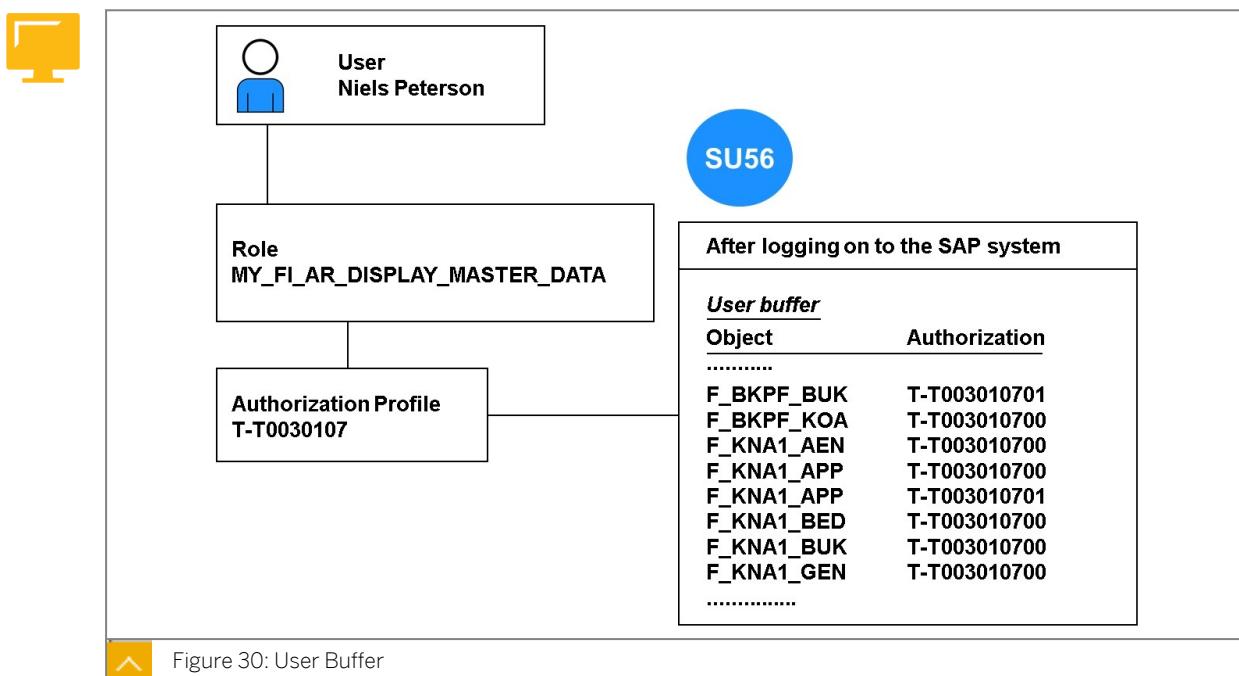
Only if the user has the authorization object *F_BKPF_BUK* with the authorization fields *ACTVT* (“02”) and *BUKRS* (“1000”) as authorization is he or she allowed to perform the transaction.

After the authorization check, the system gives back a return code. The valid return codes for the **authority-check** command are:

- **0:** The user has the authorization for the authorization object with the correct field values.
- **4:** The user has an authorization for the authorization object, but the values checked are not assigned to the user.
- **12:** The user does not have any authorizations for the authorization object.
- **16:** No profile is entered in the user master record.

The values that are returned by the program check depend on the user buffer. It decides which authorizations are available to the user and which are not.

User Buffer



When a user signs on to an SAP system, a user buffer is built containing all authorizations for the user. Each user has his or her own user buffer.

If Mr. Peterson (example from the figure) logs on to the system, his user buffer contains all authorizations that were assigned to the role **MY_FL_AR_DISPLAY_MASTER_DATA** using the profile.



Hint:

Every user can display **his or her own** user buffer using transaction SU56.

If you have some additional administrator rights, you can also view the buffers of colleagues. This is indicated most clearly if you can see the icon *Display for Different User/Authorization Object (F5)* in "SU56".

A user would fail an authorization check if:

- The authorization object does not exist in the buffer.

- The values checked by the application are not assigned to the authorization object in the user buffer.

Unit 2

Exercise 2

Practice System Exercise: Check Authorizations in the SAP System

Business Example

In practice, it is important to know the special features of the authorization check performed when a transaction is called in the system. It is also important to determine, if an unsuccessful authorization check is reported, why it was unsuccessful. This exercise will consolidate the content of the lesson with work in the system.

Task 1: Display the Definition of a Transaction

Display the definition of transaction FB03.

1. Start the transaction MAINTAIN TRANSACTION (SE93).
2. Which authorization object is checked when the transaction is called?
Authorization object: _____
3. Which authorization values must exist for the authorization check to be positive and the transaction to be started?

Task 2: Display Authorization Data for User

Log on to the system with user “ADM940-SU53” (password: ADM940). Then call transaction VA07 by entering the transaction code in the command line or by choosing the following **menu path**: SAP Menu → Logistics → Sales and Distribution → Sales → Information System → Worklists → Compare Sales - Purchasing (Order).

1. Log on to the system with user “ADM940-SU53” (password: ADM940).
2. Log on to the system as user “ADM940-SU53”.
3. Call transaction VA07
4. Can you call the transaction?

-
5. What message is returned by the system?

-
6. Find out which object was checked, and what authorizations you have.

Use transaction SU53 to find out which object was checked, and what authorizations you have.

-
7. Test the remote call using your ADM940-## user.

Task 3: Analyze Authorization in the User Buffer

Describe the user buffer and display it for user “ADM940-SU53”.

1. What do you see in the user buffer? Describe its content.

2. How can you call the user buffer?

3. Display the buffer for your user “ADM940-SU53”. How many authorization entries does this user have?

4. Log off as user ADM940-SU53.

Unit 2 Solution 2

Practice System Exercise: Check Authorizations in the SAP System

Business Example

In practice, it is important to know the special features of the authorization check performed when a transaction is called in the system. It is also important to determine, if an unsuccessful authorization check is reported, why it was unsuccessful. This exercise will consolidate the content of the lesson with work in the system.

Task 1: Display the Definition of a Transaction

Display the definition of transaction FB03.

1. Start the transaction MAINTAIN TRANSACTION (SE93).
 - a) Choose **Menu path:** SAP Menu → Tools → ABAP Workbench → Development → Other Tools → Transactions (SE93).
 - b) Enter **FB03** in the *Transaction Code* field.
 - c) Choose *Display*.
 2. Which authorization object is checked when the transaction is called?
Authorization object: _____
 - a) Take the value from the *Authorization Object* field.
Authorization object: F_BKPF_BUK
 3. Which authorization values must exist for the authorization check to be positive and the transaction to be started?

 - a) Choose the *Values* button.
Activity: 03
The company code is not checked here, so it does not matter which authorization values exist in the user master record for it.
- #### Task 2: Display Authorization Data for User
- Log on to the system with user “ADM940-SU53” (password: ADM940). Then call transaction VA07 by entering the transaction code in the command line or by choosing the following **menu path:** SAP Menu → Logistics → Sales and Distribution → Sales → Information System → Worklists → Compare Sales - Purchasing (Order).
1. Log on to the system with user “ADM940-SU53” (password: ADM940).
 2. Log on to the system as user “ADM940-SU53”.
 - a) Start SAP Logon.

- b) Select system **T41** and choose *Log On*.
 - c) Enter the user name **ADM940-SU53** in the *User* field.
 - d) Enter **ADM940** in the *Password* field.
 - e) Choose *Enter*.
3. Call transaction **VA07**
- a) Enter the transaction code in the command line or by choosing the following **menu path**: SAP Menu → Logistics → Sales and Distribution → Sales → Information System → Worklists → Compare Sales - Purchasing (Order).
4. Can you call the transaction?

a) No.

5. What message is returned by the system?
-

a) "You are not authorized to use transaction VA07"

6. Find out which object was checked, and what authorizations you have.

Use transaction **SU53** to find out which object was checked, and what authorizations you have.

a) Enter the transaction code **SU53** in the command line.

The object "S_TCODE" was checked, and your user had no authorizations for Object S_TCODE field TCD Value1 VA07.

- b) Double-click the row indicating the missing authorization for transaction VA07.
- c) Select the node *User's Authorization Data ADM940-SU53* and choose *Expand Subtree (F6)*.

The column Authorization Values shows that your user has the following authorizations for Object S_TCODE field TCD:

SESS, SESSION_MANAGER, SMEN, SSC1, SU3, SU53, and SU56 .

7. Test the remote call using your **ADM940-##** user.

- a) To do this, use your **ADM940-##** user to call **SU53**; then use the icon "*User (F5)*" for the remote call of **SU53** for a different user.

Task 3: Analyze Authorization in the User Buffer

Describe the user buffer and display it for user "**ADM940-SU53**".

1. What do you see in the user buffer? Describe its content.
-
-
-
-

- a) The user buffer has the following meaning:

Each user has his or her own user buffer, in which all authorizations that are assigned to the user are listed. This list is arranged by Object/Authorization/Object Text.

2. How can you call the user buffer?

a) With transaction SU56.

3. Display the buffer for your user “ADM940-SU53”. How many authorization entries does this user have?

a) Start transaction SU56.

b) The number of entries is 6.

- S_TCODE
- S_USER_AGR
- S_USER_AUT
- S_USER_GRP
- S_DEVELOP
- S_OC_SEND

4. Log off as user ADM940-SU53.

a) In the session for user ADM940-SU53, choose *System → Log Off* in the menu.



LESSON SUMMARY

You should now be able to:

- Identify authorization checks in the SAP System.

Learning Assessment

1. What is the primary purpose of defining roles in an SAP system?

Choose the correct answer.

- A To restrict user access to the system entirely
- B To generate real-time business reports
- C To provide user-specific menus and authorizations after they log on to the SAP system
- D To back up data in the SAP system

2. What should you do before defining your own roles in an SAP system?

Choose the correct answer.

- A Generate the authorization profile immediately.
- B Check if a suitable user role already exists in the standard SAP R/3 System.
- C Assign the role to users without authorization.
- D Organize transactions and reports arbitrarily.

3. What is required to complete a role so that users can access transactions, reports, and other menu items?

Choose the correct answer.

- A Direct coding in the SAP system
- B Deletion of previous user roles
- C Removal of authorization constraints
- D Maintenance of authorization data and generation of the authorization profile

4. What command is used in ABAP programs to perform authorization checks?

Choose the correct answer.

- A CHECK-USER
- B AUTH-CHECK
- C AUTHORITY-CHECK
- D USER-AUTH-CHECK

5. Why might a user fail an authorization check?

Choose the correct answer.

- A Incorrect SAP GUI version
- B System downtime
- C The authorization object does not exist in the user's buffer
- D Network issues

Learning Assessment - Answers

1. What is the primary purpose of defining roles in an SAP system?

Choose the correct answer.

- A To restrict user access to the system entirely
- B To generate real-time business reports
- C To provide user-specific menus and authorizations after they log on to the SAP system
- D To back up data in the SAP system

Roles in an SAP system are designed to provide specific menus and authorizations tailored for user requirements.

2. What should you do before defining your own roles in an SAP system?

Choose the correct answer.

- A Generate the authorization profile immediately.
- B Check if a suitable user role already exists in the standard SAP R/3 System.
- C Assign the role to users without authorization.
- D Organize transactions and reports arbitrarily.

It is essential to verify if an existing role fits your needs before defining new ones to save time and effort.

3. What is required to complete a role so that users can access transactions, reports, and other menu items?

Choose the correct answer.

- A Direct coding in the SAP system
- B Deletion of previous user roles
- C Removal of authorization constraints
- D Maintenance of authorization data and generation of the authorization profile

Maintaining authorization data and generating the authorization profile are crucial steps to complete a role in SAP.

4. What command is used in ABAP programs to perform authorization checks?

Choose the correct answer.

- A CHECK-USER
- B AUTH-CHECK
- C AUTHORITY-CHECK
- D USER-AUTH-CHECK

The AUTHORITY-CHECK command is used in ABAP programs to perform authorization checks.

5. Why might a user fail an authorization check?

Choose the correct answer.

- A Incorrect SAP GUI version
- B System downtime
- C The authorization object does not exist in the user's buffer
- D Network issues

A user would fail an authorization check if the authorization object does not exist in the buffer, or the necessary values are not assigned in it.

UNIT 3

Creating Users

Lesson 1

Maintaining and Evaluating User Data	66
Exercise 3: Practice System Exercise: Maintain and Evaluate User Data	83

Lesson 2

Understanding the Business User Concept	93
Exercise 4: Practice System Exercise: Create a user master record for a business user	101

UNIT OBJECTIVES

- Manage user data and the user master record.
- Understand the Business User Concept.

Maintaining and Evaluating User Data

LESSON OVERVIEW

This lesson will provide you with an overview of how to use the user master record to identify a user. First, the SAP user types are explained. The components of the user master record are then discussed. The functions of mass maintenance and change documentation are clarified.

Business Example

To access the SAP system and work in the system, a user master record with authorizations is required. Other elements of the user master record make it easier to work with the SAP system. The assignment of these authorizations can be controlled individually for each user, but also, to an extent, using mass maintenance.



LESSON OBJECTIVES

After completing this lesson, you will be able to:

- Manage user data and the user master record.

The User Master Record and its Tab Pages

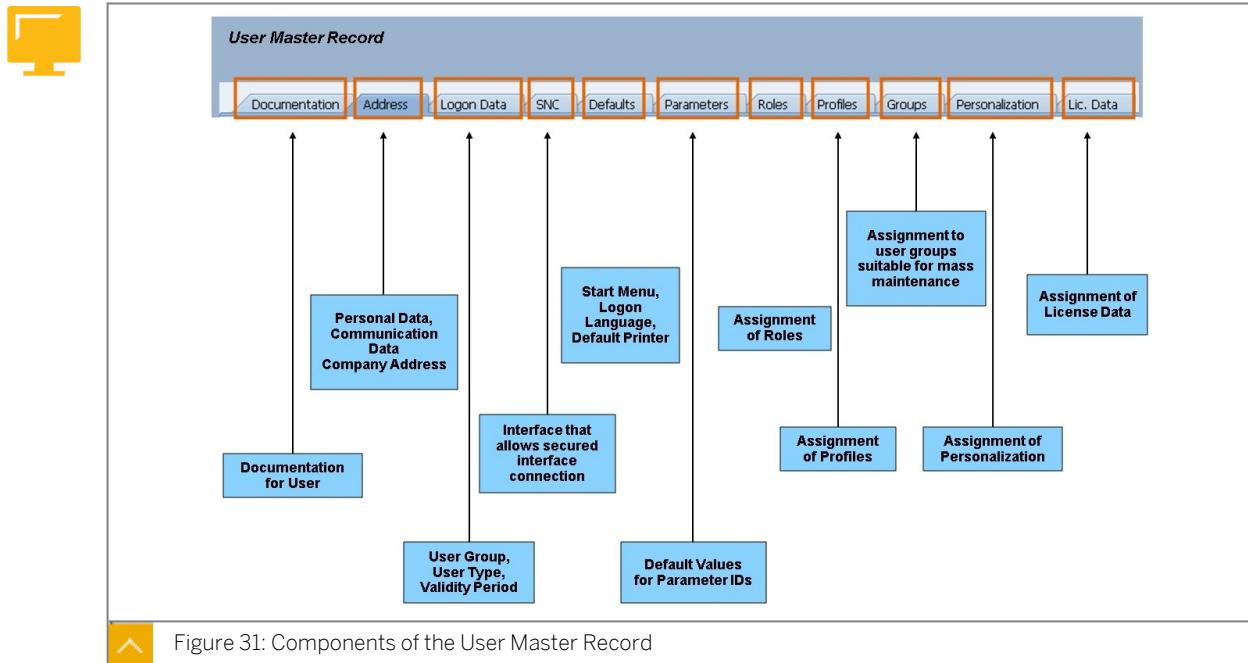
The user maintenance transaction allows you to create a user with classic address (*Create* icon) or to create a technical user (*Create Technical User* icon).

- **User with classic address:**

- You can maintain personal and workplace data using the transactions and APIs of user administration.
- You can maintain the company using transaction SUCOMP and assign it using the transactions and APIs of user administration.

- **Technical user:**

A technical user does not have any address data. Use the corresponding field on the "Documentation" tab for the description.



A user can only logon to an SAP system if a user master record with a corresponding password exists. The scope of activity of individual users in the SAP system is defined in the master record by one or more roles, and is restricted by the assignment of the appropriate authorizations.

User master records are client-specific. You must maintain your own user master records for every client in SAP systems.

The following authorization objects are required to create and maintain user master records:

- Authorization to create or maintain a user master record, and to assign it to a user group (object S_USER_GRP)
- Authorization for the authorization profiles that you assign to users (object S_USER_PRO)
- Authorization to create and maintain authorizations (object S_USER_AUTH)
- Authorization to protect roles. With this authorization object, you specify which roles can be edited, and which activities (display, change, create, and so on) are intended for the role(s) (object S_USER_AGR).
- Authorization for transactions that you may assign to the role and for which you can assign authorization to start the transaction in the Role Maintenance (object S_USER_TCD)
- Authorization to restrict values that the system administrator can include in a role or change in Role Maintenance (S_USER_VAL)

By choosing *System - User Profile - Own Data* (transaction SU3), users can themselves maintain the *Address*, *Defaults*, and *Parameters* tabs.

**Hint:**

In addition to the possibilities for assigning authorizations in the SAP system described in the following sections, you can ensure that your data is protected with additional measures:

- Secure communication in the network (Secure Network Communication [SNC])
- Secure data formats (Secure Store and Forward [SSF])
- Security in the Internet
- System passwords
- Database accesses
- Transport system
- Your own directory structures for the SAP system, and so on

For information about these topics, see the Security Guide in the SAP Service Marketplace under service.sap.com/securityguide. (You can also access this under www.service.sap.com.)

Tab Page: Documentation



User	BOJA007	
Changed By	ADM940	
Status		Revised
<input checked="" type="radio"/> Documentation <input type="radio"/> Address <input type="radio"/> Logon Data <input type="radio"/> SNC <input type="radio"/> Defaults <input type="radio"/> Parameters <input type="radio"/> Roles <input type="radio"/> Profiles		
Description	User for Trainings	
Person Responsible	ADM940	
Documentation for User: roles added: ADM940_BC_ADMIN and ADM940_RGB 20.06.2016 14:35:21 ADM940: created according to ticket 0815		

Figure 32: User Master Record: Documentation

The tab *Documentation* can be used to provide information about the users:

- *Description*: This field contains a short description of the user.
- *Person Responsible*: You can use this field to define an SU01 user who is technically and effectively responsible for this user. This can be useful for traceability in systems, especially for anonymous technical users.

- **Documentation for User:** This field contains the documentation for a user. A time stamp is automatically generated and the person who made the change is recorded for each entry. Only the creation of entries is possible. You cannot change or delete old entries.

**Hint:**

You can use the report RSUSR_DELETE_USERDOCU delivered with this enhancement to completely delete the documentation of selected users. This report is intended as a cleanup report for use after a client copy, for example. The selective deletion of individual documentation entries is not envisaged, since a consistent history needs to be ensured (like change documents).

Tab Page: Address

Figure 33: User Master Record: Address Data

**Hint:**

You must specify at least the following data to create new users in a system:

- On the *Address* tab page, you only need to maintain the *Last name* field.
- On the *Logon Data* tab page, you must enter an *Initial Password* for the new user.

All other specifications are optional and almost self-explanatory.

Tab Page: Logon Data



Maintain Users

User	BOJA01	Changed By	ADM940	06.05.2014	11:04:06	Status	Saved
<input type="button" value="Address"/> <input type="button" value="Logon Data"/> <input type="button" value="SNC"/> <input type="button" value="Defaults"/> <input type="button" value="Parameters"/> <input type="button" value="Roles"/> <input type="button" value="Profiles"/> <input type="button" value="Groups"/> <input type="button" value="Personalization"/> <input type="button" value="Lic. Data"/>							
Alias <input type="text" value="BOJA01"/> <input type="button" value="..."/> User Type <input type="button" value="Dialog"/> Security Policy <input type="text"/> Password <div style="display: flex; justify-content: space-between;"> <input type="button" value="New Password Rules (Case-Sensitive)"/> <input type="button" value="New Password"/> <input type="button" value="Repeat Password"/> <input type="button" value="F1"/> </div> <div style="display: flex; justify-content: space-between;"> <input type="text" value="*****"/> <input type="text" value="*****"/> <input type="button" value="F1"/> </div> <div style="display: flex; justify-content: space-between;"> Password Status Initial Password (Set by Administrator) <input type="button" value="F1"/> </div> User Group for Authorization Check User group <input type="text"/> Validity Period Valid from <input type="text"/> Valid through <input type="text"/> Other Data Account no. <input type="text"/> Cost center <input type="text"/>							

Figure 34: User Master Record: Logon Data

The **Alias** is an alternative ID for an SAP user. You can assign an alias to a user. This means that 40 characters are available when assigning user names (longer, more descriptive names). The user can therefore be identified using either the (12 character) user name or the alias. The alias is primarily used if users are created in a Self-Service scenario from Internet transactions. In this situation, only the alias is specified and used.

Security policy: Sometimes users require a different security policy for logon and passwords than the default values. For example, powerful users such as administrators should have passwords with a higher level of protection than standard users. Such users should be forced to change their passwords more often or have more complex rules for their passwords. However, such requirements, if applied widely, can cause an increase in help desk requests if you force standard users to comply with such requirements.

This field could be used to choose a security policy for the user. Otherwise, the user uses the standard security policy.

Initial password: To assign initial passwords you may enter the password manually, generate the password, or deactivate the password. Deactivation means that the user can no longer log on using a password, but only with Single Sign-On variants (X.509 certificate, logon ticket). This is useful if you do not require password-based logon, because logon is performed exclusively in other ways. In this case, deactivating the password increases security, as passwords that are not used are usually still initial.



Hint:

To increase security, it is possible to send encrypted e-mails with initial passwords. For details see SAP note 1750161 - User administration: Saving additional information.

User group for authorization checks: To assign the user to a user group, enter the user group. This is required if you want to divide user maintenance among several user administrators. Only the administrator that has authorization for this group can maintain users of this group. If you leave the field empty, the user is not assigned to any group. This means that any user administrator can maintain the user.

It is possible to define the user group as a required entry field for specific clients. Therefore, a user can no longer be created without entering a valid user group. Changing a user group to a blank value is also no longer possible. This function has to be activated manually. For details, see SAP note 1663177 - SU01: User group as required entry field. A valid user group must be maintained; it is used as the standard user group.

User type: The system proposal is *Dialog* (normal dialog user). The other user types can be assigned if special kinds of processing have to be performed (see the following figure).

Validity period: You can specify the validity period of the user master record with these fields. If you do not wish to restrict the validity of the user master record, leave the fields empty.

Other data: For each user or user group, you should assign an accounting number, which you can choose as required. System usage of that user is settled in the accounting system (ACCOUNTING-EXIT) using this accounting number. Useful accounting numbers, for example, are the cost center or company code of the user.

User Types in Detail

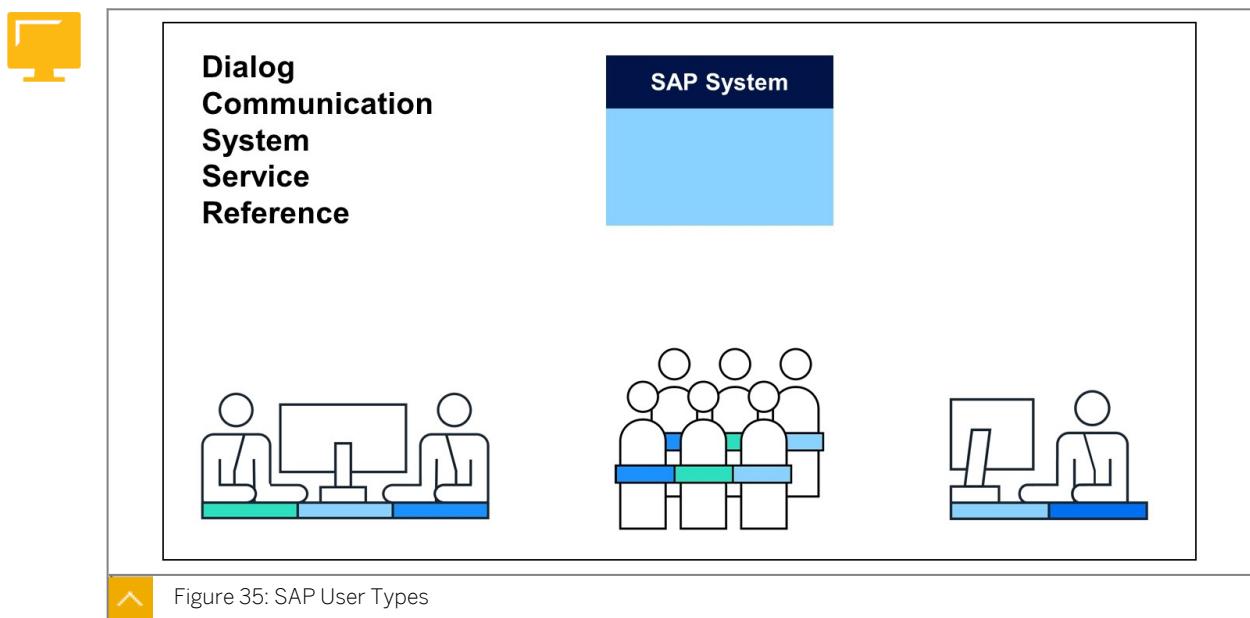


Figure 35: SAP User Types

Dialog (A)

User type for exactly one interactive user (all logon types including Internet users):

- With a dialog logon, the system checks whether the password has expired or is *initial*. The user can change their own password.
- Multiple dialog logons are checked and, where appropriate, logged.

System (B)

User type for background processing and communication within a system (internal RFC calls):

- A dialog logon is not possible.
- The system does not check whether the password has expired or is initial.
- Only the user administrator can change the password.
- Multiple logons are permissible.
- The *System* type is also frequently used in Central User Administration (CUA).

Communication (C)

User type for dialog-free communication between systems (such as RFC users for ALE, Workflow, and TMS):

- A dialog logon is not possible.
- Whether the system checks for expired or *initial* passwords depends on the logon method (interactive or not interactive). Due to a lack of interaction, no request for a change of password occurs.

Service (S)

User type that is a dialog user available to a larger, anonymous group of users. Assign only very restricted authorizations for this user type:

- During a logon, the system does not check whether the password has expired or is initial. Only the user administrator can change the password (transaction SU01, Goto, Change Password).
- Multiple logons are permissible.
- Service users are used, for example, for anonymous system accesses through an ITS service. After an individual authentication, an anonymous session started with a service user can be continued as a person-related session with a dialog user.

Reference (L)

User type for general, non-person-related users that allows the assignment of additional, identical authorizations, such as for Internet users created with transaction SU01. You cannot log on to the system with a reference user.

You should be very cautious when creating reference users. For more information, see the online documentation, or read SAP Note 330067.

Tab Page: SNC



Maintain Users

User	BOJA01	Changed By	ADM940	06.05.2014	11:04:06	Status	Saved
------	--------	------------	--------	------------	----------	--------	-------

Address Logon Data SNC Defaults Parameters Roles Profiles Groups Personalization Lic. Data

SNC Status
✖ SNC is not active on this application server
ℹ Unsecured logon is permitted for specific users

SNC Data
SNC name
⚠ Canonical name not determined
 Permit Password Logon for SAP GUI (User-Specific)

Figure 36: User Master Record: SNC

Secure Network Communications

The Secure Network Communications (SNC) functions allow you to use an external security product to secure the communications between SAP System components (for example, between application servers and front-end clients). Encryption can be used in three different areas:

- End-to-end security at the application level
- Integrity and privacy protection for data transfer
- Secure user authentication



Hint:

It is the customer's responsibility to ensure that the purchased network security products from any manufacturer does not conflict with local legislation for cryptography.

The SNC User's Guide and additional documentation is available on the SAP Help Portal or other supplemental information under the link <https://www.sdn.sap.com/irj/sdn/security>.

Tab Page: Defaults

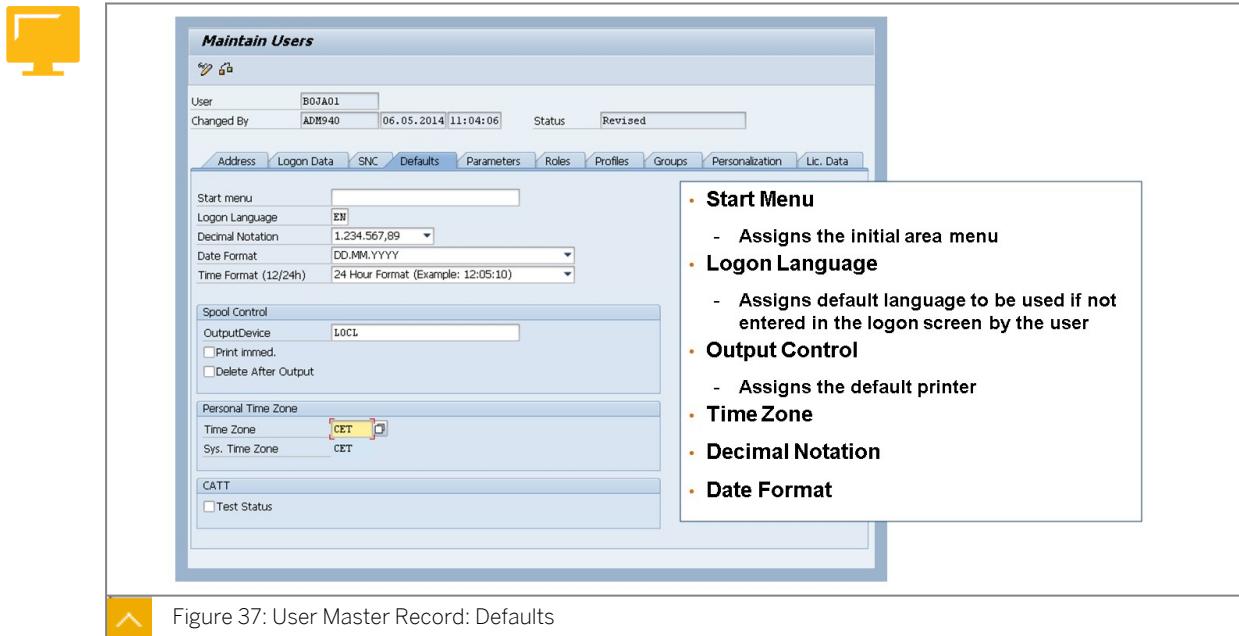


Figure 37: User Master Record: Defaults

Start Menu

In this field, you can specify an area menu, which you can choose using the possible entries help. The SAP menu (SAP Easy Access) then only contains the components of this area menu.

A user needs the credit management transactions to perform daily work. If you enter *FRMN* as the start menu in that user's data, the SAP menu displays only the transactions of credit management.

In transaction *SSM2*, you can specify the initial menu across the entire system.

Logon Language

The system language when the user logs on. On the logon screen, the user can choose another language if required.

Output Device

A (short) name of a printer in the SAP system, specified in the device definition. The users in the SAP system use this name (or the long name) to select the output device.

Time Zone

The time zone describes the location of an object in relation to its local time. The underlying set of rules describes the time difference between the time zone and UTC in hours and minutes, and the start and end of summer time.

Decimal Notation and Date Format

Different countries use different formats for numbers and dates. Enter the format normally used in your country.

Tab Page: Parameters

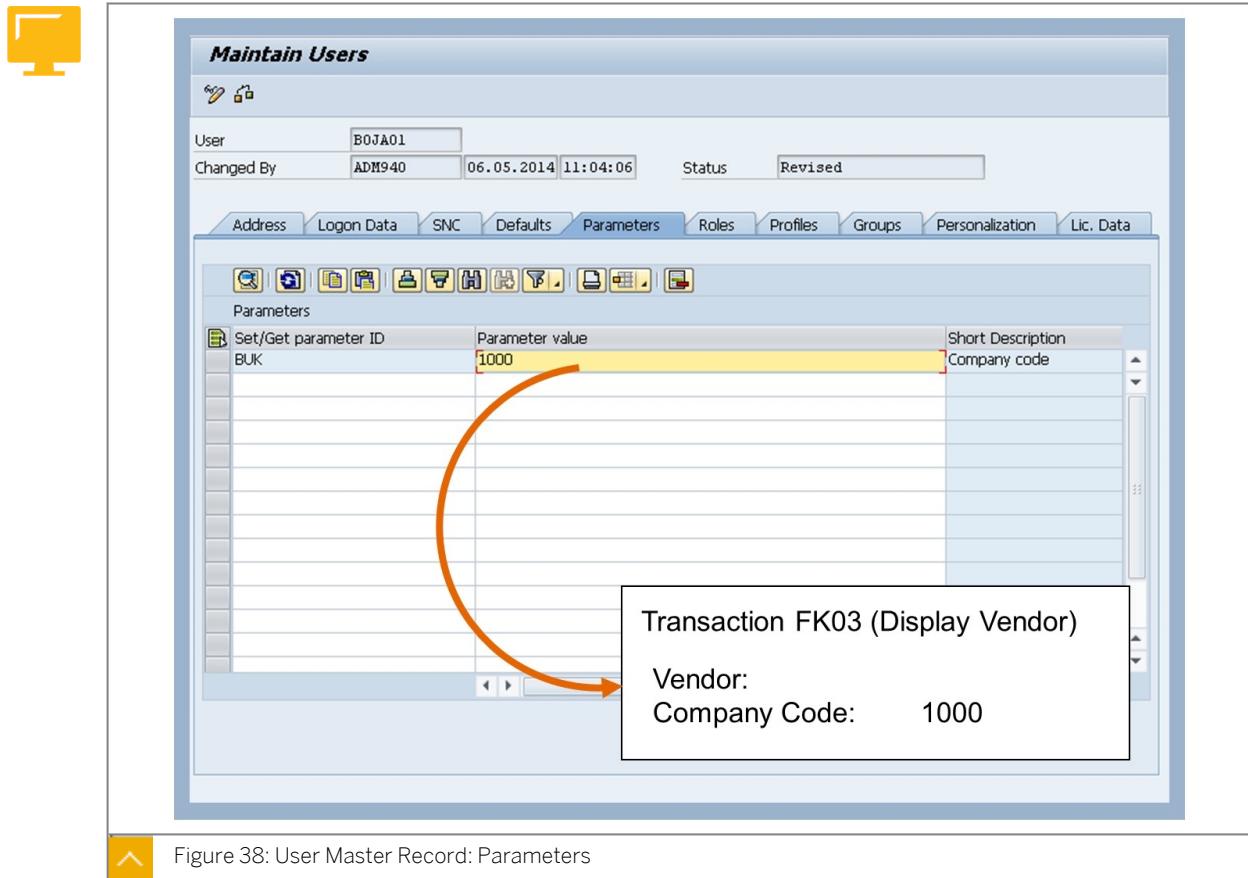


Figure 38: User Master Record: Parameters

Using a parameter ID, a field can be filled with default values from SAP memory.

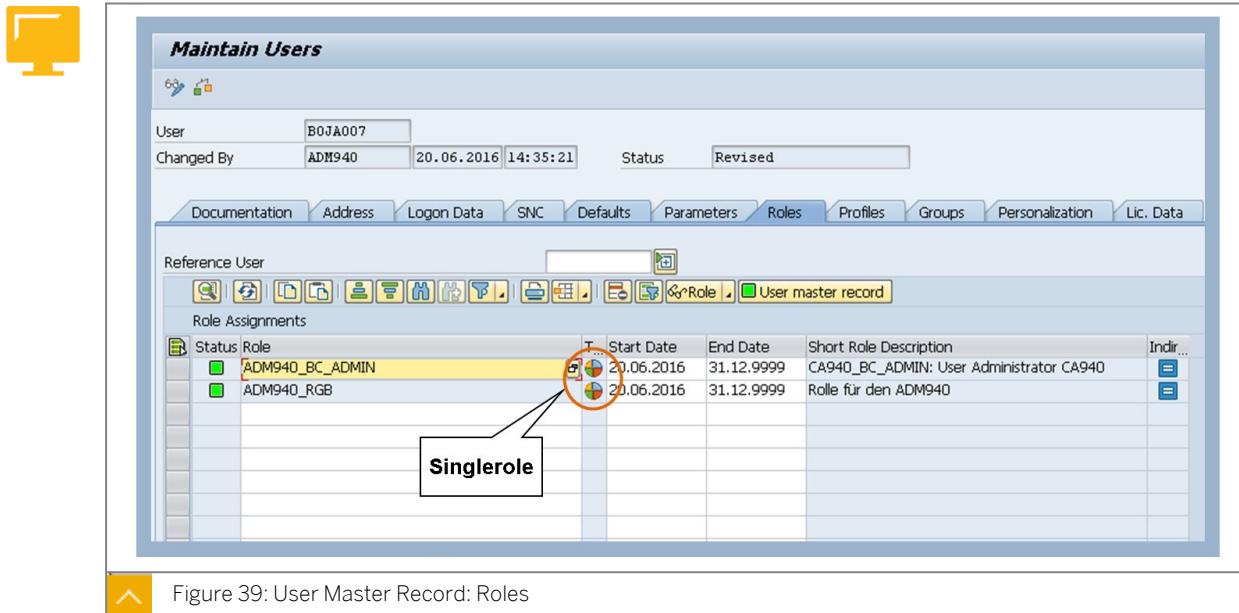
Example:

A user only has authorization for company code 1000. When a transaction starts, this company code is saved to the memory using the corresponding parameter ID. On all subsequent screens, all fields referencing the company code data element are then automatically filled with the value 1000.

A field on a screen is only filled automatically with the value saved under the parameter ID of the data element, if you have explicitly allowed this in the Screen Painter.

Tab Page: Roles

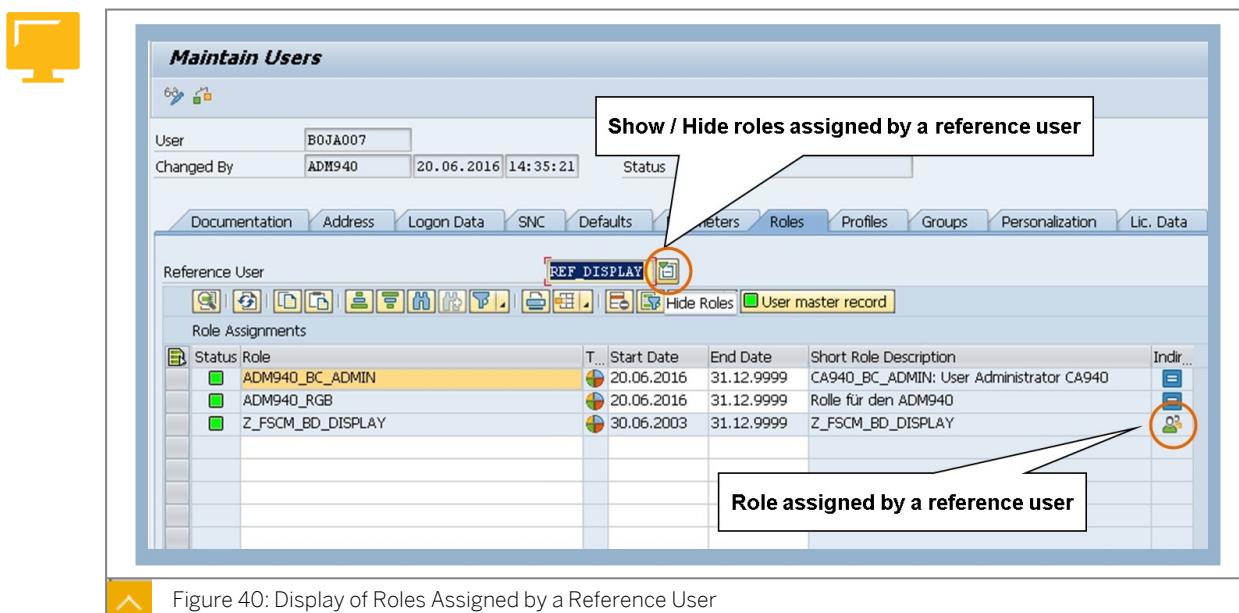
A role is a set of functions describing a specific work area. In the role, you organize transactions, reports, or web addresses in a user menu. A role can be assigned to any number of users.



On the *Roles* tab page, you can use the possible entries help (F4 help) to display a list of all available roles and then select the desired entries from that list.

You can enter any number of roles in the table, and then restrict their validity using the *Valid From* and *Valid To* columns. If you use the input help for these columns, the system displays a calendar in which you can select the date.

Further authorizations can be assigned to a user by a reference user. In addition to the roles assigned to the user itself, the user also references the roles and authorizations that are already assigned to the reference user. The roles of the reference user can be shown or hidden (see SAP Note 2110144 - SU01: Display of reference user roles).



Tab Page: Profiles

On the *Profiles* tab page, you assign manually created authorization profiles, and therefore authorizations, to a user. The generated profiles of the roles assigned to the user are also displayed there.

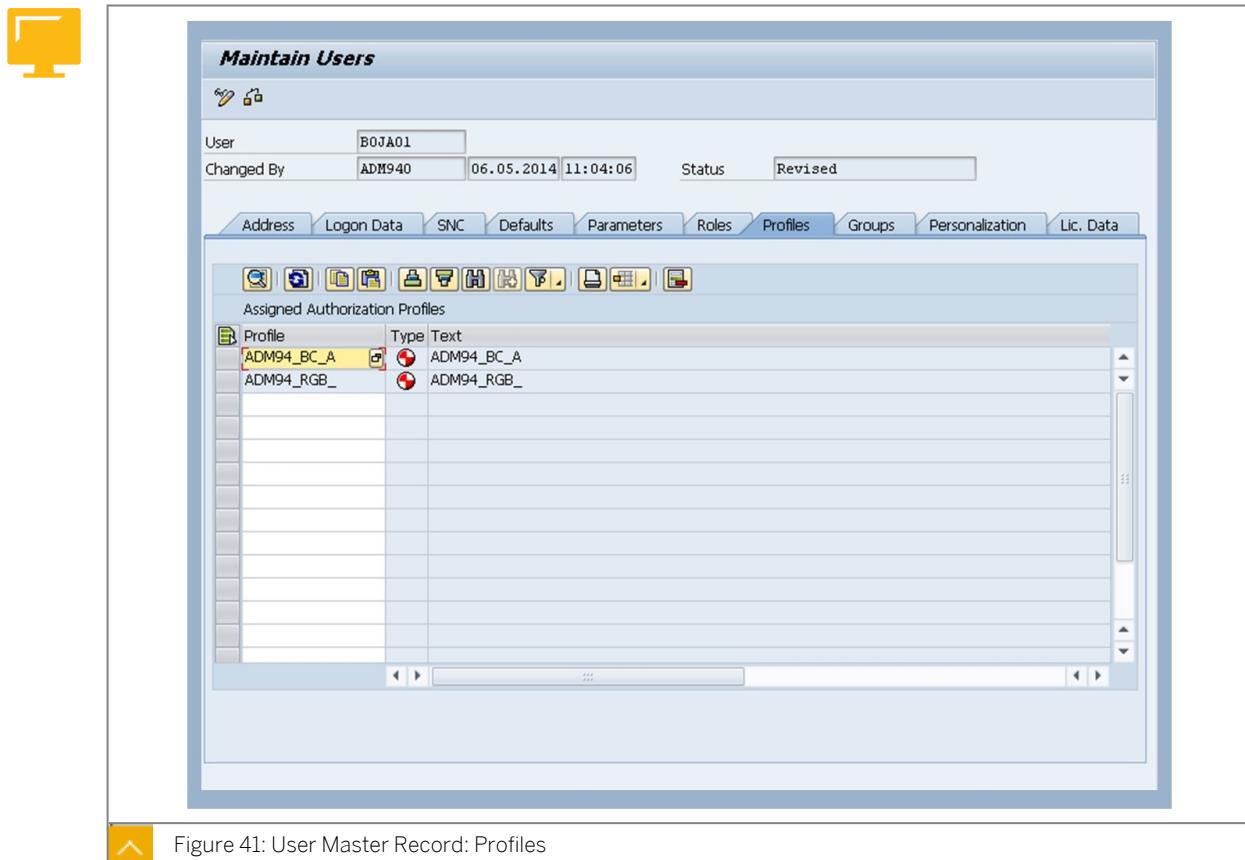


Figure 41: User Master Record: Profiles

Each profile grants the user a number of authorizations.



Hint:

Remember that we recommend you structure the contents of authorizations using transaction PFCG and not using “manual profiles”.



Caution:

Never enter the generated profiles directly on the *Profiles* tab page, because transaction PFUD deletes these assignments if there is no entry for them on the *Roles* tab page. When you assign a role to a user on the *Roles* tab page, the profile generated for this role is automatically entered on the *Profiles* tab page, and the profiles in the user master record are compared with the roles.

The SAP system contains predefined profiles, such as:

- **SAP_ALL:** To assign all authorizations that exist in the SAP system to users, assign the profile SAP_ALL.
- **SAP_NEW:** A composite profile to bridge the differences in releases in the case of new or changed authorization checks for existing functions, so that your users can continue to work as normal.

**Caution:**

This composite profile contains very extensive authorizations, since, for example, organizational levels are assigned with the full authorization asterisk (*).

Tab Page: Groups

The next tab page, *Groups*, is not currently fully actively used. The main use, for the *Global User Manager*, has officially been deactivated. For this reason, this tab page is not described in detail here. For more information, see SAP Note 433941, the current online documentation, or access the latest information through the link www.service.sap.com.

Tab Page: Personalization

Description	Personalization object key
Inbound Developer Utilities	/SPE/INB_DEVUT
Area Menu Editor Settings	AREA_MENU_SETTINGS
Settings for Business Partner Mainten...	BUPA_DIALOG_JOEL
Timesheet user settings (CATSXT)	CATSTX_USER_DFLT
Cohort Maintenance	CM_DATE_SETTINGS_COHORTS
Default selection data for Transactio...	CM_EVPLAN_SELECTION
Appraisal Calculation Attributes	CM_GRADING_CALC_ATTR
CRM Configuration Mode Enabled	CRM_CONFIG_MODE_ENABLED
Personalized Settings for Recent Obj...	CRM_PERS_RECENT_OBJECTS
CRM Personalization: Disabling of Sma...	CRM_PERS_SVH_DISABLED
CRM framework accessibility mode flag	CRM_THTMLB_PERS_ACCS
Skin color definition	CRM_THTMLB_PERS_COLOR
CRM UI No-Effects Mode	CRM_THTMLB_PERS_NOEF
CRM skin chosen by the user	CRM_THTMLB_PERS_SKIN
WebClient UI: Message bar preview i...	CRM_THTMLB_PERS_TOAST
Project Management: Storage for Us...	DPR_USER_SETTINGS
Project Management: Storage for Us...	DPR_USER_TEMP_SETTINGS
Project Management: Folders for Use...	DPR_USER_UI_SETTINGS

Figure 42: User Master Record: Personalization

On the *Personalization* tab page, you can make person-related settings using personalization objects. *Personalization* is available both from role maintenance and in user maintenance. You can define values here that control the results displayed when programs are called (such as display periods: *Last 3 months*, Number of entries: *Max. 50*, and so on).

Steps for using personalization:

1. Choose the *Personalization* tab page.
2. Go to the application component display (icon with two pages and a blue bar on the right of the display).

3. Select the component for which you want to maintain personalization data. The right side of the display lists the personalization objects provided for this component.
4. Select the desired personalization object and assign the values to be predefined in the dialog window that appears.

Tab Page: License Data

SAP software contains a measurement program with which every system produces the information used to determine the payment applicable for the installation.

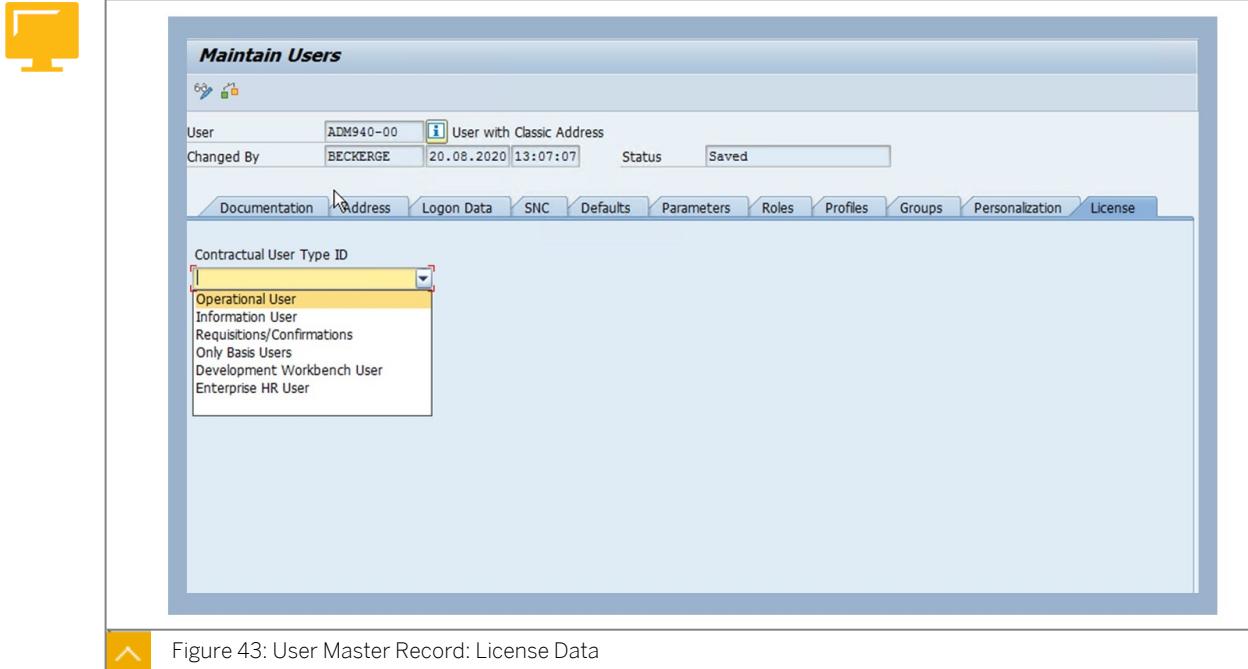


Figure 43: User Master Record: License Data

The measurement program is used exclusively to determine the number of users and the utilized units of SAP products. The results are evaluated in accordance with the contractually agreed conditions.

For more information, see the current version of the document *System Measurement Guide* (service.sap.com/licenseauditing). You can call this with or without the www prefix).

Tab Page: DBMS

Database Management System (DBMS) user management enables SAP NetWeaver Application Server (SAP NetWeaver AS) ABAP to manage users and their privileges on the DBMS.



Hint:

Currently only SAP HANA database is supported.

In a typical SAP NetWeaver Application Server ABAP installation, you maintain the users that run applications on SAP NetWeaver Application Server ABAP. In the DBMS, you maintain a few technical users, but you do not need users in the DBMS for most of your SAP NetWeaver Application Server ABAP users. There are use cases that require you to maintain users in the DBMS.

- SAP Business Warehouse (SAP BW), needs a 1:1 user mapping to map analytic privileges of the database to the virtual analysis authorizations of the SAP BW.
- Your users run applications that access the database directly. You must assign privileges to the user in the database.

The screenshot shows the 'Display Users' screen in SAP DBMS User Management. The user 'SCHWARZLS' is selected. The 'DBMS User' tab is active, displaying fields for DBMS User (SCHWARZLS), Valid from (08.03.2016), and Valid To (empty). Below these are checkboxes for 'Deactivated (Locked)' and 'Restricted User'. The 'Authentication' section includes fields for New Password and Repeat Password, and checkboxes for SAML, X509, SAP Logon Ticket, and SAP Assertion Ticket. Under 'Assigned DBMS Roles', the 'Database Management System Role' is listed with 'PUBLIC' and 'TRAINING_USER_ROLE' assigned by 'SYS' and 'SYSTEM' respectively. Other tabs like Documentation, Address, Logon Data, SNC, Defaults, Parameters, Roles, Profiles, Groups, Personalization, and Lic. Data are visible at the top.

Figure 44: DBMS User Management for a SAP HANA Database

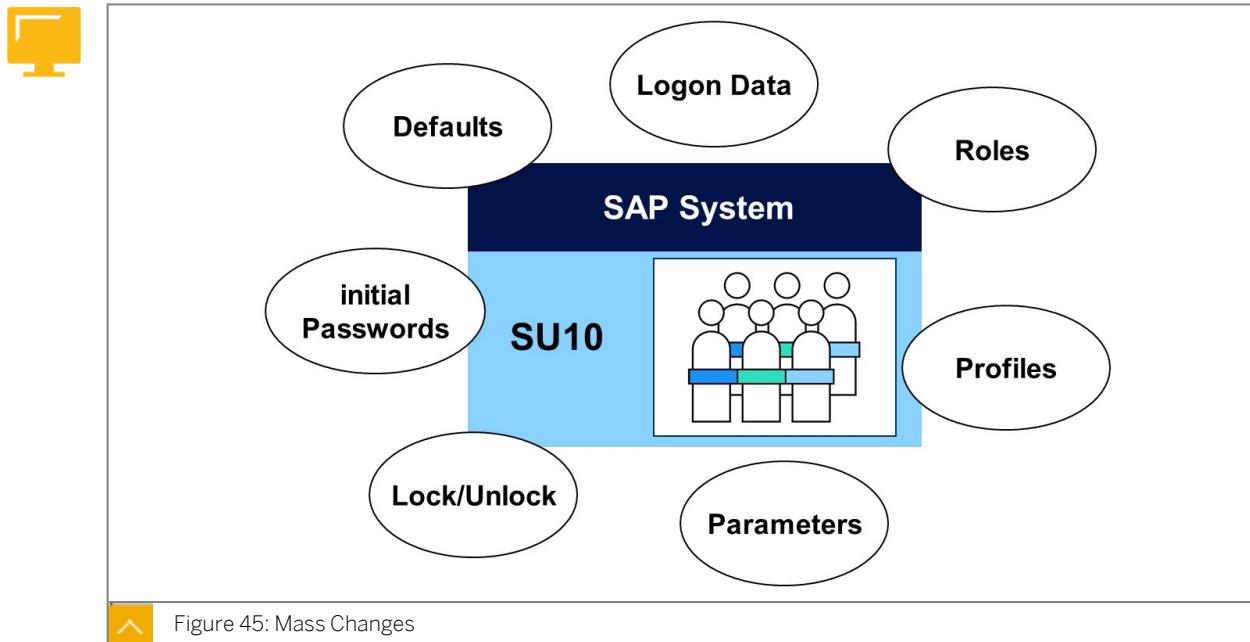
To simplify user management of the DBMS, you can create a connection between the user management of SAP NetWeaver Application Server ABAP and the DBMS. When you create users in SAP NetWeaver Application Server ABAP, the SAP NetWeaver Application Server ABAP creates the users in the DBMS automatically, with the same user ID and password. Setting an administrative lock on an SAP NetWeaver Application Server ABAP user also locks the corresponding DBMS user. You can also add and remove DBMS privileges for the DBMS user as far as this is allowed by the DBMS.

The necessary configuration steps are described in the online documentation: DBMS User Management, and in the following Security-Blog: <http://scn.sap.com/community/security/blog/2014/10/21>.



Hint:
Password synchronization and password locks are not supported.
This customization is client-specific.

Other Possibilities for User Maintenance and Change Documents



Most changes that can be made for individual users in the context of user management can also be made for a selected quantity of users.

Log-on data, defaults, parameters, roles, and profiles can be changed for a particular group of users.

In user maintenance, you can make changes to a selected group of users by choosing *Environment / Mass Changes* (transaction SU10).



Hint:

On the Address, Logon Data, and Defaults tab pages, you must select the *Change* checkbox for each change. This ensures that your changes, such as deleting the content of a field are transferred for the relevant fields.

After each mass change, a dialog box appears, asking whether you would like a log. The log shows who made changes, in which system, at which time.

The log contains several message levels, that you can expand as desired using the relevant buttons. If there is a long text for a particular message, you can also display this by choosing a button displayed next to the message.

While you can make certain specifications for the log display by choosing *Settings*, the *Color Legend* provides information about the colors used in the display.

You can print the log or save it to a file on your PC.

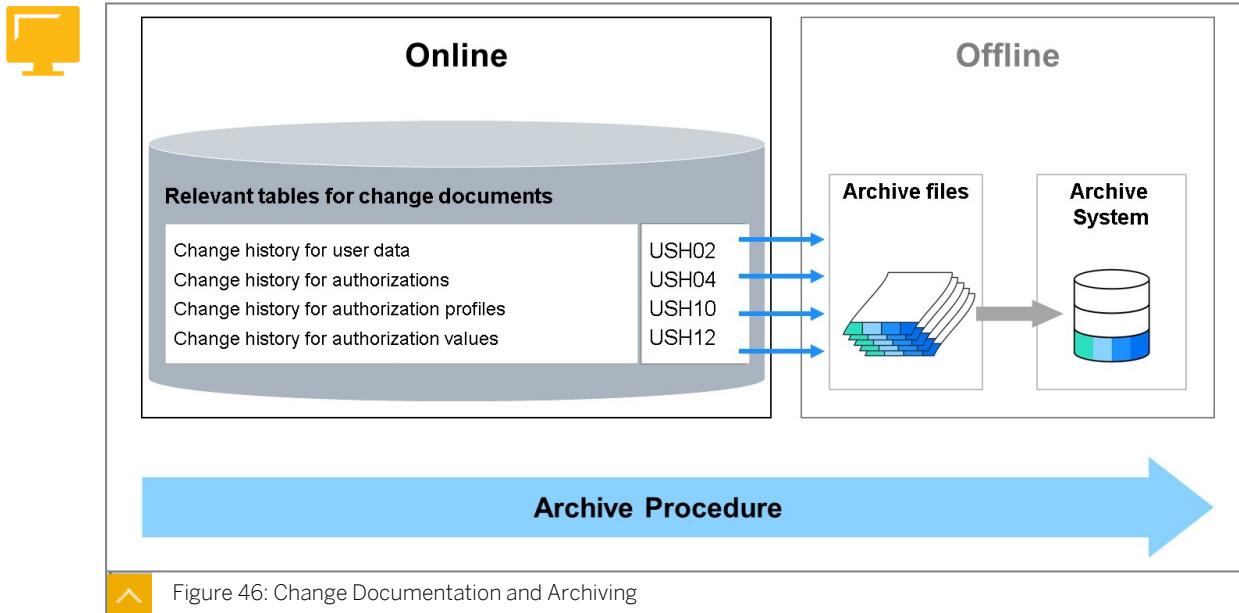


Figure 46: Change Documentation and Archiving

Display Change Documents: Choose *Environment / Information System* and then, on the overview screen that appears, "Change Documents" to display a list of changes made to user master records, authorization profiles, and authorizations.

Archive Change Documents: User master records and authorizations are saved in USR* tables. Using the archiving function, you can reduce the memory space occupied by the USR* tables in the database. Change documents are saved in USH* tables. The archiving function deletes change documents from the USR* tables that are no longer needed.

You can archive the following change documents or change records relating to user master records and authorizations from the USH* tables:

- Changes to authorizations (archiving object *US_AUTH*)
- Changes to authorization profiles (archiving object *US_PROF*)
- Changes to the authorizations assigned to a user (archiving object *US_USER*)
- Changes to a user's password or to defaults stored in the user master record (archiving object *US_PASS*)

Unit 3

Exercise 3

Practice System Exercise: Maintain and Evaluate User Data

Business Example

Almost all companies use PCs and software programs to support their employees in their daily work. However, to work with this technology, the users require access and authorizations to call the programs. A control method in an SAP system is the user master record and its roles and profiles.

Task 1: Create a user group

Create a new user group ZGR## with a description of your choice.

1. Start transaction *Maintain User Groups* (SUGR).

Task 2: Create a User Master Record

Create a user master record for a dialog user GR##-ADM.

1. Start transaction *User Maintenance* (SU01).
2. Enter an initial password of your choice and assign the user to user group ZGR##.
Initial password: Init1234
3. Assign the log-on language that you have used yourself for logging on.
4. Save your user master record.

Task 3: Assign a Predefined Role to Your New User Master Record

Assign a predefined role ADM940_BC_ADMIN to your new user master record.

1. Start transaction *User Maintenance* (SU01).
2. Save your user master record.

Task 4: Check the User Master Record

Check the user master record of your user GR##-ADM.

1. Check whether a role is assigned to your user GR##-ADM.
Assigned role:

-
2. Link your user with another role. Choose the role ADM940_PLUS.
If you are in “display mode”, then change to “change mode” (Shift+F7).
 3. Are authorization profiles assigned to your user?
Which authorization profile(s)?

_____;

-
4. Save your user master record.
 5. Go back to the SAP Easy Access menu.

Task 5: Display the Change Documents for a User

Display the change documents for your user GR##-ADM by calling up the information system for users and authorizations and selecting the report *For Users* under *Change Documents* for users and authorizations.

1. Display the change documents for your user GR##-ADM by calling up the information system for users and authorizations and selecting the report *For Users* under *Change Documents* for users and authorizations.
 2. Does the list tell you that creating the user master record and assigning the user to roles were separate steps?
-

Task 6: Log On to the System with the Credentials of the Created User

Try to log on to the system as user GR##-ADM without *Language* information.

1. Start SAP Logon and log on to the system as user GR##-ADM.
 2. Do you need to enter a log-on language?
-

3. Check the user menu (Ctrl+F10):

If you want to see the transaction codes in the user menu, select on the top menu *Extras* → *Settings* and select *Display Technical Name*.

Which functions does it contain? List some examples.

4. Check the user buffer by calling the *Analyze User Buffer* transaction.

How many authorizations exist?

For which authorization objects? List some examples.

5. Log off as user GR##-ADM and log on again as user ADM940-##.

Task 7: Create Users Using the User Mass Maintenance Transaction

Create additional user master records using the *User Mass Maintenance* transaction.

1. Start the *User Mass Maintenance* transaction.
2. Create the following six user names.

User Name
GR##-FI1
GR##-FI2

User Name
GR##-SD1
GR##-SD2
GR##-MM1
GR##-MM2

3. Assign the user group ZGR## to all users.
4. Assign the log-on language that you have used yourself for logging on.
5. Save your user master record.
6. Check the result in the change log for a given user entry.

You can copy the generated initial passwords into the tables in the exercise section.



Hint:

Passwords of 40 characters in length are automatically generated. If you want, you can copy the generated passwords from the log to the following table, or change them directly for future tasks in transaction SU01 when required, using the *Change Password* button (Shift+F8).

User name	Generated Password
GR##-FI1	
GR##-FI2	
GR##-SD1	
GR##-SD2	
GR##-MM1	
GR##-MM2	

7. You can copy the generated initial passwords into the tables in the exercise section.

Unit 3 Solution 3

Practice System Exercise: Maintain and Evaluate User Data

Business Example

Almost all companies use PCs and software programs to support their employees in their daily work. However, to work with this technology, the users require access and authorizations to call the programs. A control method in an SAP system is the user master record and its roles and profiles.

Task 1: Create a user group

Create a new user group ZGR## with a description of your choice.

1. Start transaction *Maintain User Groups* (SUGR).
 - a) SAP Menu: → Tools → Administration → User Maintenance → User Groups, (**transaction code** SUGR).
 - b) Enter **ZGR##** in the *User group* field.
 - c) Choose *Create user group* (F8).
 - d) Enter a description in the *Text* field and choose *Save* (Ctrl+S).

Task 2: Create a User Master Record

Create a user master record for a dialog user GR##-ADM.

1. Start transaction *User Maintenance* (SU01).
 - a) Choose SAP Menu: → Tools → Administration → User Maintenance → Users, (**transaction code** SU01).
 - b) Enter **GR##-ADM** in the *User* field and choose *Create* (F8).
 - c) Select the *Address* tab page.
Enter **Admuser##** in the *Last name* field.
Enter your choice of data in the other fields.
 - d) Select the *Documentation* tab page.
Enter **User for Group ##** in the *Description* field.
Enter **ADM940-##** in the *Person Responsible* field.
2. Enter an initial password of your choice and assign the user to user group ZGR##.
Initial password: Init1234
 - a) Select the *Logon Data* tab page.
Enter **Init1234** in the *New Password* and the *Repeat Password* field.
Enter **ZGR##** in the *User group* field.

3. Assign the log-on language that you have used yourself for logging on.
 - a) Select the *Defaults* tab page.
Enter the log-on language of your choice in the *Logon Language* field.
4. Save your user master record.
 - a) Choose *Save (Ctrl+S)*.
 - b) Go back to the SAP Easy Access menu.

Task 3: Assign a Predefined Role to Your New User Master Record

Assign a predefined role **ADM940_BC_ADMIN** to your new user master record.

1. Start transaction *User Maintenance (SU01)*.
 - a) Choose SAP Menu: → Tools → Administration → User Maintenance → Users, (**transaction code SU01**).
 - b) Enter **GR##-ADM** in the *User* field and choose *Change (Shift+F6)*.
 - c) Select the *Roles* tab page.
 - d) On the *Roles* tab, enter **ADM940_BC_ADMIN** in the *Role* column and press Enter.
2. Save your user master record.
 - a) Choose *Save (Ctrl+S)*.
 - b) Go back to the SAP Easy Access menu.

Task 4: Check the User Master Record

Check the user master record of your user GR##-ADM.

1. Check whether a role is assigned to your user GR##-ADM.
Assigned role:

 - a) Start transaction *User Maintenance (SU01)*
SAP Menu: → Tools → Administration → User Maintenance → Users, (transaction code **SU01**).
 - b) Enter **GR##-ADM** in the *User* field and choose *Change (Shift + F6)*.
 - c) Select the *Roles* tab page.
Answer: YES. A role is assigned on the *Roles* tab page: **ADM940_BC_ADMIN**.
2. Link your user with another role. Choose the role **ADM940_PLUS**.
 - a) On the *Roles* tab, enter **ADM940_PLUS** in the *Role* column and press Enter.
If you are in “display mode”, then change to “change mode” (Shift+F7).
3. Are authorization profiles assigned to your user?
Which authorization profile(s)?

;

 - a) Select the *Profiles* tab page.

Assigned authorization profiles:

- Profile for role ADM940_BC_ADMIN
- Profile for role ADM940_PLUS.

4. Save your user master record.
 - a) Choose Save (Ctrl+S).
5. Go back to the SAP Easy Access menu.

Task 5: Display the Change Documents for a User

Display the change documents for your user GR##-ADM by calling up the information system for users and authorizations and selecting the report *For Users* under *Change Documents* for users and authorizations.

1. Display the change documents for your user GR##-ADM by calling up the information system for users and authorizations and selecting the report *For Users* under *Change Documents* for users and authorizations.
 - a) SAP Menu: → Tools → Administration → User Maintenance → Information System → Change Documents → Users
Select the report: *For Users*.
 - b) Enter **GR##-ADM** in the User field.
 - c) Choose Select All on the User Attributes tab page in the Selection Criteria area.
 - d) Choose Select All on the Roles/Profiles tab page in the Selection Criteria area.
 - e) Choose Execute (F8).
2. Does the list tell you that creating the user master record and assigning the user to roles were separate steps?

a) Analyze the values in the Time column.

Yes. The different time stamps and the numbering tell you that the changes were made in different steps/lines and one after another.

Task 6: Log On to the System with the Credentials of the Created User

Try to log on to the system as user GR##-ADM without Language information.

1. Start SAP Logon and log on to the system as user GR##-ADM.
 - a) Start SAP Logon.
 - b) Select system T41 and choose Log On.
 - c) Enter **GR##-ADM** in the User field.
 - d) Enter the initial password **Init1234** in the Password field.
 - e) Leave the Language field empty.
 - f) Choose Enter.
 - g) Enter a password of your choice, for example **Welcome1** in the New Password and the Repeat Password fields.
 - h) Choose Transfer (Enter).

i) Choose *Continue (Enter)*.

2. Do you need to enter a log-on language?

a) No, the log-on language is set in the user master record.

3. Check the user menu (Ctrl+F10):

If you want to see the transaction codes in the user menu, select on the top menu *Extras → Settings* and select *Display Technical Name*.

Which functions does it contain? List some examples.

a) The user menu contains transaction codes for:

- Users (SU01)
- Display users (SU01D)
- User mass maintenance (SU10)
- Maintain user groups (SUGR)
- Analyze user buffers (SU53) and
- Analyze user buffers (SU56) and
- Analyze user buffers (SUIM) and
- An additional submenu *Information System* with other entries.

4. Check the user buffer by calling the *Analyze User Buffer* transaction.

How many authorizations exist?

For which authorization objects? List some examples.

a) Start transaction SU56 in your user menu or in the SAP menu.

SAP Menu: → Tools → Administration → Monitor → User Buffer, (transaction code SU56).

b) The number of authorization objects is shown in the *Number of Authorizations* field.

Number of Authorizations: 20

c) List of authorization objects:

- S_RFC
- S_TCODE (twice)
- S_SECPOL
- S_TABU_DIS
- S_USER_AGR (three times)
- S_USER_AUT (twice)

- S_USER_GRP (three times)
- S_USER_PRO (twice)
- S_USER_SAS
- S_DEVELOP (twice)
- S_OC_SEND
- PLOG

5. Log off as user GR##-ADM and log on again as user ADM940-##.

- a) In the session for user GR##-ADM, choose *System → Log Off* in the menu.
- b) Start/Choose SAP Logon.
- c) Select system T41 and choose *Log On*.
- d) Log on with user ADM940-##.

Task 7: Create Users Using the User Mass Maintenance Transaction

Create additional user master records using the *User Mass Maintenance* transaction.

1. Start the *User Mass Maintenance* transaction.

- a) SAP Menu:
→ *Tools → Administration → User Maintenance → User Mass Maintenance*,
(transaction code SU10).

2. Create the following six user names.

User Name
GR##-FI1
GR##-FI2
GR##-SD1
GR##-SD2
GR##-MM1
GR##-MM2

- a) In the *User* column, enter the user names listed in the table and choose the *Create (F8)* icon.

3. Assign the user group ZGR## to all users.

- a) Select the *Logon Data* tab page.
Enter **ZGR##** in the *User group* field.

4. Assign the log-on language that you have used yourself for logging on.

- a) Select the *Defaults* tab page.
Enter the log-on language of your choice in the *Logon Language* field.

5. Save your user master record.

- a) Choose *Save (Ctrl+S)* to save your result and to create the users.

6. Check the result in the change log for a given user entry.

You can copy the generated initial passwords into the tables in the exercise section.



Hint:

Passwords of 40 characters in length are automatically generated. If you want, you can copy the generated passwords from the log to the following table, or change them directly for future tasks in transaction SU01 when required, using the *Change Password* button (Shift+F8).

User name	Generated Password
GR##-FI1	
GR##-FI2	
GR##-SD1	
GR##-SD2	
GR##-MM1	
GR##-MM2	

- a) The result including the generated password is shown in the *Mass User Changes* protocol.



Hint:

Another option is to copy the log information to the *SAP Business Workplace* area using the *Export/Office* function, from where it can be called again at any time (SBWF), into "Private Folders" with a free *Title*.

7. You can copy the generated initial passwords into the tables in the exercise section.



LESSON SUMMARY

You should now be able to:

- Manage user data and the user master record.

Understanding the Business User Concept



LESSON OBJECTIVES

After completing this lesson, you will be able to:

- Understand the Business User Concept.

Business User Concept

As most SAP users are employees of the company, their master data, such as name, e-mail address, etc., is maintained multiple times: as employees in the HR system, in the user master in SU01 and as business partners of the employee type.

In the classic user concept all three entities use their own data repository. Data changes have to be maintained within all participating entities separately.

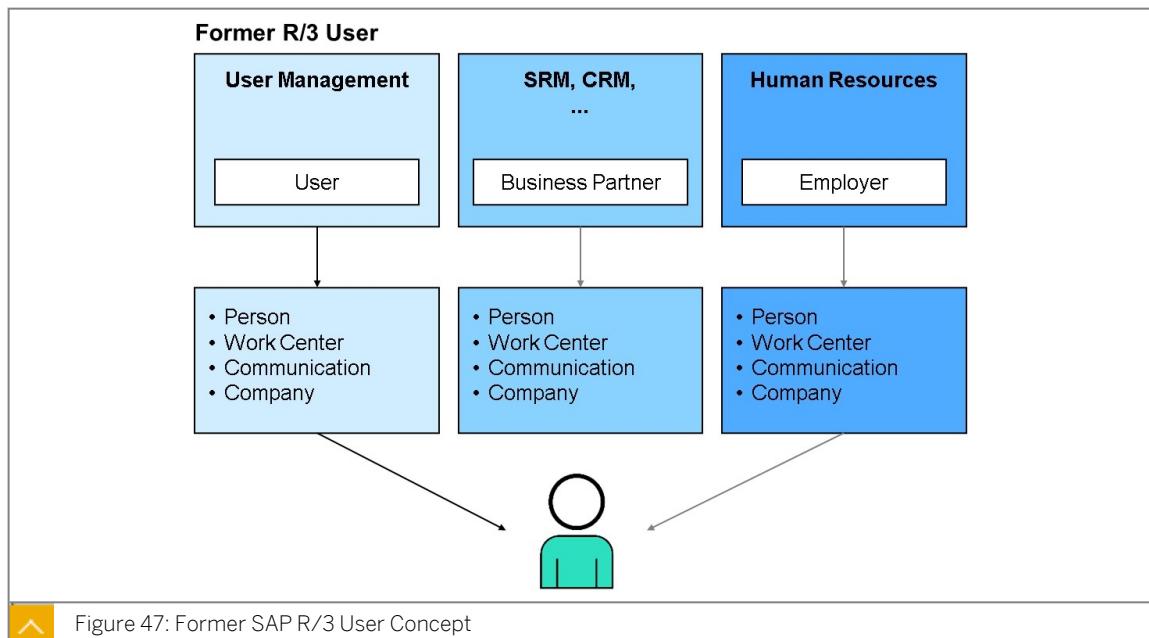


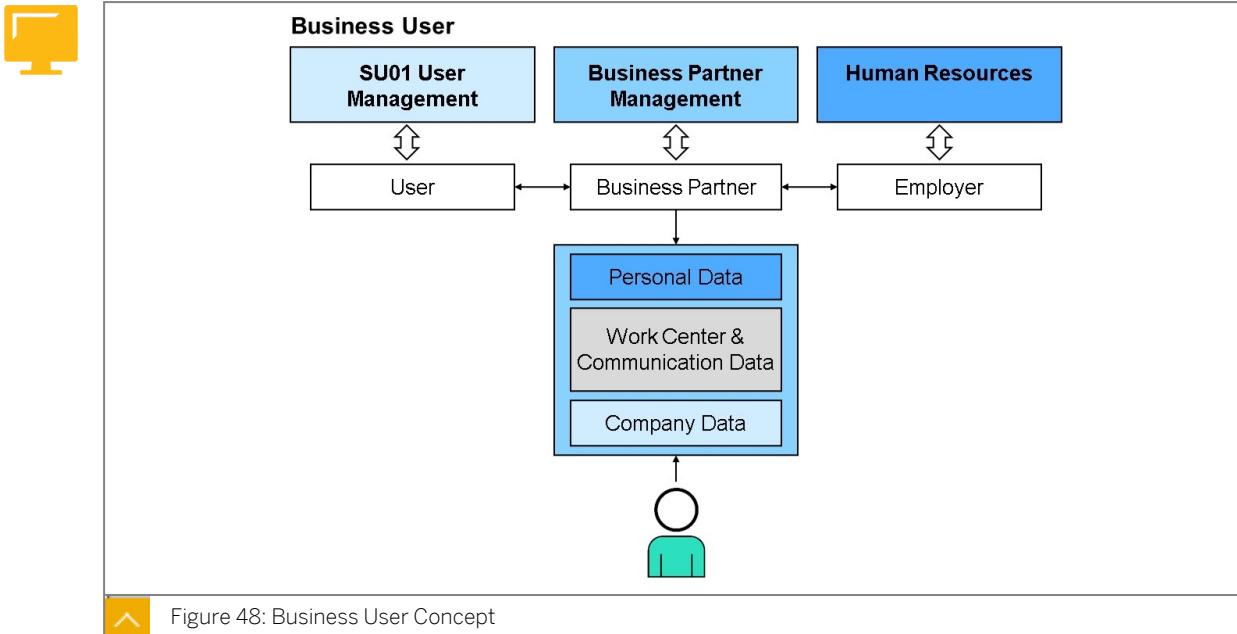
Figure 47: Former SAP R/3 User Concept

This harbours the risk of inconsistencies and also generates additional maintenance work. The business user concept is designed to avoid this.

SAP S/4HANA is introducing a new identity model for business users, which is based on the "principle of one". A business user is defined as a natural person who is represented by a business partner and a link to a user in the system. Business users interact with the software in the context of a business process, for example, in the role of a purchaser, a sales representative, or a production planner.

SAP S/4HANA Business User Management enables and supports the entire life cycle of business users such as organizational changes, change of employment, or retirement. A user in SAP S/4HANA has a one-to-one relationship with a corresponding business partner.

(natural person). This reduces redundant maintenance and prevents outdated information. Personal data and workplace address data can be obtained centrally.



User and Business User

The business user is a SU01 user, but also has a one-to-one relation to the corresponding business partner. This relationship is time independent and cannot be changed anymore.

The business user concept is used in many new applications in SAP S/4HANA. SU01 users with Classic Address (Identity Address Type 00 - User's Old Type 3 Address) lead to limitations because the new business user model is a prerequisite for many business applications. As soon as Fiori apps are activated and used, business users are mandatory (for example Teams, CreditAnalyst in Credit Management or Situations).

The business partner contains the personal information, for example private address, workplace address, bank details, vendor and customer related data. The business partner and SU01 user share personal details and workplace address related data. The advantage of the new business user model is that the entire lifecycle of that person works without redundant maintenance of user address data. Business users can still be managed using transaction SU01, Central User Administration or identity management systems.



Note:

In the SAP Business Suite, you can use transaction BP (Business Partner Maintenance) to assign users to business partners. In SAP S/4HANA this is not possible anymore to avoid an inconsistent data model for business users. Existing business partners cannot be converted to business users, because of Data Protection and Privacy (DPP). Already existing business partners could have been part of a distribution scenario.

With the new business user model in SAP S/4HANA we have a clear maintenance ownership. It can be owned by Human Capital Management (HCM), Business Partner (BP) or User Management. The ownership of HCM is only relevant when HCM integration is active.

Using the example of SU01 the following data categories exist:

Person

The personal data for the business user is derived from the corresponding business partner. In case HCM integration is active this data is mapped from the corresponding employee of the HCM system (SAP SuccessFactors or SAP HCM).

Work Center

The work center data for the business user is derived from the workplace address of the corresponding business partner. In case HCM integration is active, the function and department fields are mapped by default from the corresponding employee of the HCM system.

Communication

The communication data for the business user is derived from the workplace address of the corresponding business partner.

Company

During the conversion of a SU01 user from SAP Business Suite (classic user) to a business user in SAP S/4HANA the company address is copied to the business partner workplace address.

The business partner data are centrally hosted. The assignment between business partner and user is always 1:1. You can assign one user to each business partner.



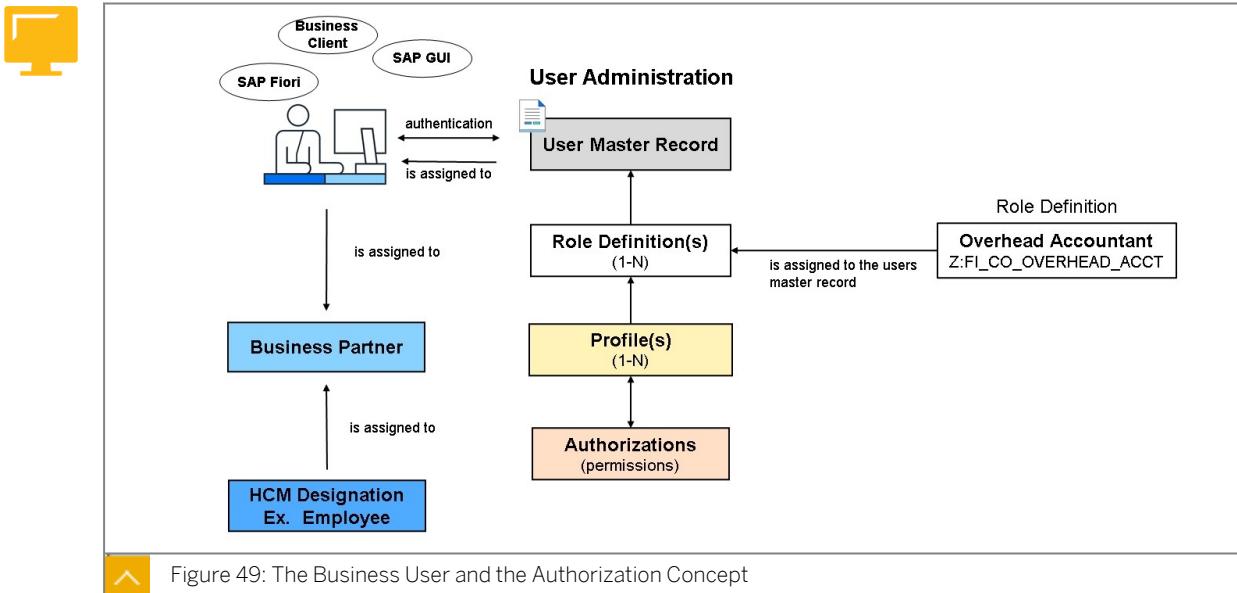
Note:

Users can still be maintained in SU01. The business user merely provides an additional option for user master data maintenance.

However, business users can only be created for employees and, if applicable, business partners. Technical users, for example for interfaces (RFC) or batch processing as well as other, non-personal users must be managed in SU01 as before.

Business User and the Authorization Concept

The following figure shows the relationship between the business user and the authorization concept and indicates how they relate to the role of User Administrator.



A business user is defined as a natural person who logs on to the SAP system to interact with the software in the context of a business process, for example, in the role of a cost accountant.

Each business user is represented in the system by a unique user ID. This user ID is defined in a User Master Record, and is assigned to the user. The user master record provides a place to maintain all the basic data for a user, such as their user ID, first name, last name, phone number, and so on.

The business user ID is automatically mapped (1:1) with a Business Partner definition that provides a workplace address and the application-specific context required to perform specific business functions. This is done using an associated business partner role.

Integrating the user ID and the business partner centralizes the maintenance of the work center and communication data, along with the company address data into a central data model.

This data model can be further enhanced by activating SAP HCM integration, which links the user master record and business partner directly with the users HR record. When HR integration is active, personal data for the business user is maintained directly in the HR system.

In SAP S4HANA, access to business functionality is controlled using authorization roles. These roles are designed and tailored for a particular position or job and contain the authorizations needed to execute the programs and applications necessary to perform that job. Authorizations represent the specific permissions required to perform each business function.

The user administrator is responsible for assigning or provisioning role definitions for the business user. The User Administrator assigns each role to the user master record for a set period of time. The system uses this “validity period” to reconcile the role assignment to the user master record by linking the role to its Profile.

Profiles are generated when the role definition is created and contain the authorizations needed for the applications, programs, and reports defined in the role. Profile assignment makes the authorizations available to the business user when they execute an application, a transaction, or a report.

Create a user master record for a business user



There are 2 variants for creating an employee master record:

If the HCM integration is active you can maintain business users via

- Transaction PA30 and PA40
- HCM integration

The screenshot shows the SAP Personnel Actions interface. In the search bar, 'Personnel no.' is set to '1384', 'Name' is 'User Business', 'EE group' is '1 Active', and 'EE subgroup' is 'Y1 Employees'. Below the search bar, there are icons for collective search help, search term, and free search.

If the HCM integration is inactive, you can maintain business users via

- Fiori app Maintain Employees

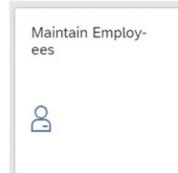


Figure 50: Creating an Employee Master Record

HCM integration active means that you rely on the HR mini master (HR infotype based PERNR data model including the PA-Tables). This HR mini master can be locally maintained (for example via transaction PA30 or PA40) or via real integration scenarios with SAP SuccessFactors Employee Central or an external (third party) HCM system.

Create a Business User using PA30 and PA40

The prerequisite for this scenario is that HCM integration is active.

Using transaction PA40, an employee must be created in HCM to whom a System ID is assigned in transaction PA30.

You then create a user for this System ID in SU01. The Maintain Users screen indicates that this is a user with business partner assignment.



PA40: Create an employee

The screenshot shows the SAP PA40: Create an employee screen. The 'Personnel no.' field is set to '1384', 'Name' is 'User Business', 'EE group' is '1 Active', and 'EE subgroup' is 'Y1 Employees'. The 'Name' section includes fields for Title, Last Name, First Name, Name prefix, Title, and Other title. The 'Additional data' section includes fields for Gender, Birth date (01.01.2000), Birthplace, C/R Birth, State, Nationality (GB British GB), and 2nd/3rdNat.

PA30: Maintain SystemID

The screenshot shows the SAP PA30: Maintain SystemID screen. The 'Personnel no.' field is set to '1384'. The 'Basic personal data' tab is selected, showing sections for Infotype Text, Actions, Organizational assignment, Personal data, Addresses, and Communication. The 'Display Communication' section shows a communication entry for Type '0001 System user name (SY-UNAME)' and System ID 'ADM940-BU'.

Figure 51: Create an Employee using PA40 and PA30



SU01 : Create User

User Maintenance: Initial Screen

User **ADM940-BU**

Alias

Maintain Users

User **ADM940-BU** User with Business Partner Assignment (Business Partner: 9980001574)

Changed By Status Not saved

Documentation Address Logon Data SNC Defaults Parameters Roles Profiles

Person

Title: User
Last Name: User
First Name: Business
Academic Title:
Full Name: Business User
Language: EN English

Figure 52: Create User with Business Partner Assignment (Variant 1)

Create a Business User using Maintain Employees App

The prerequisite for this scenario is that HCM integration is not active.

You can use the SAP Fiori app to create a business partner of the type Employee. The employee is assigned an Employee ID and a User ID. Therefore start SAP Fiori App Maintain Employees and choose Create. Then create an Employee with Employee ID and User ID.



Maintain Employees

Maintain Employees

Standard

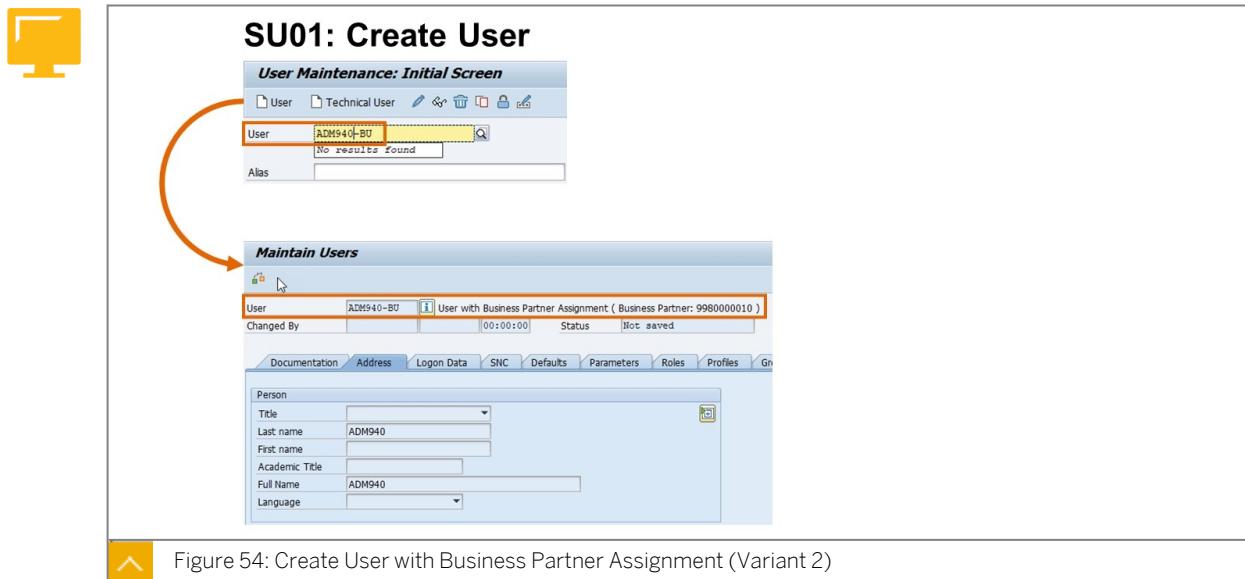
Employee ID: **ADM940-EMPLOYEE**

First name: **ADM940**

User ID: **ADM940-BU**

Figure 53: Create an Employee using Maintain Employees App

You then create a user for this User ID in Su01. Start transaction SU01 to create an SU01 user. Enter the User ID in the User field and choose Create User. The Maintain Users screen indicates that this is a user with business partner assignment.



Unit 3 Exercise 4

Practice System Exercise: Create a user master record for a business user

Business Example

As most SAP users are employees of the company, their master data, such as name, e-mail address, etc., is maintained multiple times: as employees in the HR system, in the user master in SU01 and as business partners of the employee type.

To avoid the risk of inconsistencies and additional maintenance work you can create a business user where personal data and workplace address data can be maintained centrally.

A business partner of role employee to whom the System ID *GR##-BU* was created in HCM using transaction PA40 and transaction PA30.

Task 1: Check that a business partner has already been created

Create a user master record for business user with the System ID *GR##-BU*. The Maintain Users screen indicates that this is a user with business partner assignment.

1. Start transaction *Maintain Business Partner (BP)*.

Task 2: Create a user master record for a business user

Create a user master record for business user with the System ID *GR##-BU*. The Maintain Users screen indicates that this is a user with business partner assignment.

1. Start transaction *User Maintenance (SU01)*.
2. Enter an initial password of your choice and assign the user to user group *ZGR##*.
Initial password: Init1234
3. Assign the log-on language that you have used yourself for logging on.
4. Save your user master record.

Task 3: Assign a Predefined Role to Your New User Master Record

Assign a predefined role *ADM940_SD_SALES* to the user master record of the user **GR##-BU**.

1. Start transaction *User Maintenance (SU01)*.
2. Save your user master record.

Task 4: Check the User Name assigned to the business partner.

Check the assignment of the user name *GR##-BU* to the business partner *Business User##*.

1. Start transaction *Maintain Business Partner (BP)*.

Unit 3 Solution 4

Practice System Exercise: Create a user master record for a business user

Business Example

As most SAP users are employees of the company, their master data, such as name, e-mail address, etc., is maintained multiple times: as employees in the HR system, in the user master in SU01 and as business partners of the employee type.

To avoid the risk of inconsistencies and additional maintenance work you can create a business user where personal data and workplace address data can be maintained centrally.

A business partner of role employee to whom the System ID **GR##-BU** was created in HCM using transaction PA40 and transaction PA30.

Task 1: Check that a business partner has already been created

Create a user master record for business user with the System ID **GR##-BU**. The Maintain Users screen indicates that this is a user with business partner assignment.

1. Start transaction *Maintain Business Partner (BP)*.
 - a) Choose SAP Menu: → *Logistics* → *Transportation Management* → *Master Data* → *Maintain Business Partner, (transaction code BP)*.
 - b) Select **2 Search Term** in the *By* field.
 - c) Enter **User##** in the *Search Term 1* field and choose *Start*.

Result

The business partner *Business User##* is displayed.

Task 2: Create a user master record for a business user

Create a user master record for business user with the System ID **GR##-BU**. The Maintain Users screen indicates that this is a user with business partner assignment.

1. Start transaction *User Maintenance (SU01)*.
 - a) Choose SAP Menu: → *Tools* → *Administration* → *User Maintenance* → *Users, (transaction code SU01)*.
 - b) Enter **GR##-BU** in the *User* field and choose *Create (F8)*.
- #### Result
- The *Maintain Users* screen shows that the user **GR##-BU** has been created with business partner assignment: *User with Business Partner Assignment*.
- c) Select the *Address* tab page.
The values for the last name and the first name have been taken over from the assigned business user.
 - d) Select the *Documentation* tab page.
- 102
- © Copyright. All rights reserved.

Enter **ADM940-##** in the *Person Responsible* field.

2. Enter an initial password of your choice and assign the user to user group ZGR##.
Initial password: Init1234
 - a) Select the *Logon Data* tab page.
Enter **Init1234** in the *New Password* and the *Repeat Password* field.
Enter **ZGR##** in the *User group* field.
3. Assign the log-on language that you have used yourself for logging on.
 - a) Select the *Defaults* tab page.
Enter the log-on language of your choice in the *Logon Language* field.
4. Save your user master record.
 - a) Choose *Save* (*Ctrl+S*).
 - b) Go back to the SAP *Easy Access* menu.

Task 3: Assign a Predefined Role to Your New User Master Record

Assign a predefined role **ADM940_SD_SALES** to the user master record of the user **GR##-BU**.

1. Start transaction *User Maintenance* (SU01).
 - a) Choose SAP Menu: → *Tools* → *Administration* → *User Maintenance* → *Users*, (**transaction code SU01**).
 - b) Enter **GR##-BU** in the *User* field and choose *Create* (F8).
 - c) Select the *Roles* tab page.
 - d) On the *Roles* tab, enter **ADM940_SD_SALES** in the *Role* column and press *Enter*.
2. Save your user master record.
 - a) Choose *Save* (*Ctrl+S*).
 - b) Go back to the SAP *Easy Access* menu.

Task 4: Check the User Name assigned to the business partner.

Check the assignment of the user name **GR##-BU** to the business partner *Business User##*.

1. Start transaction *Maintain Business Partner* (BP).
 - a) Choose SAP Menu: → *Logistics* → *Transportation Management* → *Master Data* → *Maintain Business Partner*, (**transaction code BP**).
 - b) Select **2 Search Term** in the *By* field.
 - c) Enter **User##** in the *Search Term 1* field and choose *Start*.

Result
The business partner *Business User##* is displayed.
- d) Double-klick on the entry of your business partner *Business User##* in the list.
- e) Enter **BUP003 Employee** in the *Display in BP role* field and choose *Create* (F8).
- f) Select the *Identification* tab page.

Result
The user name **GR##-BU** of the employe is displayed in the *User Name* field.



LESSON SUMMARY

You should now be able to:

- Understand the Business User Concept.

Learning Assessment

1. User master records are client-specific.

Determine whether this statement is true or false.

- True
- False

2. Where is the personal data for a business user derived from if HCM integration is not active?

Choose the correct answer.

- A The corresponding employee of the HCM system
- B The corresponding business partner
- C The workplace address of the corresponding business partner
- D The company address

3. Which of the following data points are derived from the workplace address of the corresponding business partner?

Choose the correct answers.

- A Communication data
- B Work center data
- C Personal data
- D Company address

Learning Assessment - Answers

1. User master records are client-specific.

Determine whether this statement is true or false.

True

False

The statement is true. User master records are client-specific.

2. Where is the personal data for a business user derived from if HCM integration is not active?

Choose the correct answer.

A The corresponding employee of the HCM system

B The corresponding business partner

C The workplace address of the corresponding business partner

D The company address

The personal data for a business user is derived from the corresponding business partner when HCM integration is not active.

3. Which of the following data points are derived from the workplace address of the corresponding business partner?

Choose the correct answers.

A Communication data

B Work center data

C Personal data

D Company address

Both communication data and work center data are derived from the workplace address of the corresponding business partner.

UNIT 4

Working with the Role Maintenance

Lesson 1

Creating Standard Roles	108
Exercise 5: Practice System Exercise: Maintain Standard Roles	125

Lesson 2

Creating Customizing Roles	141
----------------------------	-----

Lesson 3

Implementing a Composite Role Strategy	143
--	-----

Lesson 4

Implementing a Derived Role Strategy	147
Exercise 6: Practice System Exercise: Maintain Special ABAP Roles	151

Lesson 5

Outlining Subtleties of Authorization Maintenance	168
Exercise 7: Practice System Exercise: Understand the Subtleties of Authorization Maintenance	177

UNIT OBJECTIVES

- Manage business roles, profiles and authorization data.
- Create the project team customizing roles.
- Implement a composite role strategy.
- Implement a derived role strategy.
- Describe the special features in SAP Business Role Maintenance.

Unit 4

Lesson 1

Creating Standard Roles

LESSON OVERVIEW

There are two lessons about role maintenance, covering simple and advanced maintenance with the Role Maintenance. This lesson contains the basic role maintenance functions and the automatic generation of SAP Easy Access user menus for various work centers and the associated authorizations, profiles, and user assignments.

Business Example

When you create authorizations and authorization profiles for groups of users, you should use the Role Maintenance. Based on selected menu functions, the Role Maintenance automatically generates authorization data and offers it for postprocessing. The authorization data assigned in this way is combined into profiles and can be assigned indirectly to users through roles.



LESSON OBJECTIVES

After completing this lesson, you will be able to:

- Manage business roles, profiles and authorization data.

Basic Maintenance of Roles Using Role Maintenance



What is Role Maintenance?

Role Maintenance is the central tool for generating authorizations and authorization profiles and assigning them to users.

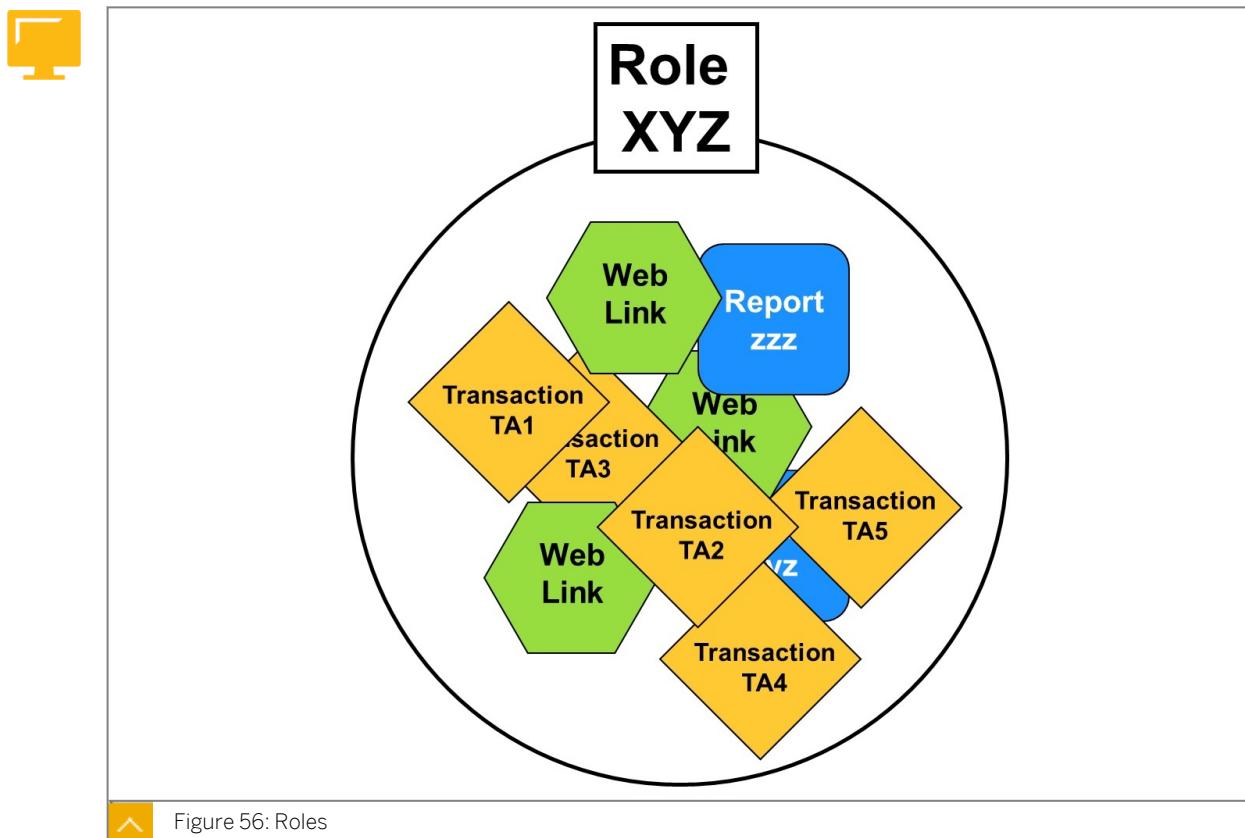
In Role Maintenance, system administrators choose transactions, menu branches (from the SAP menu) or area menus. The functions chosen correspond to the field of activity of a user or a group of users. Role Maintenance offers two different maintenance views:

- Basic maintenance (menus, profiles, and other objects)
- Complete view (Organizational Management and workflow)

The menu tree set up by system administrators for users with a specific role in the company corresponds to the user menu that appears if a user (to whom the corresponding role is assigned) logs on to the SAP system.

Role Maintenance automatically provides the corresponding authorizations for the functions chosen. Some of these authorizations have default values. Traffic light symbols tell you which values you need to maintain.

Finally, Role Maintenance generates an authorization profile from this data, which you can assign through the role.



What are roles?

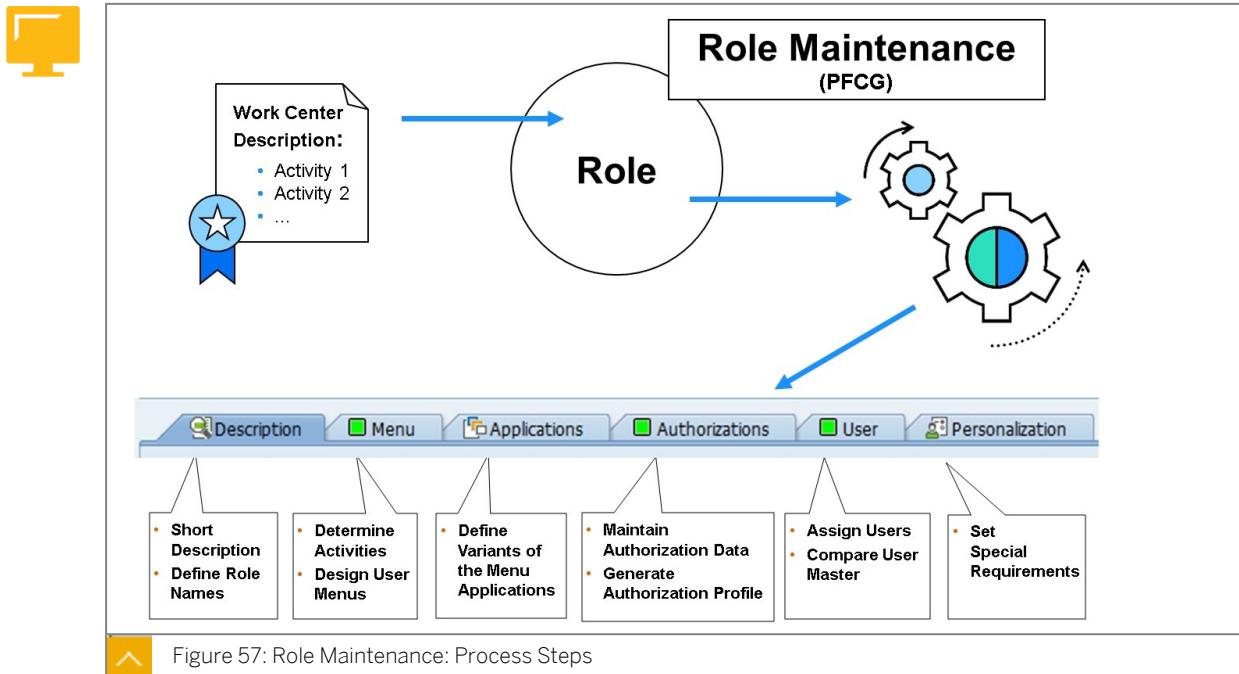
A role is a set of functions describing a specific work area. The “Accounts Receivable Accountant” role, for example, contains transactions, reports, and/or Internet/Intranet links that an accounts receivable accountant needs for his or her daily work. Through roles, you also assign the authorizations that the user, in the example, the accounts receivable accountant, needs to access the transactions, reports, and so on, contained in the menu.

Roles are used to implement the menus that users can work with after they have logged on to the SAP System. You can use roles predefined by SAP and roles that you have created

yourself. You can find the predefined roles using the “F4” help under SAP Menu: Tools Administration User Maintenance Role Administration Roles, or using the menu path Menu → Display Role Menu, or by choosing the “Other Menu” button.

You can use the report RSUSR070 to display the role templates that are delivered by SAP.

In addition to the normal “Login” users, you can assign object types such as jobs, organizational units, or positions to roles. This is referred to as integration using Organizational Management.



All the work steps you need to perform to create a role, including assigning the role to the user, are listed in the following as a thread.

To call Role Maintenance, choose “Create menu” on the SAP Easy Access initial screen, or choose the following menu path: Tools → Administration → User Maintenance → Role Administration → Roles. The corresponding transaction code is “**PFCG**”.

Thread

- The first step is defining the role and entering a short description of its contents.
- In the second step, you define the activities for the user role. The result of this definition process is a role (or several roles) that collects all activities of the role - represented by means of transactions, reports, and Web addresses.
- Simultaneously, you define what the menu tree for the new user role should look like.
- Thereafter, the authorizations for the activities selected are created and profiles generated. This step normally involves the greatest administrative maintenance effort.
- Subsequently, the users are assigned to the roles.
- Finally, depending on the settings in PFCG, the comparison with the user master records of the users which have just been assigned to the roles is performed.

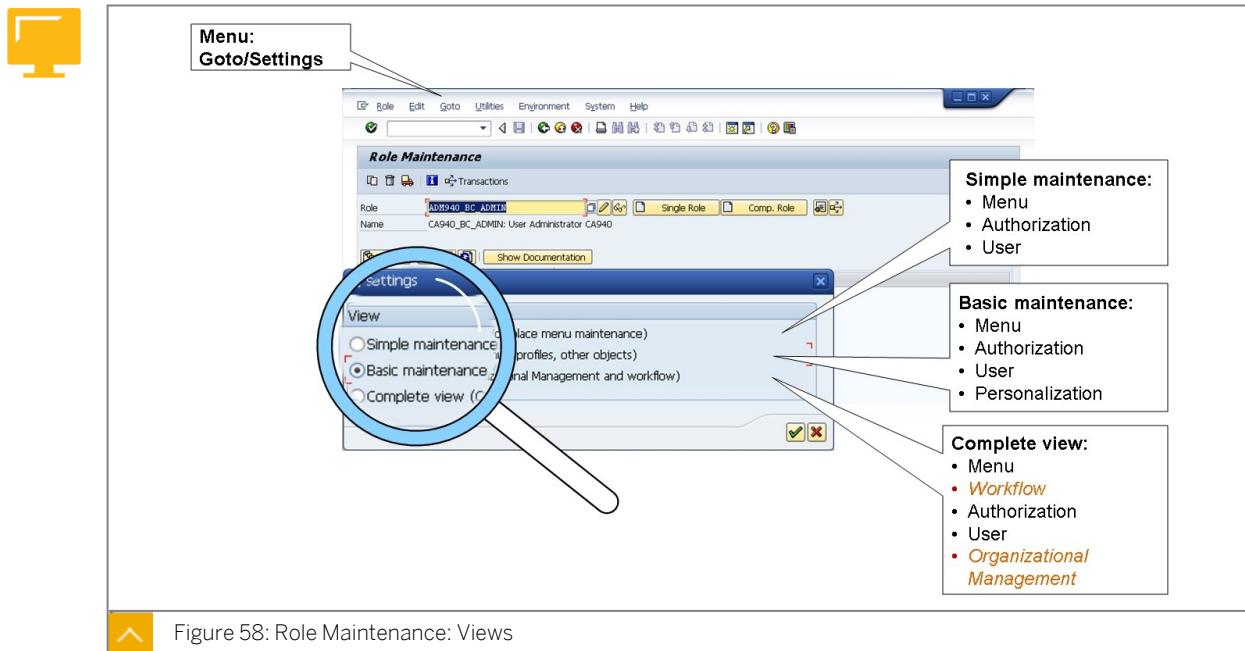


Figure 58: Role Maintenance: Views

Basic Maintenance allows you to:

- Access all of the functions for role maintenance
- Assign the roles only to SAP users

The **Complete View** (Organizational Management) displays all assignments and data for a role.

This view is useful for users in Personnel Planning and Development, particularly for organizational management and workflow. The Complete View allows you to:

- Access all of the functions for role maintenance
- Change the validity time period of the role
- Link tasks with a role
- Assign the role to objects in the organizational plan and restrict the validity dates for each assignment

To make the process of creating a role easier to remember, all process steps are shown repeatedly in the form of a "to do" list in this lesson.

Define Role Name

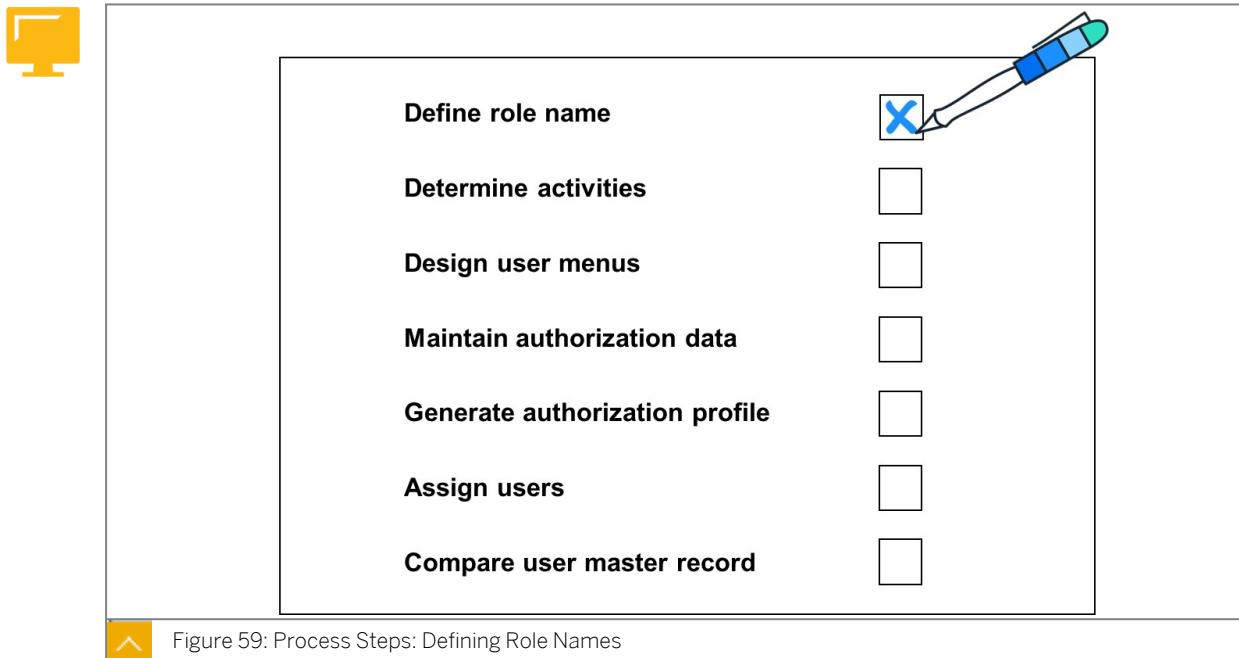


Figure 59: Process Steps: Defining Role Names

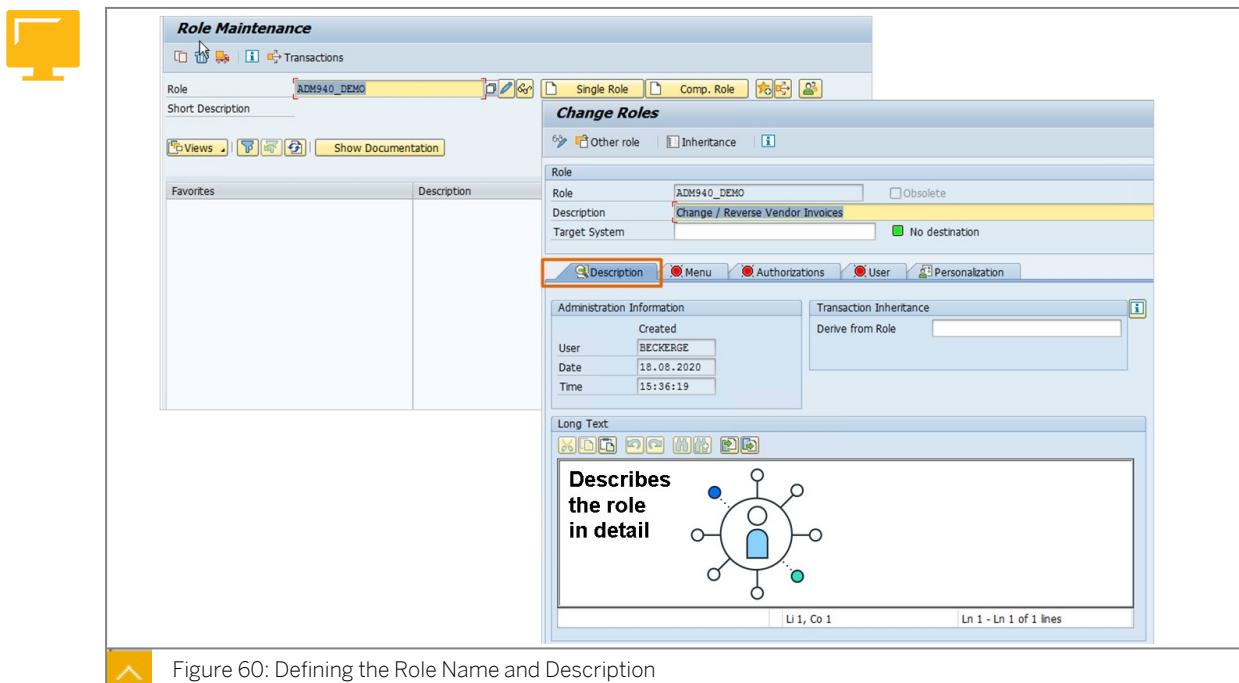


Figure 60: Defining the Role Name and Description

Note that the roles delivered by SAP start with the prefix “SAP_” and can be used as templates. If you want to create your own user roles, do not use the SAP namespace.

**Caution:**

Roles with the “SAP_” prefix **may be overwritten** during an upgrade or when relevant Support Packages that contain roles of the same name are imported. It is therefore recommended that you only use these roles as templates. When they then exist in the customer namespace, they can be adapted to meet the requirements.

SAP does not use different names for single and composite roles. When creating or naming your roles, you should consider a naming concept that differentiates between single and composite roles. It is also useful to include a system abbreviation in the naming concept.

**Hint:**

Up to 30 characters are available to you for the role name. The name that you select, however, is **not language-dependent**.

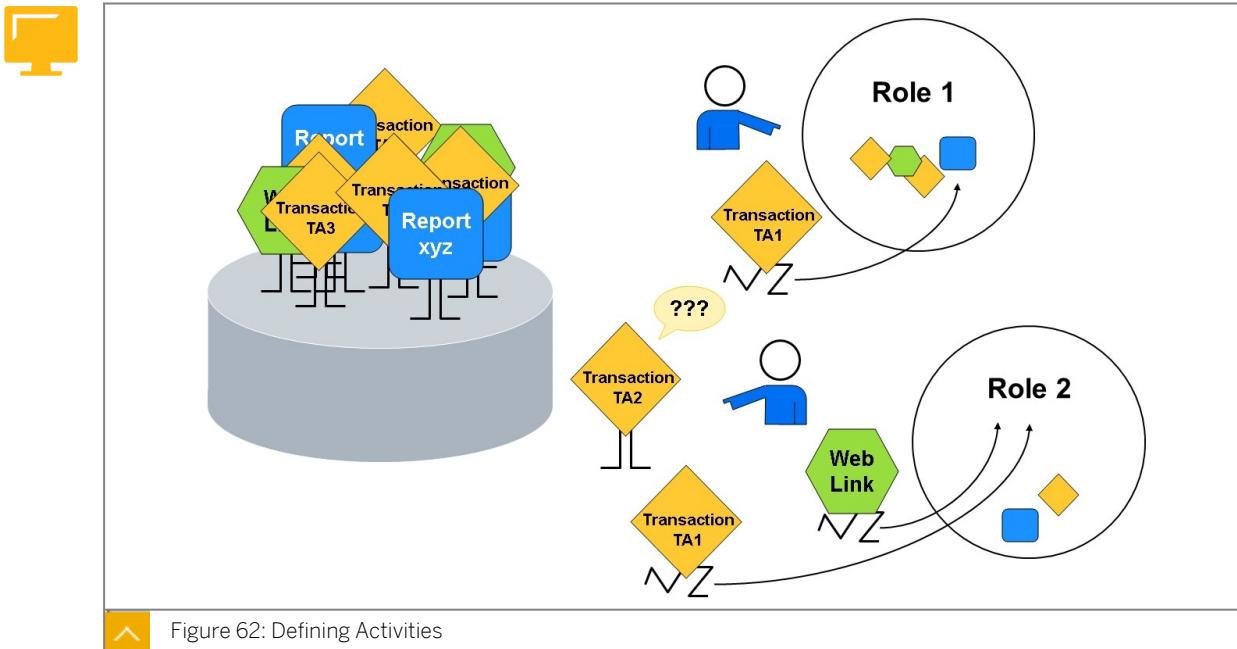
Determine Activities and Design User Menus



Define role name	<input checked="" type="checkbox"/>
Determine activities	<input checked="" type="checkbox"/>
Design user menus	<input type="checkbox"/>
Maintain authorization data	<input type="checkbox"/>
Generate authorization profile	<input type="checkbox"/>
Assign users	<input type="checkbox"/>
Compare user master record	<input type="checkbox"/>



Figure 61: Process Step: Define Activities



Definition of the roles:

Using roles, you define which activities are assigned to a specific role in the company. The authorization administrator selects those transactions in Role Maintenance that users with a specific role in the company must perform regularly. The administrator also chooses any Web addresses if these are useful for the daily work of a role holder (for example, a weather forecast service would be of interest to field service personnel). In addition, frequently needed reports can also be added to the user menu.



Hint:

If, for example, a report is included, it is important to know the special features associated with this:

- If they are used in a role, reports always have a transaction code.
- The transaction code can be automatically generated by the system or specified by the administrator.
- If you assign a new transaction code although a transaction code has already been created for this report (for example, for another role), the system displays a message that informs you about the situation. If necessary, you can choose between the new and the old T codes.

You can create completely new roles if required. In most cases, however, it is easier to use the roles delivered by SAP as a **template**, to **copy** them, and then change them to meet your own requirements. You can choose the copy icon on the initial screen of transaction PFCG.

You have two options when copying:

1. “Copy selectively”

You decide what is copied.

2. “Copy all”

Personalization and user assignment are also automatically copied.

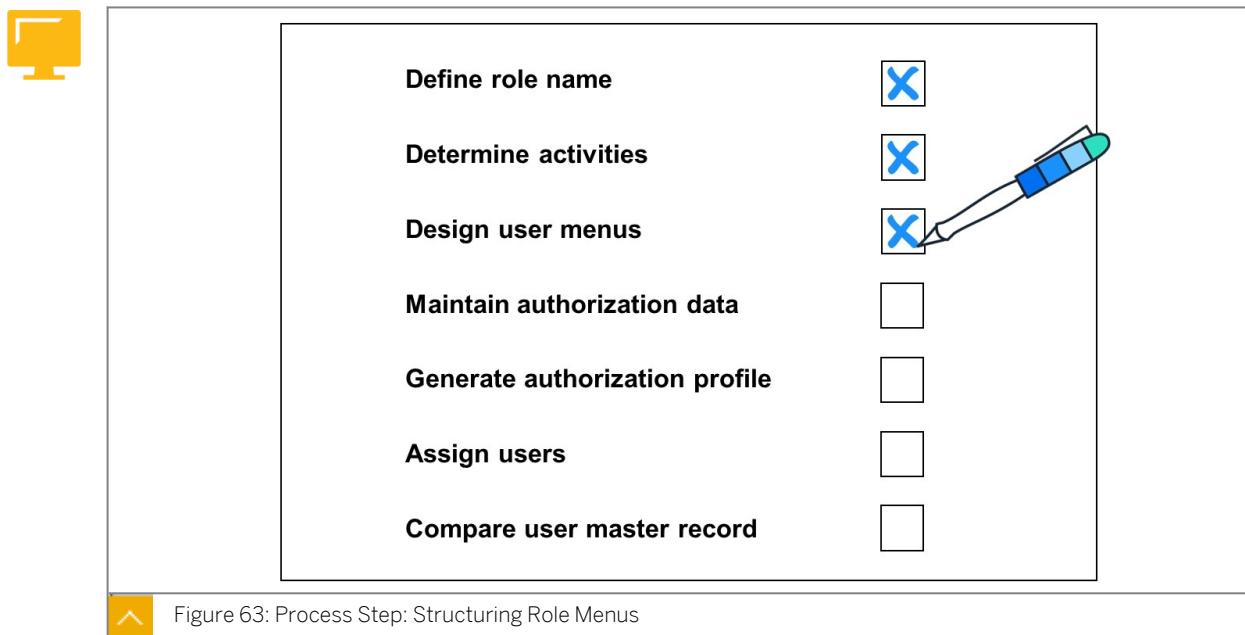


Figure 63: Process Step: Structuring Role Menus

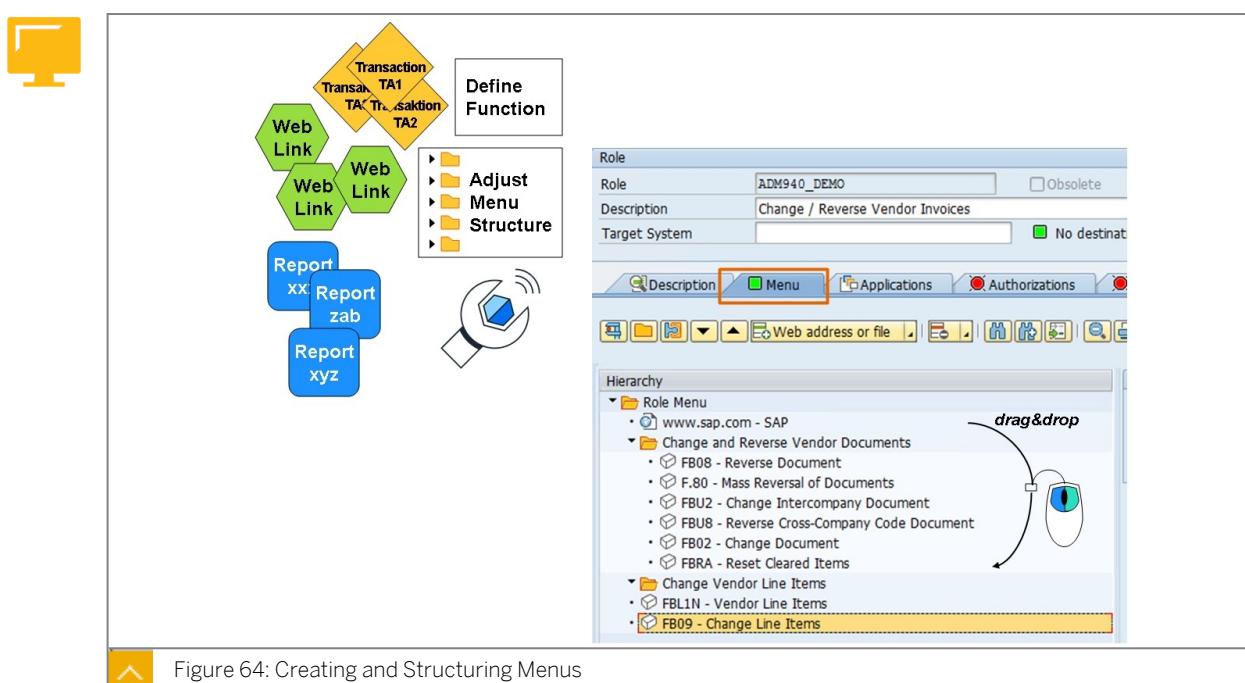


Figure 64: Creating and Structuring Menus

Changing the functions:

You can adjust the transactions listed in the menu tree of a role to meet your individual requirements:

- You can delete transactions that you do not need and add new ones (by choosing the "Transaction" button or by copying transactions "from other roles" or from other "menus").
- You can add reports (by choosing the "Report" button). Role Maintenance generates a transaction code (which is either created automatically or which you define yourself) that

can be used to start the report from the menu. You can also include queries, BW reports, and transactions with variants in this way.

- You can add Internet sites (by choosing the “Other” button). Similarly, you can add links to documents (such as Microsoft Excel files). You add links to documents in the same way as you add links to Internet pages. Instead of the URL, you then enter the path of the required file.



Hint:

When defining Web addresses or file paths, you can specify variables that are defined in transaction `SM30_SSM_VAR`. You should then enter the variables in upper case letters in angle brackets in the Web address, such as `<VARIABLE_NAME>`. When the Web address is started, the variable is automatically replaced by the associated value.

Changing the menus:

You can create, delete, move, or rename directories. The operation is similar to that of graphical file managers.

To distribute the role to a particular target system, choose *Distribute*. Note that the authorization data for the role is not distributed together with the role. You must therefore add the authorization data for distributed roles in the target system. There are other settings that you need to take into account for this distribution. For more information, see the *F1* help.

You can also use transaction `ROLE_CMP` to compare and adjust role menus across systems.



Show or hide applications with variants:

Show all applications:

		Description	Menu	Applications	Authorizations
		Only variants	All	All	All
Active	Type	Name	Variant	Description	
<input checked="" type="checkbox"/>	Transaction	F.80		Mass Reversal of Documents	
<input checked="" type="checkbox"/>		FB02		Change Document	
<input checked="" type="checkbox"/>		FB08		Reverse Document	
<input checked="" type="checkbox"/>		FB09		Change Line Items	
<input checked="" type="checkbox"/>		FBL1N		Vendor Line Items	
<input checked="" type="checkbox"/>		FBRA		Reset Cleared Items	
<input checked="" type="checkbox"/>		FBU2		Change Intercompany Document	
<input checked="" type="checkbox"/>		FBU8		Reverse Cross-Company Code Document	

Show only applications with existing variants:

		Description	Menu	Applications	Authorizations
		Only variants	All	All	All
Active	Type	Name	Variant	Description	
<input checked="" type="checkbox"/>	Transaction	F.80		Mass Reversal of Documents	

Figure 65: Application Variants

Show or hide applications with variants

The creation of application variants in transaction `SU24` (customer variants) or `SU22` (SAP standard variants) allows you to maintain authorization default values that are adapted to the special requirements of certain industry solutions. You replace or enhance the authorization default values of the source application so that you do not need to change default values in the authorization data maintenance of roles if the variants are designed optimally.

On the new *Applications* tab in transaction `PFCG`, the role administrator defines which variants of the menu applications of an individual role are taken into account in authorization data maintenance. However, all applications are displayed instead of just applications with variants. Following the implementation of this correction, two display options are available.

Regardless of the processing mode (display or change), a button is available in the *Applications* tab page to the left above the application list. You can use it to show or hide applications without variants. The displayed table text describes the application set to be expected when the button is pressed. Applications with variants are not affected; they are always displayed. If you only ask to see applications with variants, but the role menu contains only applications without variants, the list remains empty.

The last selected view is saved as a personal user setting in the database and is reused the next time transaction PFCG is called.

Maintain Authorizations Data and Generate Authorization Profile

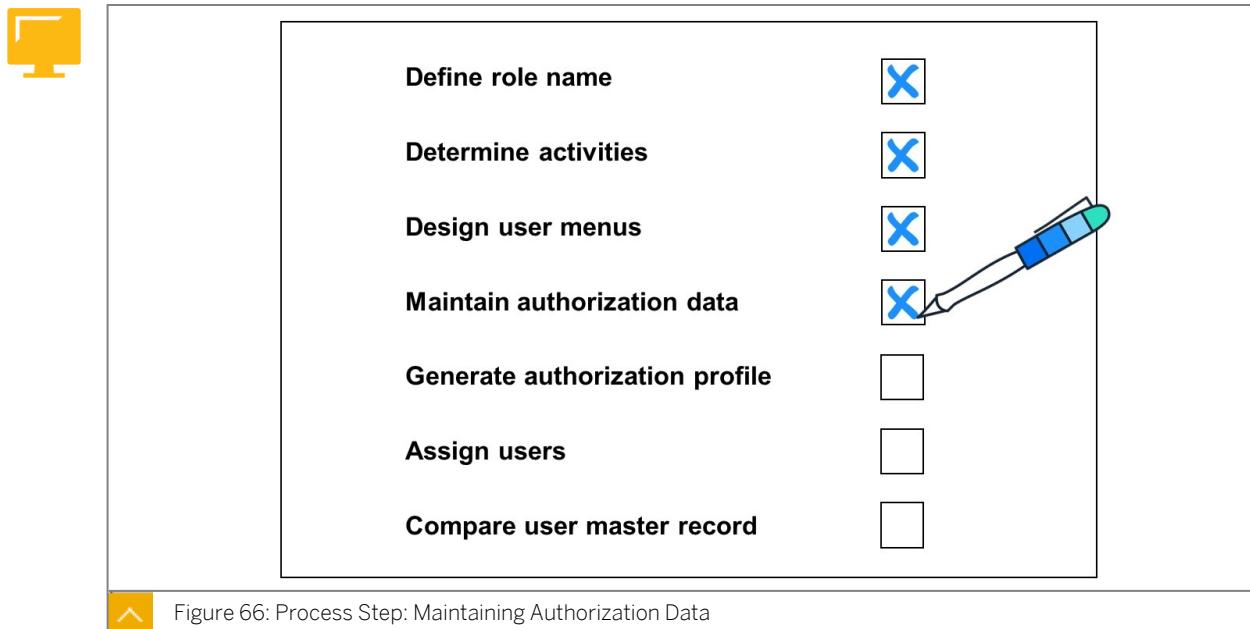


Figure 66: Process Step: Maintaining Authorization Data

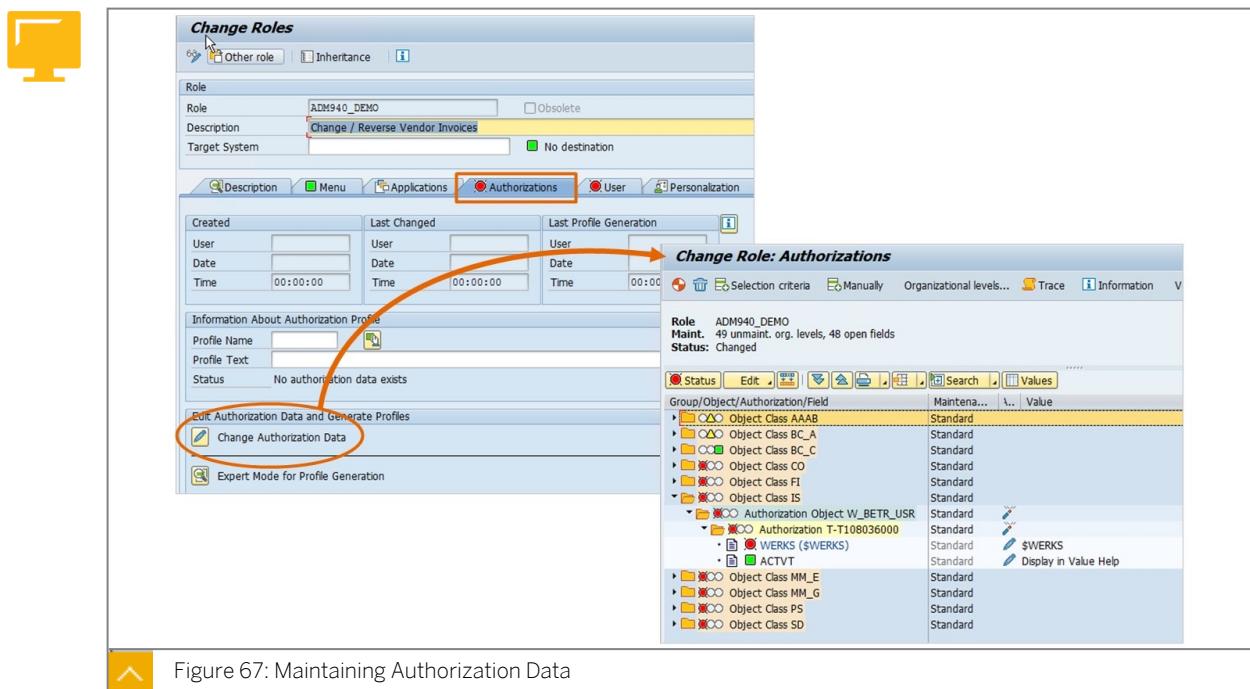
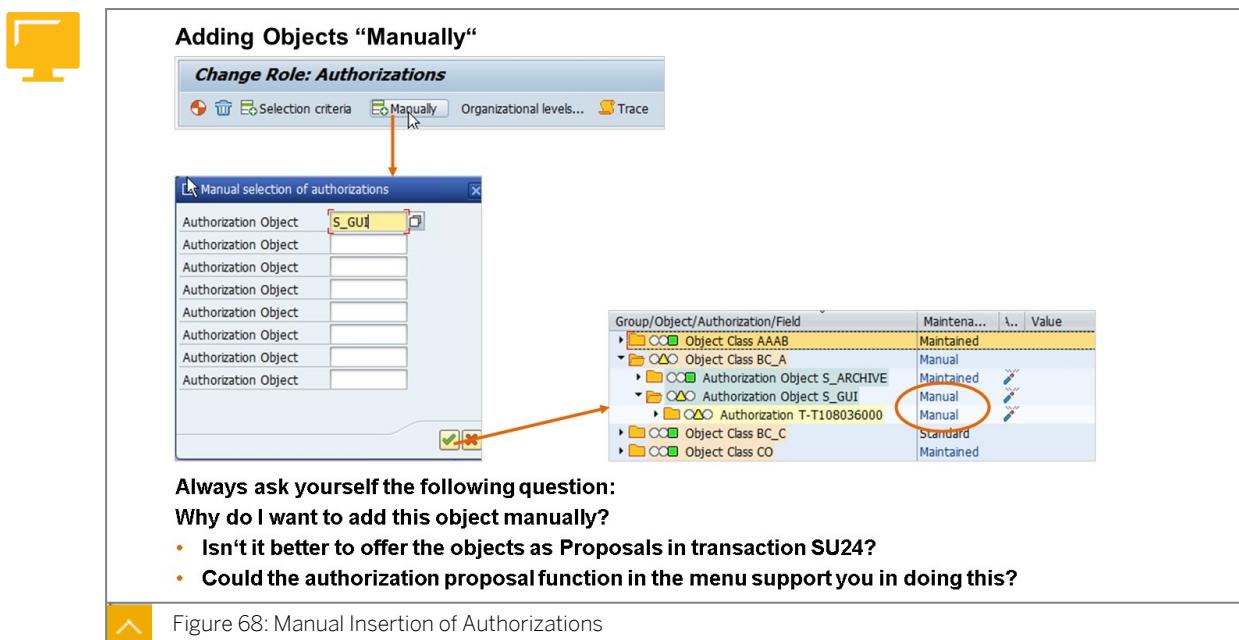


Figure 67: Maintaining Authorization Data

Creating the authorizations and authorization profiles:

Role Maintenance automatically generates authorizations based on the menu functions that you have chosen before. Role Maintenance cannot, however, propose “default value” authorizations that are suitable for everyone in the company. Therefore, the authorization administrator must normally post-process the authorizations manually in cooperation with the user departments and the audit division. By choosing “Organizational Levels”, you can simultaneously maintain a large number of authorization fields. This greatly simplifies the manual post-processing work.

In the example, the transaction S001 (SAP Office) was added to the role “MY_ROLE” (which was created by copying the SAP template). As a result, the yellow traffic lights appear in the menu tree in the above example. The authorization for file access is a good example to show why manual post-processing is necessary. Role Maintenance cannot know if the users should have only **read access** or also **write access** to the files.



Although Role Maintenance automatically generates the authorizations, you can also add authorizations manually to an existing profile, which might be desirable in some cases. To do this, choose the “Change Authorization Data” button on the “Authorizations” tab page, and then “Edit → Insert Authorizations”. The following options are available:

- Selection criteria:

Here you can find authorizations for objects grouped by object class.

- Manual input:

If you know the name of the authorization object for which you want to manually add authorizations, you can enter it here directly.

- Full authorization:

This option fills all authorizations with the value “*”.

- From profile...:

Here you can use authorizations from individual profiles.

- From template...:

If you want to create a user with “almost all” authorizations, you can use the SAP authorization templates designed for this purpose.

Question?

Why do you want to insert an object “manually”?

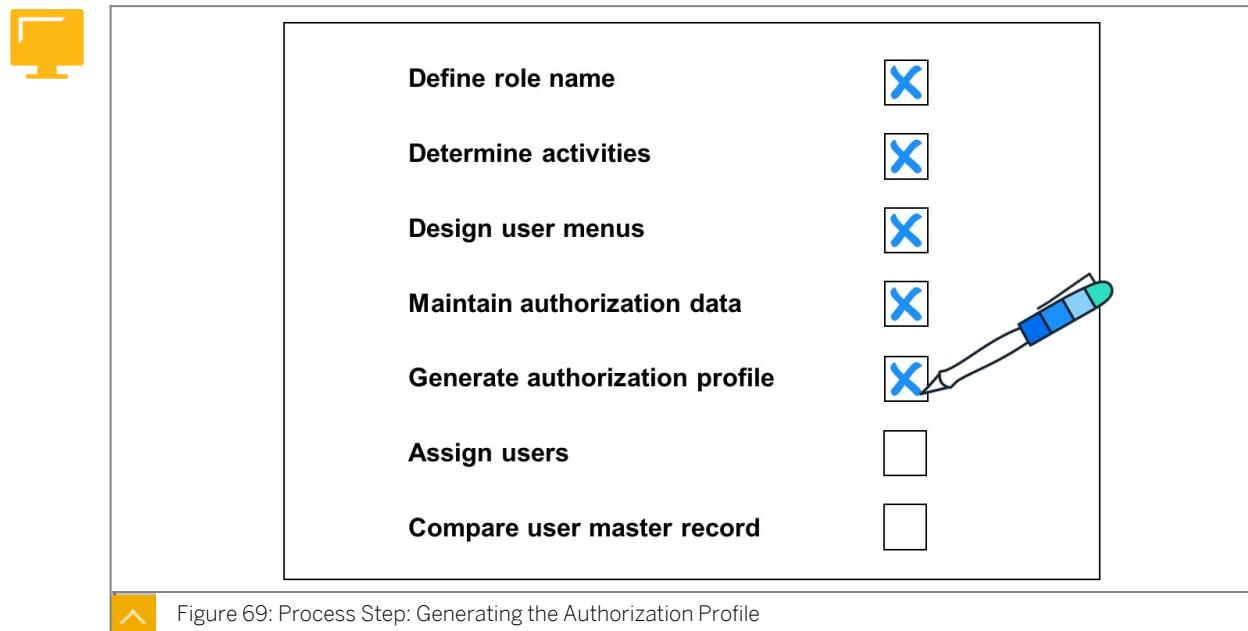
Why not allow Role Maintenance propose this object?

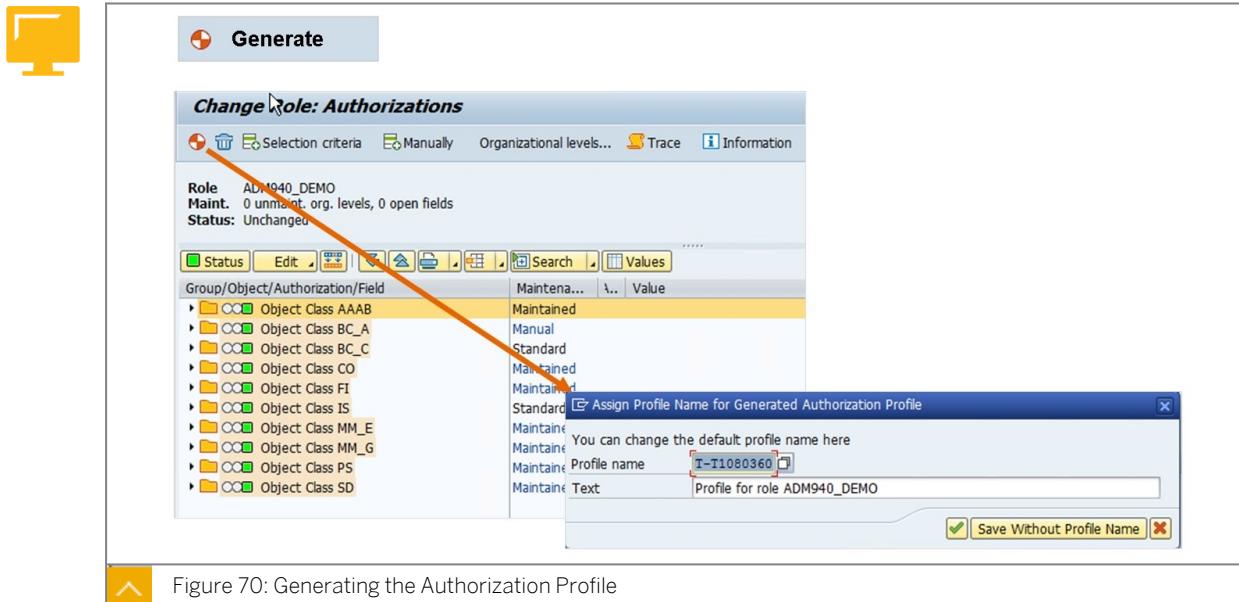
Is it sensible to insert an object manually?

You will often hear statements such as:

- It has been developed as part of the customer standard.
- It is missing from SAP's proposals.
- The end user is not meant to see it in the user menu (applies to S_TCODE) only.

For more information, see transaction SU24 (Maintain Assignment of Authorization Objects) or the function of the “Authorization Proposal” button on the “Menu” tab page.



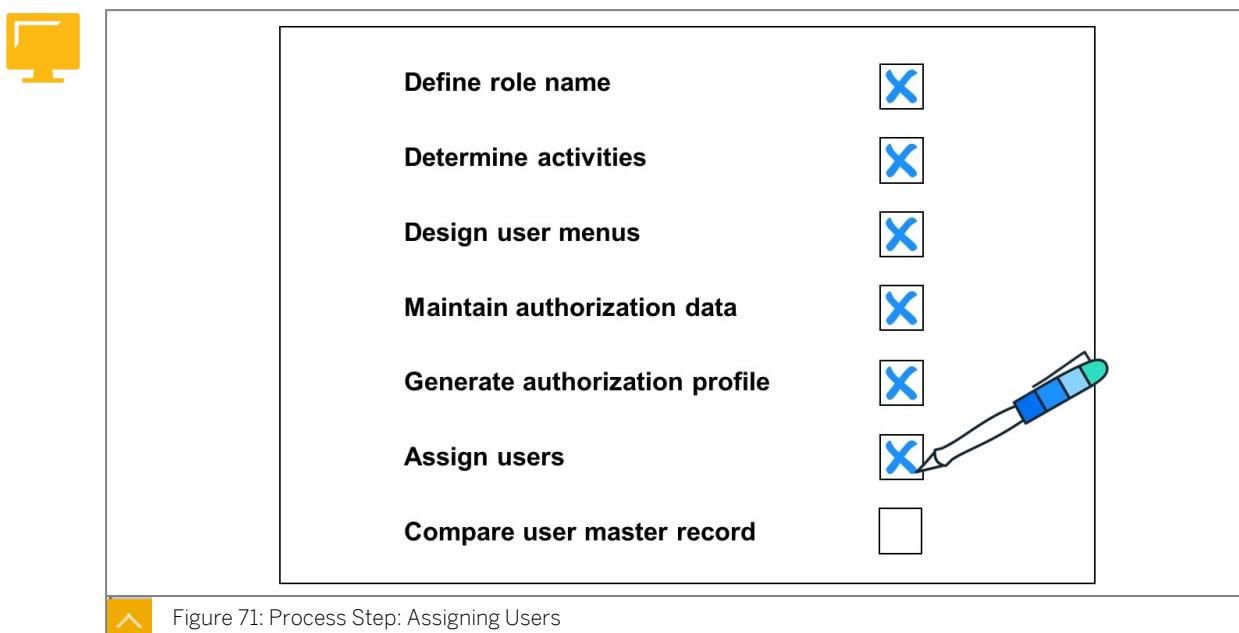


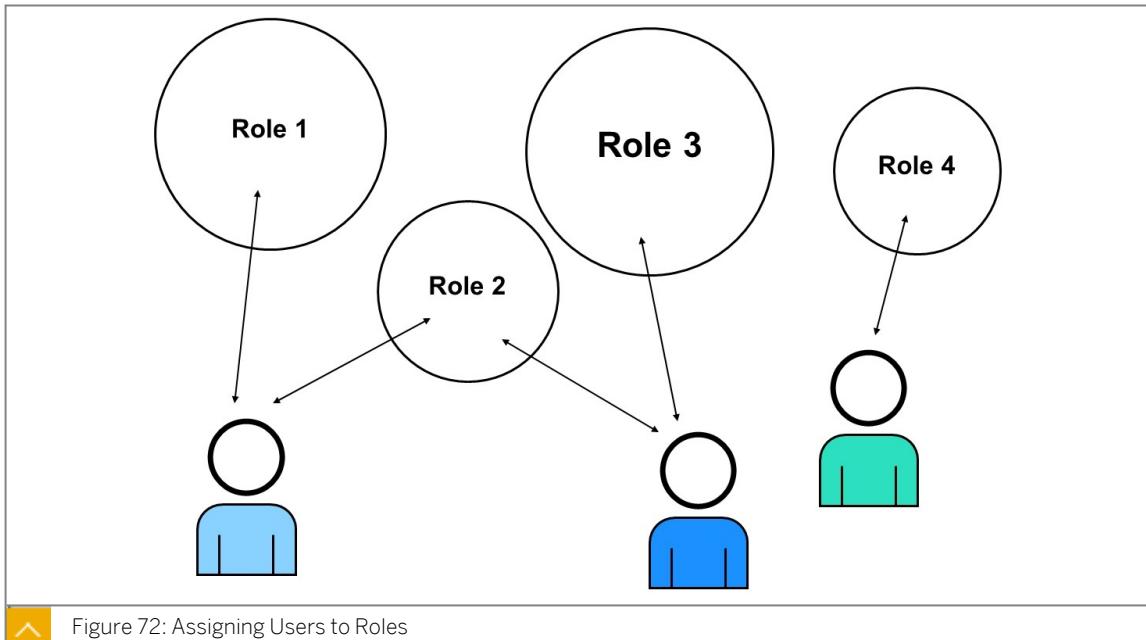
Having maintained the authorizations in accordance with the policies of your company, you can generate the authorization profile. It is only then that the authorizations contained take effect.

During the generation, Role Maintenance collects all entered values and assigns them to a profile. However, one profile can only contain a certain number of authorizations. It is therefore possible that one role has several profiles. You can recognize these profiles from the fact that they have identical names for the first **10 characters**, and an appended number starting with 1-99 (SAP Note 16466). These are known as sequential profiles.

This division is performed automatically and is decided by Role Maintenance. It depends on the fields used and on the number of entries.

Assign Users and Compare User Master Record





Assigning users:

You must assign roles to users so that users are provided with the menu tree for their role when they log on to the system.

You assign roles to users by adding the corresponding names to the list on the *User* tab page of Role Maintenance. Users can be assigned to more than one role. It makes sense to define roles for specific cross-role activities. An example is the activity "Print". Regardless of their function, all users (who are authorized to print) can be assigned to a role with the activity "Print". This eliminates the need to add the "Print" transaction to a large number of roles, which is a cumbersome task.

It is also possible to assign roles to users for a limited period of time. This makes sense, for example, for year-end closing: Physical inventory activities should only be allowed for a limited time. So that a time-dependent assignment of an activity profile to a user master record becomes effective, you must perform a comparison (see the figure *Compare User Master Record*).

There are two ways to do this:

1. As a background job: Report `pfcg_time_dependency` is run before the start of the business day, but after midnight, meaning that the authorization profiles in the user master record always have the most up-to-date status in the morning.
2. Alternatively, using transaction `PFDU`, (User Master Data Reconciliation).

As an administrator, you should regularly execute this transaction as a check. In this way, you can manually process errors that may have occurred and been reported during the background job. Choose the *Complete Reconciliation* radio button to compare all roles.

The last step to be performed is the user master comparison from transaction `PFCG`.

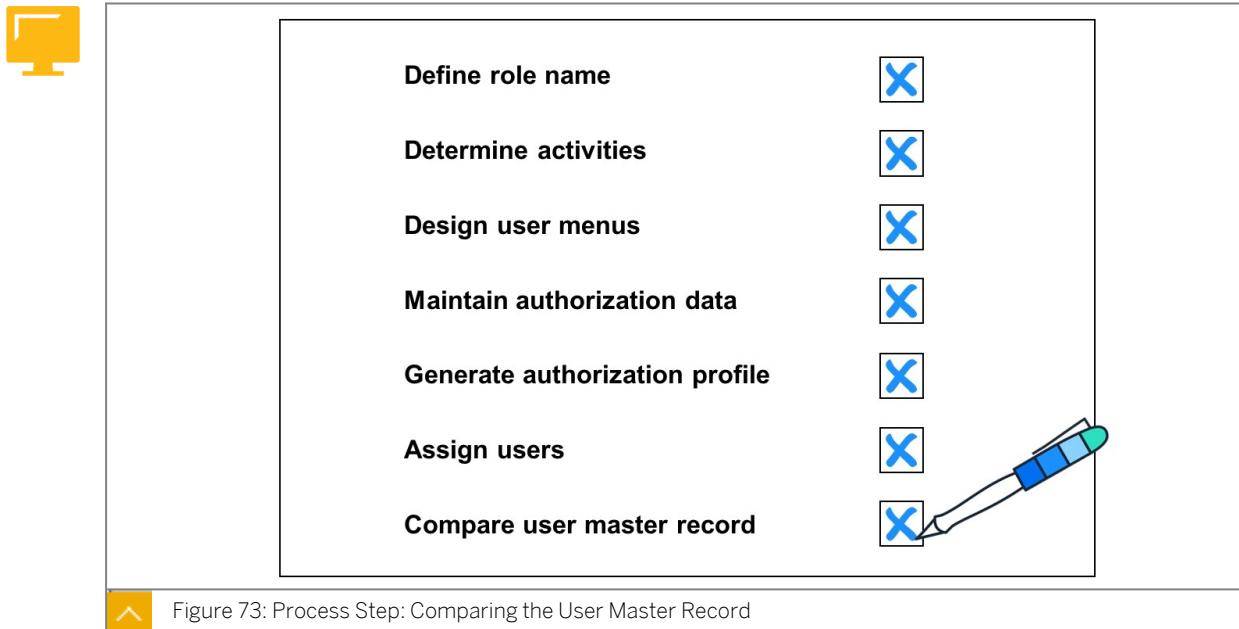


Figure 73: Process Step: Comparing the User Master Record

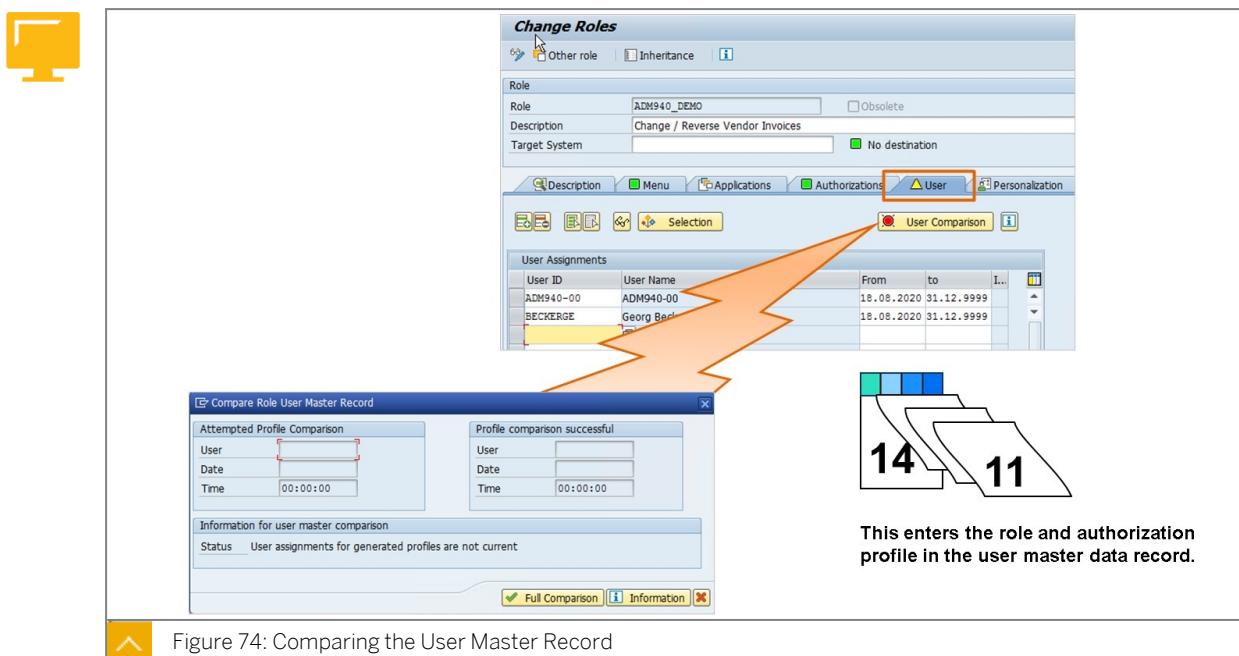


Figure 74: Comparing the User Master Record

Comparing the user master:

So that users are allowed to execute the transactions contained in the menu tree of their roles, their user master record must contain the profile for the corresponding roles.

You can start the user compare process from within Role Maintenance ("User" tab page and "User Comparison" button). As a result of the comparison, the profile generated by Role Maintenance is entered into the user master record.



Hint:

The condition for this however, is that the validity period of the role includes the current date. If this is not the case, the role is assigned and entered into the master record, but the profile is not.

If you assign roles to users for a limited period of time only, you must perform a comparison at the beginning and at the end of the validity period. We recommend that you schedule the background job *pfcg_time_dependency* in such cases.



Caution:

Never enter generated profiles directly into the user master record ("SU01").

During a user comparison, for example automatically with report

pfcg_time_dependency, **generated** profiles are removed from the user masters if they are not among the roles that are assigned to the user.

Unit 4

Exercise 5

Practice System Exercise: Maintain Standard Roles

Business Example

This role maintenance exercise deals with “basic maintenance” using Role Maintenance (*Goto / Settings* in the menu). The following tasks should familiarize you with the basic role maintenance functions and the automatic generation of SAP Easy Access user menus for various work centers and the associated authorizations, profiles, and user assignments. If you are attending SAP course ADM940, the next two lessons deal with special role types and the subtleties of authorization maintenance.

Prerequisites



Note:

In the prerequisites of this exercise, you familiarize yourself with the authorization concept that you implement in this and the following exercises. You do **not** create all the roles at once. This is done in the course for the individual subtasks.

When you see “Use the transactions in accordance with the example authorization concept”, you need to refer to the following tables: distribution of **roles for transaction codes** and distribution of **job roles for roles**.

Name of the Role	Transactions for this Role
GR##_MM_MAT_ANZ	MM03, MM04, MM19
GR##_FI_ACCREC_MAINT	FD01, FD02, FD03
GR##_SD_CUST_MAINT	VD01, VD02, VD03
GR##_SD_SALES	VA21, VA22, VA23, VA25, VA01, VA02, VA03, V.01
GR##_MM_IM_POST	MB1C, MB90, VL21
GR##_FI_IP_POST	F-18, F-26, F-28

Role/Transaction Distribution (Table 1: Example Authorization Concept)

Business area	FI	SD	SD	MM
Work Place Description	AccRec	SDClerk	SDMan	Whouse
SAP R/3 Links: T Code	Scope	Scope	Scope	Scope
MM01				

Business area	FI	SD	SD	MM
Work Place Description	AccRec	SDClerk	SDMan	Whouse
SAP R/3 Links: T Code	Scope	Scope	Scope	Scope
MM02				
MM03	X	X	X	X
MM19	X	X	X	X
MM04	X	X	X	X
FD01	X		X	
FD02	X		X	
FD03	X		X	
VD01		X	X	
VD02		X	X	
VD03		X	X	
VA21		X	X	
VA22		X	X	
VA23		X	X	
VA25		X	X	
VA01		X	X	
VA02		X	X	
VA03		X	X	
V.01		X	X	
MB1C				X
MB90				X
VL21				X
F-18	X			
F-26	X			
F-28	X			

Job Role/Roles (Table 2: Example Authorization Concept)

Task 1: Create a Role to Display a Material Master

Create a role GR##_MM_MAT_ANZ to display a material master.

1. Start the Role Maintenance transaction and create the predefined role. Enter a short description, and save.
2. Add the corresponding transactions in accordance with the sample authorization concept (**Roles for Transaction Codes** table from the prerequisites of this exercise).

A brief extract from the table in the prerequisites is provided here to make the task more comprehensible.

Name of the Role	Transactions for this Role
GR##_MM_MAT_ANZ	MM03, MM04, MM19

3. Create a folder with the name **WWW Links** and add a Web address with the name SAP and the URL <http://www.sap.com> to this folder.
4. Maintain Authorizations - Maintain authorization values for the organizational levels.
5. Maintain Authorizations - Check the traffic light symbol status.
For which authorization object class are all authorization field contents maintained?
Authorization object class:

For which authorization objects of the object class MM_G do you have to supply authorization values?

Authorization Objects:

6. Maintain Authorizations - Set the authorization for the maintenance status in the authorization object M_MATE_STA to full authorization.
What is the status of the authorization after your change?

7. Maintain Authorizations - Set all open authorization values to full authorization.
Set all open authorization values to full authorization (top set of traffic lights).
What happens to the traffic light symbol for object class MM_G after you have assigned values to all open fields?

8. Maintain Authorizations - Generate the authorization profile for your role.
9. Check the status of your authorization profile in the information section of the *Authorizations* tab and complete the maintenance of this role and return to the initial screen of transaction PFCG.
What is the status of your authorization profile?

Task 2: Create a Role with Authorizations for a Warehouse Supervisor

Create a role GR##_MM_IM_POST with authorizations for a warehouse supervisor.

1. Start the role maintenance transaction and create the predefined role. Enter a short description, and save.
2. Add the corresponding transactions in accordance with the sample authorization concept (**Roles for Transaction Codes** table from the prerequisites of this exercise).
3. Maintain Authorizations - Maintain authorization values for the organizational levels.
4. Maintain Authorizations - Add the authorization values 561 and 562 to the authorization values for the *Movement Type* field of the authorization object M_MSEG_BWA.
5. Maintain Authorizations - Set all open authorization values to full authorization.
6. Maintain Authorizations - Generate the authorization profile for your role.
7. Complete the maintenance of this role and return to the initial screen of transaction PFCG.

Task 3: Copy a Role

The following exercise is optional.

Use the role GR##_MM_IM_POST as a template to create the role GR##_MM_IM_POST1020. To do this, choose the **Copy Role** icon and copy all settings from the template.

1. Create the role GR##_MM_IM_POST1020 as a copy of the role GR##_MM_IM_POST.
2. Maintain Authorizations - Check the status of the authorization profile.
Check the status of the authorization profile in the information section of the tab page.
What is the status of the authorization profile?

3. Maintain Authorizations - Check the authorization values of the authorization profile.
Did the system copy the authorizations of the copy template?

4. Maintain Authorizations - Assign **only** the value 1200 to the organizational level *Plant*.
5. Maintain Authorizations - Generate the authorization profile for your role and check the status of the authorization profile.
What is the status of the authorization profile?

6. Complete the maintenance of this role and return to the initial screen of transaction PFCG.

Task 4: Create a Role and Assign it to All Users

Create a role GR##_BC_PORTALS. The content of the role should be copied by choosing **From Other Role** on the "Menu" tab page. This role should then be assigned to all "GR##*" users and contain functions of general interest.

1. Start the role maintenance transaction and create the predefined role. Enter a short description, and save.
2. Go to the Menu tab page and copy the menu from the predefined role SAP_BC_SRV_USER by selecting all transactions.
3. Maintain Authorizations - Set all open authorization values to full authorization.
4. Maintain Authorizations - Generate the authorization profile for your role.

5. Assign the role to all users.

What is the status of the *User* tab page?

Assign your role to all users that you have created with the user name "GR##*", with your group ID (the users GR##-FI1, GR##-FI2, GR##-SD1, GR##-SD2, GR##-MM1, GR##-MM2 should exist with the user group ZGR##, from another lesson of the SAP course ADM940).

Check the settings for the user comparison (menu: *Utilities* → *User Settings*). Ensure that a user master adjustment (record comparison) is automatically performed when you save.

6. Save your role and perform a user comparison

What happens to the status of the "User" tab after you have saved.

7. Assign the role *ADM940_PLUS* to all of your users ("GR##-*").

Save your user assignments, and perform a master record comparison.



Hint:

With this exercise, it is possible that participants lock each other when saving the settings. If this happens, wait a moment and try again. After the comparison, exit the transaction PFCG.

Unit 4 Solution 5

Practice System Exercise: Maintain Standard Roles

Business Example

This role maintenance exercise deals with “basic maintenance” using Role Maintenance (Goto / Settings in the menu). The following tasks should familiarize you with the basic role maintenance functions and the automatic generation of SAP Easy Access user menus for various work centers and the associated authorizations, profiles, and user assignments. If you are attending SAP course ADM940, the next two lessons deal with special role types and the subtleties of authorization maintenance.

Prerequisites



Note:

In the prerequisites of this exercise, you familiarize yourself with the authorization concept that you implement in this and the following exercises. You do **not** create all the roles at once. This is done in the course for the individual subtasks.

When you see “Use the transactions in accordance with the example authorization concept”, you need to refer to the following tables: distribution of **roles for transaction codes** and distribution of **job roles for roles**.

Name of the Role	Transactions for this Role
GR##_MM_MAT_ANZ	MM03, MM04, MM19
GR##_FI_ACCREC_MAINT	FD01, FD02, FD03
GR##_SD_CUST_MAINT	VD01, VD02, VD03
GR##_SD_SALES	VA21, VA22, VA23, VA25, VA01, VA02, VA03, V.01
GR##_MM_IM_POST	MB1C, MB90, VL21
GR##_FI_IP_POST	F-18, F-26, F-28

Role/Transaction Distribution (Table 1: Example Authorization Concept)

Business area	FI	SD	SD	MM
Work Place Description	AccRec	SDClerk	SDMan	Whouse
SAP R/3 Links: T Code	Scope	Scope	Scope	Scope
MM01				

Business area	FI	SD	SD	MM
Work Place Description	AccRec	SDClerk	SDMan	Whouse
SAP R/3 Links: T Code	Scope	Scope	Scope	Scope
MM02				
MM03	X	X	X	X
MM19	X	X	X	X
MM04	X	X	X	X
FD01	X		X	
FD02	X		X	
FD03	X		X	
VD01		X	X	
VD02		X	X	
VD03		X	X	
VA21		X	X	
VA22		X	X	
VA23		X	X	
VA25		X	X	
VA01		X	X	
VA02		X	X	
VA03		X	X	
V.01		X	X	
MB1C				X
MB90				X
VL21				X
F-18	X			
F-26	X			
F-28	X			

Job Role/Roles (Table 2: Example Authorization Concept)

Task 1: Create a Role to Display a Material Master

Create a role GR##_MM_MAT_ANZ to display a material master.

1. Start the Role Maintenance transaction and create the predefined role. Enter a short description, and save.
 - a) SAP Menu:
Tools → Administration → User Maintenance → Role Administration → Roles, (transaction code PFCG).
 - b) Enter the name for the role **GR##_MM_MAT_ANZ** in the *Role* field.
 - c) Choose *Create Single Role*.
 - d) Under the Role Name, in the field *Description* enter: **Display a material master**.
 - e) Then choose *Save (CTRL+S)* to save your role.
2. Add the corresponding transactions in accordance with the sample authorization concept (**Roles for Transaction Codes** table from the prerequisites of this exercise).
A brief extract from the table in the prerequisites is provided here to make the task more comprehensible.

Name of the Role	Transactions for this Role
GR##_MM_MAT_ANZ	MM03, MM04, MM19

 - a) Go to the *Menu* tab page.
 - b) Choose the *Transaction* button and enter the following transaction codes in the *Transaction code* field:
MM03
MM04
MM19
 - c) Choose *Assign Transactions*.
 - d) Then choose *Save (CTRL+S)* to save your role.
3. Create a folder with the name **WWW Links** and add a Web address with the name SAP and the URL <http://www.sap.com> to this folder.
 - a) Choose the *Create Folder* button.
 - b) Enter **WWW Links** in the *Folder Name* field.
 - c) Choose *Continue (Enter)*.
 - d) Next to the button *Transaction*, use the black triangle to choose *Other → Web address or file* in the context menu of the *Transaction* button.
 - e) Enter the description **SAP . com** in the *Text* field.
 - f) Enter the URL **https://www.sap.com** in the *Web address or file* field.
 - g) Choose *Copy (Enter)*.
 - h) Then choose *Save (CTRL+S)* to save your role.
4. Maintain Authorizations - Maintain authorization values for the organizational levels.
 - a) Go to the *Authorizations* tab page.

b) Choose *Change Authorization Data*.

c) Enter the following values in the *Define Organizational Levels* window:

When you maintain organizational levels, you usually only see those lines where values have been assigned. If an organizational level field has not yet been maintained, only one line is displayed. You can display multiple lines by choosing the *More Values* button.

- Company code: **1010**,
- Warehouse number/complex: *****,
- Sales organization: **1010**,
- Distribution Channel: *****,
- Plant: **1000, 1010, 1020**.

d) Choose *Save (CTRL+S)* to save the authorization values for the organizational levels.

5. Maintain Authorizations - Check the traffic light symbol status.

For which authorization object class are all authorization field contents maintained?

Authorization object class:

For which authorization objects of the object class MM_G do you have to supply authorization values?

Authorization Objects:

a) Check the *Group/object/Authorization Field* column for authorization object class where all authorization field contents are maintained.

Object class: AAAB, Cross-application Authorization Objects

b) Check the *Group/object/Authorization Field* column for authorization objects of the object class MM_G with a yellow traffic light.

Authorization objects whose authorization field values are not completely maintained are flagged with a yellow traffic light.

The following authorization objects are not completely maintained:

- M_MATE_MAR
- M_MATE_MAT
- M_MATE_STA
- M_MATE_WGR

6. Maintain Authorizations - Set the authorization for the maintenance status in the authorization object M_MATE_STA to full authorization.

What is the status of the authorization after your change?

-
- a) Expand Authorization Object *M_MATE_STA*.
 - b) In the context menu (click the right-mouse button) of the *STATM* field and choose *Set field Values to '*'*.
Status: *Maintained*, traffic light: *Green*.

7. Maintain Authorizations - Set all open authorization values to full authorization.

Set all open authorization values to full authorization (top set of traffic lights).

What happens to the traffic light symbol for object class *MM_G* after you have assigned values to all open fields?

- a) Choose the *Status* button.
- b) Choose *Execute (Enter)* in the *Assign Full Authorization of Subtree* window.
The traffic light symbol for object class *MM_G* then switches the structure to *Green*.

8. Maintain Authorizations - Generate the authorization profile for your role.

- a) Choose the *Generate* icon.
- b) In the *Assign Profile Name for Generated Authorization Profile* window, accept the proposed profile name and choose *Execute (Enter)*.
- c) Choose *Back (F3)* to return to the *Change Roles* screen.

9. Check the status of your authorization profile in the information section of the *Authorizations* tab and complete the maintenance of this role and return to the initial screen of transaction *PFCG*.

What is the status of your authorization profile?

- a) Check the *Status* field on the *Authorizationstab*
Status: *Authorization profile is current*.
- b) Choose *Back (F3)* to return to the initial screen of *Role Maintenance*.

Task 2: Create a Role with Authorizations for a Warehouse Supervisor

Create a role **GR##_MM_IM_POST** with authorizations for a warehouse supervisor.

1. Start the role maintenance transaction and create the predefined role. Enter a short description, and save.

- a) SAP Menu:
Tools → Administration → User Maintenance → Role Administration → Roles, (transaction code *PFCG*).

- b) Enter the name for the role **GR##_MM_IM_POST** in the *Role* field.
- c) Choose *Create Single Role*.
- d) Under the *Role Name*, in the field *Description* enter **Warehouse supervisor**.
- e) Then choose *Save (CTRL+S)* to save your role.

2. Add the corresponding transactions in accordance with the sample authorization concept (**Roles for Transaction Codes** table from the prerequisites of this exercise).

- a) Go to the *Menu* tab page.
 - b) Choose the *Transaction* button and enter the following transaction codes in the *Transaction code* field:
 - MB1C
 - MB90
 - VL21
 - c) Choose *Assign Transactions*.
 - d) Then choose *Save (CTRL+S)* to save your role.
3. Maintain Authorizations - Maintain authorization values for the organizational levels.
- a) Go to the the *Authorizations* tab page.
 - b) Choose *Change Authorization Data*.
 - c) Enter the following values in the *Define Organizational Levels* window:
 When you maintain organizational levels, you usually only see those lines where values have been assigned. If an organizational level field has not yet been maintained, only one line is displayed. You can display multiple lines by choosing the *More Values* button.
 - *Shipping Point*: *,
 - *Plant*: **1000, 1010, 1020**.
 - d) Choose *Save (CTRL+S)* to save the authorization values for the organizational levels.
4. Maintain Authorizations - Add the authorization values 561 and 562 to the authorization values for the *Movement Type* field of the authorization object M_MSEG_BWA.
- a) Expand *Object Class MM_B*.
 - b) Expand *Authorization Object M_MSEG_BWA*.
 - c) Expand *Authorization Authorizat. 00*.
 - d) Choose the *Pencil* button on the right side of the *BWART* field.
 - e) Enter **561** and **562** in the *Field values* window.
 - f) Choose *Transfer (Enter)*.
5. Maintain Authorizations - Set all open authorization values to full authorization.
- a) Choose the *Status* button.
 - b) Choose *Execute (Enter)* in the *Assign Full Authorization of Subtree* window.
6. Maintain Authorizations - Generate the authorization profile for your role.
- a) Choose the *Generate* icon.
 - b) In the *Assign Profile Name for Generated Authorization Profile* window, accept the proposed profile name and choose *Execute (Enter)*.
 - c) Choose *Back (F3)* to return to the *Change Roles* screen.
7. Complete the maintenance of this role and return to the initial screen of transaction PFCG.
- a) Choose *Back (F3)* to return to the initial screen of the *Role Maintenance*.

Task 3: Copy a Role

The following exercise is optional.

Use the role GR##_MM_IM_POST as a template to create the role GR##_MM_IM_POST1020. To do this, choose the **Copy Role** icon and copy all settings from the template.

1. Create the role GR##_MM_IM_POST1020 as a copy of the role GR##_MM_IM_POST.

a) While still in the Role Maintenance transaction, enter the name for the role

GR##_MM_IM_POST in the *Role* field.

b) Choose **Copy Role** (*Shift + F11*).

c) Enter **GR##_MM_IM_POST1020** in the *to role* field.

d) Choose **Copy All** (*Enter*).

e) Choose **Change** on the *Role Maintenance* screen.

2. Maintain Authorizations - Check the status of the authorization profile.

Check the status of the authorization profile in the information section of the tab page.

What is the status of the authorization profile?

a) Go to the *Authorizations* tab page.

b) Check the *Status* field on the *Authorizations* tab.

Status: *Current version not generated*.

3. Maintain Authorizations - Check the authorization values of the authorization profile.

Did the system copy the authorizations of the copy template?

a) Choose **Change Authorization Data** on the *Authorizations* tab.

Did the system copy the authorizations of the copy template?

Yes, they were copied too.

4. Maintain Authorizations - Assign **only** the value *1200* to the organizational level *Plant*.

a) Choose **Organizational levels** (*Ctrl+F8*).

Plants 1000, 1010, and 1020 have been copied

b) Delete the entries for plants 1000 and 1010.

c) Choose **Save** (*Ctrl+S*).

5. Maintain Authorizations - Generate the authorization profile for your role and check the status of the authorization profile.

What is the status of the authorization profile?

a) Choose the **Generate** icon.

b) In the *Assign Profile Name for Generated Authorization Profile* window, accept the proposed profile name and choose **Execute** (*Enter*).

- c) Choose Back (F3) to return to the *Change Roles* screen.
 - d) Check the *Status* field on the *Authorizations* tab.
Status: Authorization profile is current.
6. Complete the maintenance of this role and return to the initial screen of transaction PFCG.
- a) Choose Back (F3) to return to the initial screen of *Role Maintenance*.
- Task 4: Create a Role and Assign it to All Users**
- Create a role GR##_BC_PORTALS. The content of the role should be copied by choosing **From Other Role** on the "Menu" tab page. This role should then be assigned to all "GR##*" users and contain functions of general interest.
1. Start the role maintenance transaction and create the predefined role. Enter a short description, and save.
 - a) While still in the Role Maintenance transaction, enter the name for the role **GR##_BC_PORTALS** in the *Role* field.
 - b) Choose *Create Single Role*.
 - c) Under the *Role Name*, in the field *Description* enter **General role for communication, workflow, and so on.**
 - d) Then choose *Save (Ctrl+S)* to save your role.
 2. Go to the Menu tab page and copy the menu from the predefined role SAP_BC_SRV_USER by selecting all transactions.
 - a) Go to the *Menu* tab page.
 - b) Choose *From Menus → From Another Role → Local*.
 - c) Enter **SAP_BC_SRV_USER** in the *Single Role* field.
 - d) Choose *Start Search*.
 - e) Choose *Copy*.
 - f) Select all items and choose *Add*.
 - g) Then choose *Save (Ctrl+S)* to save your role.
 3. Maintain Authorizations - Set all open authorization values to full authorization.
 - a) Go to the *Authorizations* tab page.
 - b) Choose *Change Authorization Data*.
 - c) Choose the *Status* button.
 - d) Choose *Execute (Enter)* in the *Assign Full Authorization of Subtree* window.
 4. Maintain Authorizations - Generate the authorization profile for your role.
 - a) Choose the *Generate* icon.
 - b) In the *Assign Profile Name for Generated Authorization Profile* window, accept the proposed profile name and choose *Execute (Enter)*.
 - c) Choose Back (F3) to return to the *Change Roles* screen.
 5. Assign the role to all users.

What is the status of the *User* tab page?

Assign your role to all users that you have created with the user name "GR##-*", with your group ID (the users GR##-FI1, GR##-FI2, GR##-SD1, GR##-SD2, GR##-MM1, GR##-MM2 should exist with the user group ZGR##, from another lesson of the SAP course ADM940).

Check the settings for the user comparison (menu: *Utilities* → *User Settings*). Ensure that a user master adjustment (record comparison) is automatically performed when you save.

- a) Check the status of the *User* tab page.

The *User* tab page is "red", which means that no users have yet been assigned to this role.

- b) Go to the *User* tab page.

- c) Assign the following users by entering the names into the *User ID* column.

User name
GR##-FI1
GR##-FI2
GR##-SD1
GR##-SD2
GR##-MM1
GR##-MM2

6. Save your role and perform a user comparison

What happens to the status of the "User" tab after you have saved.

-
- a) Choose *Save* (*Ctrl+S*)

The status display of the tab page is yellow.

- b) Choose *User Comparison*.

The user comparison enters the generated profiles for a role (if the validity period includes today's date), and the role itself, in the user master record.

- c) Choose *Full Comparison* on the *Compare Role User Master Record* window.

The *Status* field indicates: *Comparison of user master record completed*.

- d) Choose *Cancel* (*F12*) on the *Compare Role User Master Record* window.

You can activate automatic user adjustment when saving a role by choosing *Utilities* → *User Settings* and selecting the appropriate checkbox (*Automatic User Adjustment when Saving Role*).

The status display of the tab page is green.

- e) Choose *Back* (*F3*) to return to the *Role Maintenance* screen.

7. Assign the role *ADM940_PLUS* to all of your users ("GR##-*").

Save your user assignments, and perform a master record comparison.



Hint:

With this exercise, it is possible that participants lock each other when saving the settings. If this happens, wait a moment and try again. After the comparison, exit the transaction PFCG.

- a) While still in the Role Maintenance transaction, enter the name for the role: **ADM940_PLUS** in the *Role* field.
- b) Choose the *Change* icon.
- c) Go to the *User* tab page.
- d) Assign the following users by entering the names into the *User ID* column.

User name
GR##-FI1
GR##-FI2
GR##-SD1
GR##-SD2
GR##-MM1
GR##-MM2

- e) Choose *User Comparison*.
- f) Choose Yes on the *Save the role* window.
- g) Choose *Full Comparison* on the *Compare Role User Master Record* window.
- h) Choose *Cancel (F12)* on the *Compare Role User Master Record* window.
- i) Choose *Back (F3)* to return to the *Role Maintenance* screen.



LESSON SUMMARY

You should now be able to:

- Manage business roles, profiles and authorization data.

Creating Customizing Roles

LESSON OVERVIEW

This is the second lesson on the topic of *Role Maintenance*, and describes advanced maintenance of role types, which extend standard roles in a useful way with special properties. A typical requirement in a company is, for example, to create a role that has as clear a menu as possible, but which also describes a complete work center or position. These attributes are realized in the composite role.

Reference, derived, and Customizing roles round off the requirements. You can create these advanced types of role with the Role Maintenance.

Business Example

The different requirements in companies often require nesting of roles and the possibility to set up dependencies. Composite, reference, and derived roles exist for this purpose. However, before the end user roles are created, the system is Customized for customer requirements. Customizing roles are used for this purpose.



LESSON OBJECTIVES

After completing this lesson, you will be able to:

- Create the project team customizing roles.

Customizing Role

You can assign projects or project views of the Implementation Guide (IMG) to a *Customizing role*. The purpose of such an assignment is to specifically generate the authorization for certain IMG activities and assign it to users.

If you are on the *Menu* tab page in the Role Maintenance transaction, you can assign projects or view from the Implementation Guide (IMG) by choosing *Utilities* → *Customizing Auth*. When the profile is generated, the system creates the authorization, which is necessary to perform all activities of the IMG projects/project views assigned.

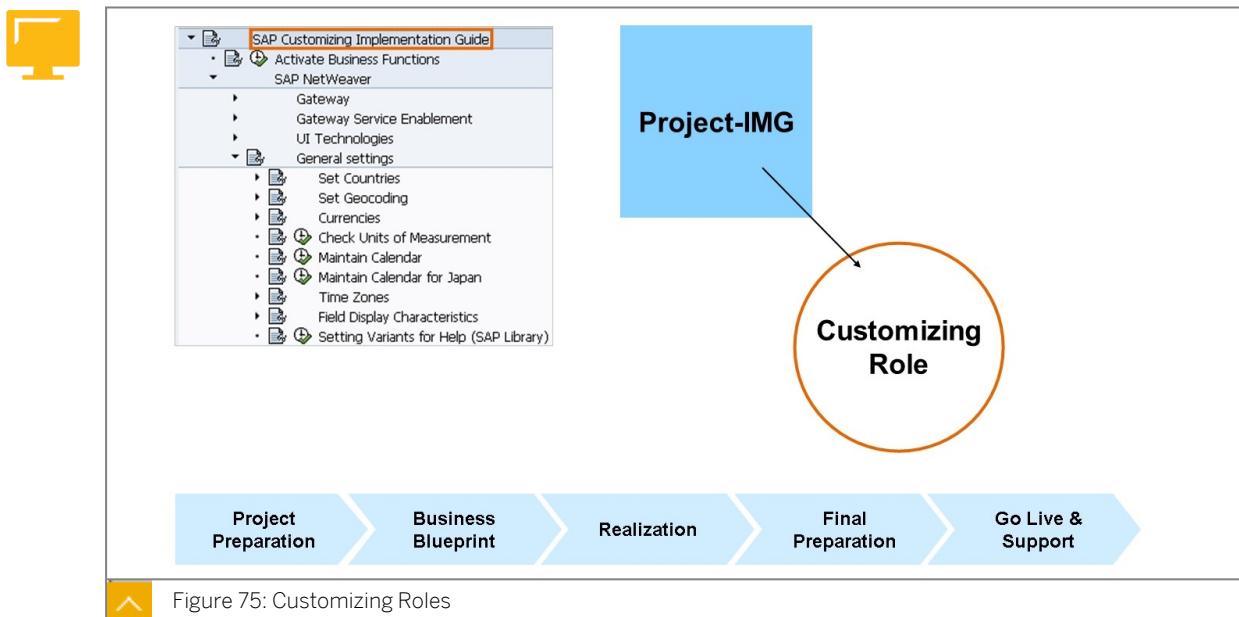


Figure 75: Customizing Roles

**Caution:**

If a project or project view has been assigned to a role, it is no longer possible to manually assign transactions to this role. This means that the role can only be used for generating and assigning Customizing authorizations. In the same way, a role to which transactions have been manually assigned cannot be used for Customizing authorizations.

The transactions of the project or project view are not displayed in the Session Manager and the "SAP Easy Access" menu. If the Enterprise IMG or Project IMG is changed, the authorization data of this role must be regenerated.

**Hint:**

Since Customizing activities are performed on a project-related basis and for a limited period, you should maintain the end date for the assigned users. This ensures that the users assigned to the role lose the authorization for the projects/project views assigned upon completion of the project. This only applies, of course, if the user comparison is regularly performed.

**LESSON SUMMARY**

You should now be able to:

- Create the project team customizing roles.

Implementing a Composite Role Strategy



LESSON OBJECTIVES

After completing this lesson, you will be able to:

- Implement a composite role strategy.

Composite Roles

It is often necessary to describe a work center using more than one single role and the information stored within it about menu structure, authorization data, and user assignments. To simplify maintenance and improve reusability, it is also possible to modularize a work center using several roles, which are then combined in a composite role. This possibility simplifies user administration and makes it easier for the company's HR team or Support department to assign authorizations.

Advantages of Composite Roles

- One work center
- One composite role
- One assignment
- One central menu

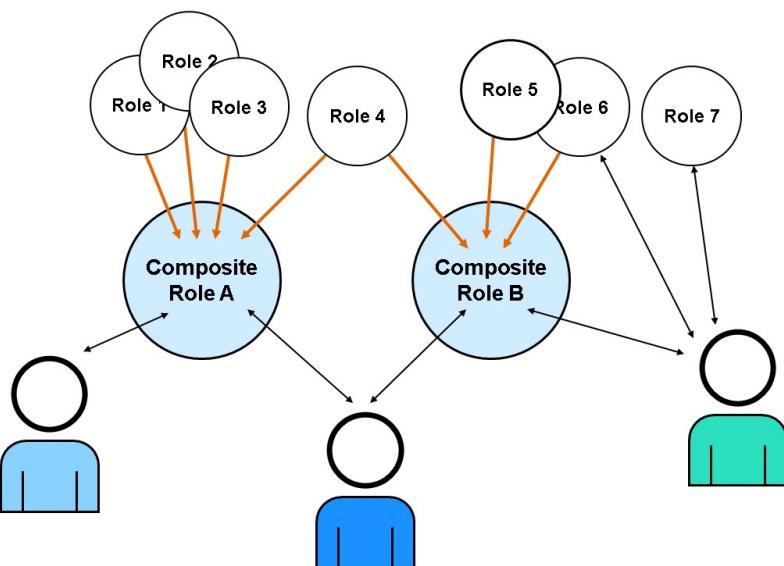


Figure 76: Composite Roles and User Assignment

This container can contain any content. For reasons of clarity, it does not make sense and is therefore not possible to add composite roles to composite roles.

**Hint:**

The SAP system does not use different names for single and composite roles. When creating or naming your roles, you should consider a naming convention that supports the differentiation of single and composite roles.

Disadvantages of Composite Roles

Since composite roles are only a shell for combined roles, they do not have **any authorization data** themselves.

**Hint:**

If you want to change the authorizations (that are represented by a composite role), you must maintain the data for each role of the composite role.

Creating composite roles makes sense if some of your employees need authorizations from several roles. Instead of adding each user separately to each role required, you can set up a composite role and assign it to the users of that group.

The users assigned to a composite role are automatically assigned to the corresponding (elementary) roles during the comparison. The contents of the composite roles are automatically resolved and the single roles contained in them are entered.

In the master record, the assigned composite roles are displayed as usual, but the associated roles are displayed with “*blue text on a gray background*”. These fields cannot be changed. The user assignment can only be changed through the composite role.

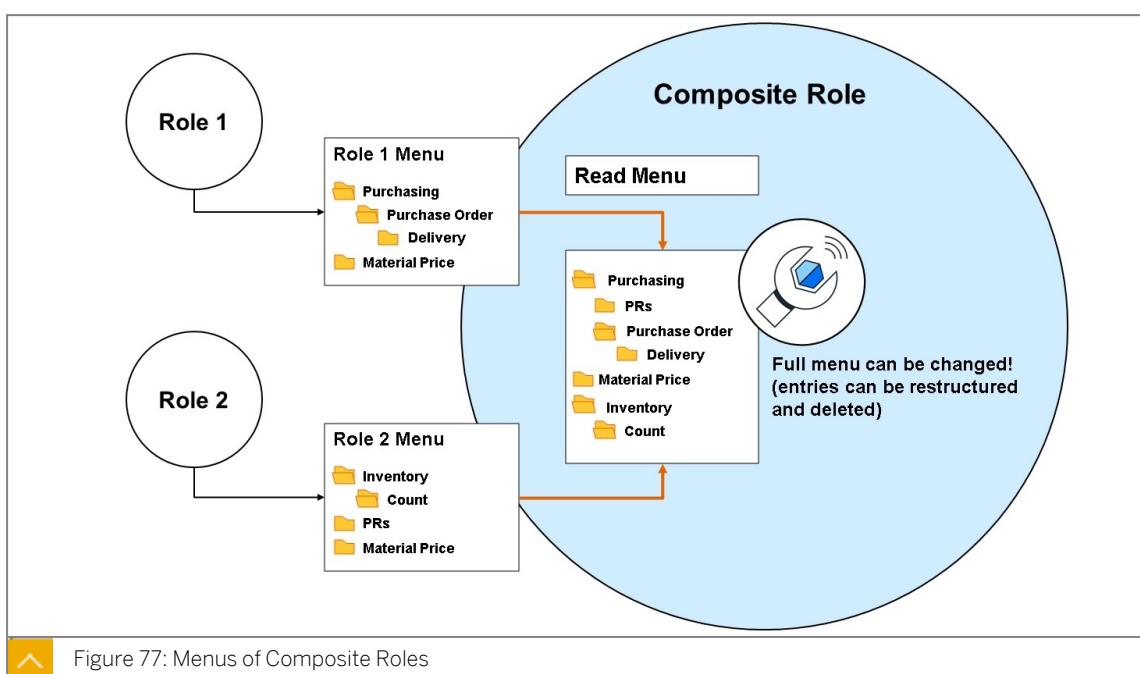
Composite Role Strategy

Figure 77: Menus of Composite Roles

If you assign a number of single roles to a user, multiple listings of individual menu entries can occur. For example, if a transaction or a path that is contained in role 1 **and** in role 2, it appears twice. The user menu then contains more than one entry for menu nodes, and frequently confuses end users.

The menu tree of a composite role is, in the simplest case, a combination of the menus of the roles contained. When you create a new composite role, the initial menu tree is empty at first. You can build the menu tree with the menus of the integrated roles by choosing “Read menu” (*Menu tab page*).



Caution:

Menus for composite roles usually do not reflect the authorizations that the user has through the authorizations of the single roles. There can be two reasons for this:

1. Menu displays more than the composite role authorizes.

If the combination of a role reduces (previously read and used in a composite role), this has, of course, consequences for the existing menu tree. In such a case, Role Maintenance allows you to completely rebuild the menu tree or process only the changes. If you choose the latter option, Role Maintenance removes all items from the entire menu, which are no longer contained in any of the roles referenced.

2. Menu displays less than the composite role authorizes.

If the contents of the assigned roles are extended (menu or authorizations change), these are not automatically visible in the composite role menu.

If you want to change the authorizations (that are represented by a composite role), you must maintain the data for each role of the composite role.

Note: A comparison is required in both cases.

On the *Roles tab page*, enter the roles for which the composite role should consist (use the possible entries help by choosing *F4*).

On the *Menu tab page*, you can then create the menus of the roles contained in the composite role by choosing *Read menu*, and restructure it as you wish.



Hint:

You can remove transactions in the composite role menu. You can only add entries using the assigned single roles.

There are two possibilities in role maintenance for the structure of the menu:

1. If the composite role menu has never yet been built, when you choose *Read menu*, every menu of the single roles that have been assigned is immediately imported.
2. However, if it is a *Refresh*, an additional query appears (see the next presentation slide).

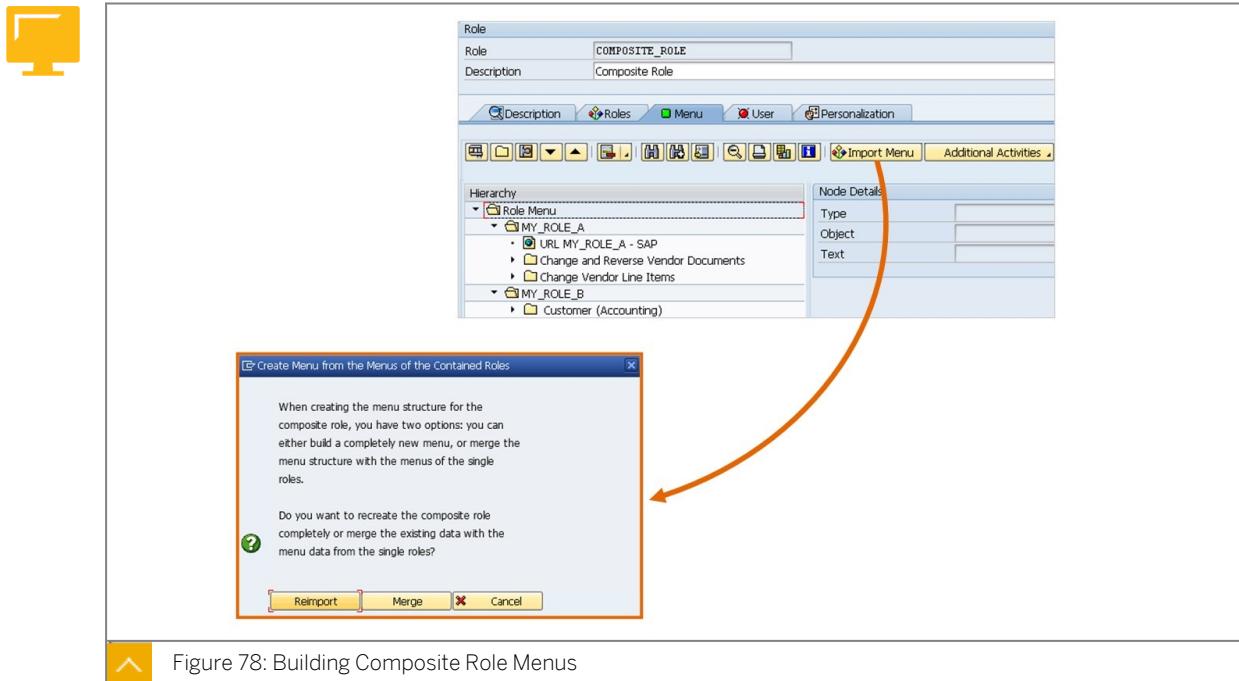


Figure 78: Building Composite Role Menus

You can now choose between *Merge* and *Reimport*. If you want to discard your settings and restructure the menu, choose *Reimport*. *Merge*, on the other hand, creates a delta between the “actual” situation and the situation as it “ought” to be. This delta describes the change set.

- **Reduction:** In this case, the transactions that no longer appear in the roles are removed from the menu of the composite role. Empty folders may be created. These are displayed in red, and you can delete them manually or by choosing *Delete Empty Folders*.
- **Extension:** Those transactions which now additionally appear in the roles are added. You can find these transactions in a separate folder with the description *New menu options*. You can then distribute these to the menu manually. Single roles that have been newly added to the composite role are added with their hierarchy, while transactions from single roles already contained in the composite role are included with no hierarchy.

**Hint:**

When a composite role menu is restructured, the system creates a new folder for each single role contained in the composite role at the top hierarchy level. This folder initially contains the corresponding menu. You can decide whether the text for each folder consists of the technical name or the short text of the role. You can deactivate this function by setting the Customizing switch *COLL_READ_LEVEL_1* to *OFF* in the Customizing table *SSM_CUST*.

**LESSON SUMMARY**

You should now be able to:

- Implement a composite role strategy.

Implementing a Derived Role Strategy



LESSON OBJECTIVES

After completing this lesson, you will be able to:

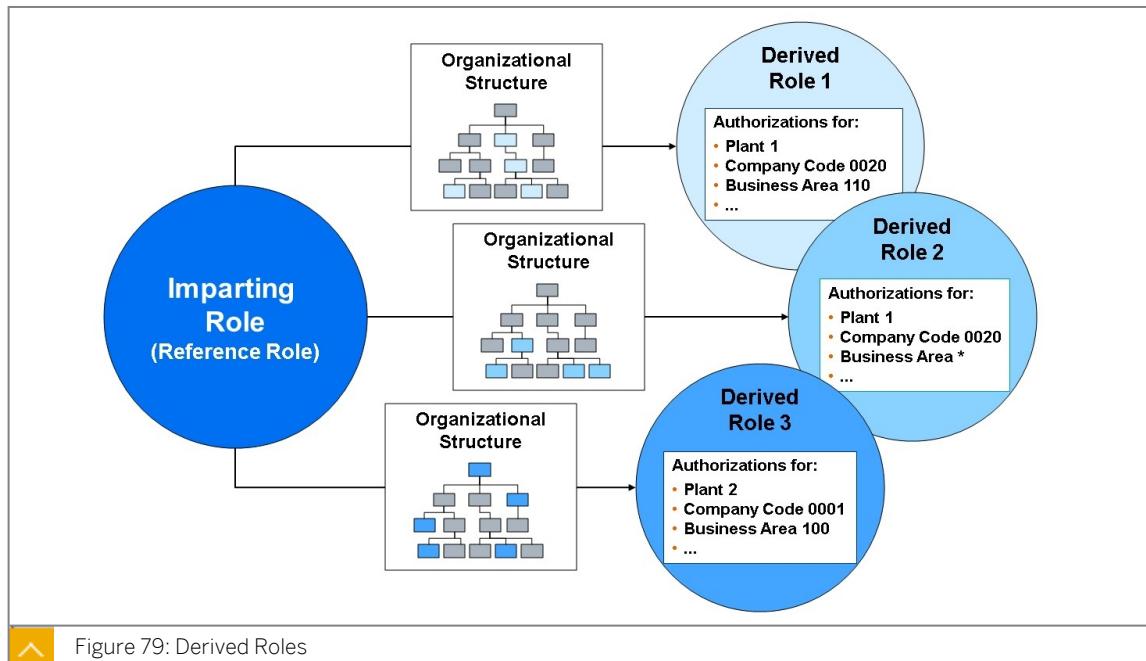
- Implement a derived role strategy.

Derived Role Strategy

In practice, there are a number of requirements to create roles whose content differs only in the authorizations and not in the transactions. For example: two sales and distribution employees with the same work center description, but different plants (1000 and 2000). Here are two useful examples for the use of *derived roles*.

1. The menu of the roles is to be identical, but the authorizations for the actions contained in the menu are reassigned in the derived role.
2. The menu and the authorizations of the derived role are to be identical, but the organizational units are reassigned in the derived role.

The relationships are described in detail on the following pages, and you can see that these roles can be created and maintained very elegantly.



Derived roles refer to roles that already exist. The derived roles inherit the menu structure and the functions included (transactions, reports, Web links, and so on) from the referenced role.

However, the user assignments are **not** inherited.



Hint:
Enter the name of the role from which all transactions including the menu structure are to be copied in the *Derive from Role* field on the *Description* tab page. In this way, each role can become a *referencing role*.

There are two ways to perform the comparison between the roles:

Comparison from the Imparting Role

“Generate Derived Roles” button

This action usually copies the **normal fields** (not the organizational levels) to all derived roles and generates the profiles.



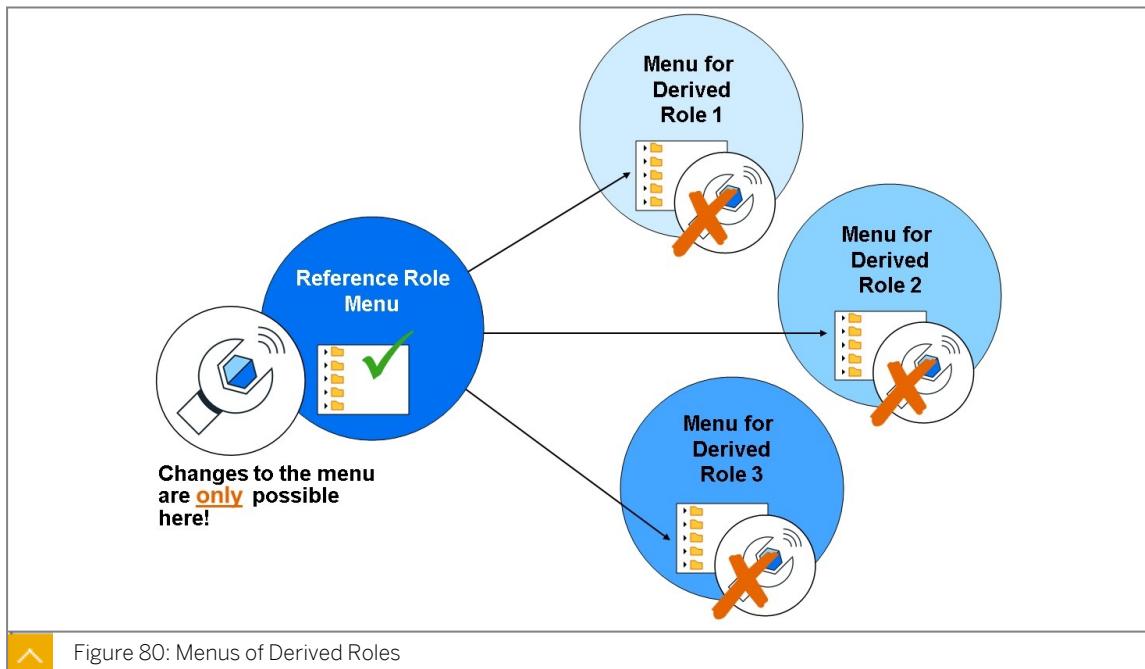
Hint:
The data for the **organizational levels** is only transferred when the authorization data for the derived roles is first modified. If organizational levels have already been maintained in the derived role(s), this is **not overwritten** (see SAP Note 314513).



Comparison from the Derived Role

“Transfer Data” button

This button is usually used for the “*initial fill*” of the authorizations. This call always copies all general authorization values from the template. If an organizational level in the derived role is not filled, it is also set to the value from the reference role.



Unlike composite roles, the derived role has the complete filled menu of the template immediately after the referencing role is entered and the role is saved. The inherited menus **cannot be changed** in the derived roles.



Hint:

The menu is maintained in the **imparting** role only. Changes have an immediate effect on all inheriting roles.

The inheritance relationship can be canceled, but the previously inheriting role is then handled similarly to a normal role. The cancellation of the relationship cannot be undone.

Unit 4

Exercise 6

Practice System Exercise: Maintain Special ABAP Roles

Business Example

This exercise is concerned with advanced role maintenance. The exercises should provide ideas about how composite, reference, and derived roles can simplify your administration work.

Task 1: Create a Composite Role

Create the composite role GR##_MM_WHOUSE.



Hint:

Ensure that you use the *Create Comp. Role* button on the initial screen of Role Maintenance.

1. Start the Role Maintenance transaction and create the predefined role. Enter a short description, and save.
If you look at the tab pages, what do you notice?

2. Add single roles to your composite role.

Your composite role should consist of the roles of the role definition in the sample authorization concept for the work center *Warehouse*.

In accordance with the sample authorization concept, these are:

- GR##_MM_MAT_ANZ
- GR##_MM_IM_POST

Enter these in the relevant fields.

3. Read the menus of the inserted roles into your composite role.

You can choose to make further modifications to the menu of the composite role. (Do not delete any entries. However, you can move or rename them).

4. Assign user GR##-MM1 and save your user assignment.

5. Perform a user master comparison.

6. Complete the maintenance of this role and return to the initial screen of transaction PFCG.

Task 2: Describe the Options for a User Master Comparison

1. Where can you perform a user master comparison? List at least two possibilities.

- _____.
- _____.
2. What does the report *pfcg_time_dependency* do?
- _____
- _____
- _____

Task 3: Display the User Master Record of user GR##-MM1

Display the user master record of user GR##-MM1.

1. Start the User Maintenance transaction and answer the following questions.

If your user GR##-MM1 does not yet have the role ADM940_PLUS, assign the role and perform a user master comparison.

Which roles is the user assigned?

Display the authorization profiles. How many profiles are assigned?

_____ authorization profiles

Why are there fewer profiles than roles?

Task 4: Log on to the System as User GR##-MM1 (Optional)

The following exercise is optional.

Log on to the system as user GR##-MM1. Use the password automatically generated in the exercise for the *user master record* or assign a new initial password in user maintenance.

Change the password when you log on: _____



Hint:

You can show the transaction codes by choosing *Extras → Settings* ("Display technical names").

1. Log on to the system as user GR##-MM1.

2. Set up a user-specific favorites list by defining the transactions MM03 and MB1C as favorites.



Hint:

You can show the transaction codes by choosing *Extras → Settings* ("Display technical names").

3. Start transaction MM03, and display the accounting view of material P605-100 in plant 1010.

Can you also display the accounting view of material P605-100 in plant 1040?

- No, because you **do not** have authorization for plant 1040.

4. Display the failed authorization check.

Why are you not able to display material P605-100 in plant 1040?

5. Log off as GR##-MM1.

Task 5: Create a Derived Role

Create a **derived** role GR##_MM_IM_POST1010 with authorizations for a warehouse supervisor in plant 1010.

1. Create a **derived** role GR##_MM_IM_POST1010 . Assign the imparting role GR##_MM_IM_POST and save your role.
Display the inheritance hierarchy of the roles (choose *Ctrl+Shift+F3* or the *Inheritance Hierarchy* icon).
2. Display the inheritance hierarchy of the roles.
3. Can you add other applications (menu entries, transaction codes, and reports, for example) or delete existing applications?

-
4. Maintain Authorizations - Define the organizational levels.

Plant: 1010

Did the system copy the authorizations of the imparting role?

-
5. Maintain Authorizations - Copy the authorization data from the imparting role.

6. Maintain Authorizations - Generate the authorization profile for your role.

Task 6: Optional: Copy a Role

In this additional exercise, you can create a single role GR##_SD_SALES by copying the predefined work center example ADM940_SD_SALES without user assignment.

1. Start the Role Maintenance transaction and create the role GR##_SD_SALES as a copy of the role ADM940_SD_SALES.
2. Maintain Authorizations - Generate the authorization profile for your role.
3. Complete the maintenance of this role and return to the initial screen of transaction PFCG.

Task 7: Optional: Create the Missing Three Single Roles of the Sample Authorization Concept

In this additional exercise, you can create the missing three single roles of the *sample authorization concept*.

After the creation of roles was carried out in detail in the previous exercises, you should now perform these exercises without a detailed solution.

Create the following roles:

Role	Transactions
GR##_FI_ACCREC_MAINT	FD01, FD02, FD03
GR##_FI_IP_POST	F-18, F-26, F-28
GR##_SD_CUST_MAINT	VD01, VD02, VD03

Restrict the requested organizational levels with the values specified here. The system **never** queries all the organizational levels listed here for a role. Use the following values for the fields used.

Organizational Level	Field Value
Company code	1010
Business area	1000
Account type	D
Controlling area	0001
Division	*
Sales organization	1010
Distribution channel	*

1. Create the role **GR##_FI_ACCREC_MAINT**.
2. Create the role **GR##_FI_IP_POST**.
3. Create the role **Role GR##_SD_CUST_MAINT**.

Task 8: Optional: Create Three Composite Roles that Correspond to the Sample Authorization Concept

In this additional exercise, you can create three composite roles, which correspond to the *sample authorization concept*.

After the creation of roles was carried out in detail in the previous exercises, you should now perform these exercises without a detailed solution

Create the following three composite roles.

Composite role	Corresponds to the work center from the <i>Sample Authorization Concept</i>
GR##_FI_ACCREC	Accounts receivable accountant (AccRec)
GR##_SD_SALCLK	Sales clerk (SClerk)
GR##_SD_SALMGR	Sales and Distribution manager (SDMan)

These composite roles should contain the following single roles:

Composite Role	Contained Roles
GR##_FI_ACCREC	GR##_MM_MAT_ANZ GR##_FI_ACCREC_MAINT GR##_FI_IP_POST
GR##_SD_SALCLK	GR##_MM_MAT_ANZ GR##_SD_CUST_MAINT GR##_SD_SALES
GR##_SD_SALMGR	GR##_MM_MAT_ANZ GR##_FI_ACCREC_MAINT GR##_SD_CUST_MAINT GR##_SD_SALES

1. Create the composite role **GR##_FI_ACCREC**.
2. Create the composite role **GR##_SD_SALCLK**.
3. Create the composite role **GR##_SD_SALMGR**.

Unit 4 Solution 6

Practice System Exercise: Maintain Special ABAP Roles

Business Example

This exercise is concerned with advanced role maintenance. The exercises should provide ideas about how composite, reference, and derived roles can simplify your administration work.

Task 1: Create a Composite Role

Create the composite role GR##_MM_WHOUSE.



Hint:

Ensure that you use the *Create Comp. Role* button on the initial screen of Role Maintenance.

1. Start the Role Maintenance transaction and create the predefined role. Enter a short description, and save.

If you look at the tab pages, what do you notice?

- a) SAP Menu:

Tools → Administration → User Maintenance → Role Administration → Roles
(transaction code PFCG).

- b) Enter the name for the role **GR##_MM_WHOUSE** in the *Role* field.

- c) Choose *Create Comp. Role*.

- d) Enter description **Composite role Warehouse** in the *Description* field.

- e) Then choose *Save (Ctrl+S)* to save your role.

- f) Check the tab pages, what do you notice?

The tab page *Roles* has been added.

The tab page *Authorizations* has been removed.

2. Add single roles to your composite role.

Your composite role should consist of the roles of the role definition in the sample authorization concept for the work center *Warehouse*.

In accordance with the sample authorization concept, these are:

- GR##_MM_MAT_ANZ

- GR##_MM_IM_POST

Enter these in the relevant fields.

- a) Go to the *Roles* tab page.
- b) Enter the following role names in the *Role* column:
 - GR##_MM_MAT_ANZ
 - GR##_MM_IM_POST
- c) Then choose *Save (Ctrl+S)* to save your role.

3. Read the menus of the inserted roles into your composite role.

You can choose to make further modifications to the menu of the composite role. (Do not delete any entries. However, you can move or rename them).

- a) Go to the *Menu* tab page, and choose *Import Menu*.
- b) Then choose *Save (Ctrl+S)* to save your role.

4. Assign user GR##-MM1 and save your user assignment.

- a) Go to the *User* tab page
- b) Enter **GR##-MM1** in the *User ID* field.
- c) Then choose *Save (Ctrl+S)* to save your role.

5. Perform a user master comparison.

- a) Choose the *User comparison* button to enter the roles in the master record of user GR##-MM1.

6. Complete the maintenance of this role and return to the initial screen of transaction PFCG.

- a) Choose *Back (F3)* to return to the initial screen of *Role Maintenance*.

Task 2: Describe the Options for a User Master Comparison

1. Where can you perform a user master comparison? List at least two possibilities.

_____,
_____.

- a) With additional steps in transactions: SU01, PFCG, and PFUD or with the report “*pfcg_time_dependency*”.

2. What does the report *pfcg_time_dependency* do?

- a) You can schedule an automatic user master comparison at regular intervals with this report. This compares all links and relationships between roles, users, and profiles in the master records (in the background).

Task 3: Display the User Master Record of user GR##-MM1

Display the user master record of user GR##-MM1.

1. Start the User Maintenance transaction and answer the following questions.

If your user GR##-MM1 does not yet have the role ADM940_PLUS, assign the role and perform a user master comparison.

Which roles is the user assigned?

Display the authorization profiles. How many profiles are assigned?

_____ authorization profiles

Why are there fewer profiles than roles?

a) SAP Menu:

→ Tools → Administration → User Maintenance → Users, (transaction code SU01).

b) Enter the user name **GR##-MM1** in the User field.

c) Choose the *Display* icon.

d) Go to the *Roles* tab page.

You will find the following roles on the *Roles* tab page.

- ADM940_PLUS
- GR##_BC_PORTALS
- GR##_MM_IM_POST
- GR##_MM_MAT_ANZ
- GR##_MM_WHOUSE

e) Go to the *Profiles* tab page.

Display the authorization profiles. How many profiles are assigned?

- 4 authorization profiles

Why are there fewer profiles than roles?

- Because the composite role does not have its own profile.

f) Choose *Back (F3)* to return to the *User Maintenance: Initial Screen*.

Task 4: Log on to the System as User GR##-MM1 (Optional)

The following exercise is optional.

Log on to the system as user GR##-MM1. Use the password automatically generated in the exercise for the *user master record* or assign a new initial password in user maintenance.

Change the password when you log on: _____



Hint:

You can show the transaction codes by choosing *Extras → Settings* ("Display technical names").

1. Log on to the system as user GR##-MM1.
 - a) Start SAP Logon.
 - b) Select system *T41* and choose *Log On*.
 - c) Enter the user name **GR##-MM1** in the *User* field.
 - d) Enter the generated password in the *Password* field.
Use the password automatically generated in the exercise for the *user master record* or assign a new initial password in user maintenance.
 - e) Choose *Enter*.
 - f) Enter a new productive password of your choice in the *New Password* and the *Repeat Password* fields.
New password : _____
 - g) Choose *Transfer (Enter)*.
 - h) Choose *Continue (Enter)*.
2. Set up a user-specific favorites list by defining the transactions **MM03** and **MB1C** as favorites.
 - a) Copy transactions **MM03** and **MB1C** from the *User menu* to the *Favorites* folder. To do so, open all Folders, search for the transactions and use drag-and-drop for each transaction to copy them from the *User Menu* sub-folder to the *Favorites* folder.



Hint:

You can show the transaction codes by choosing *Extras → Settings* ("Display technical names").

3. Start transaction **MM03**, and display the accounting view of material **P605-100** in plant **1010**.
Can you also display the accounting view of material **P605-100** in plant **1040**?
- No, because you **do not** have authorization for plant **1040**.
 - a) Call transaction **MM03** from the *Favorites* list.
 - b) Enter the material ID **P605-100** in the *Material* field.
 - c) Choose *Select view(s)*.
 - d) Choose the *Accounting 1* view
 - e) Choose *Continue (Enter)*.
 - f) Enter **1010** in the field *Plant* and choose *Continue (Enter)*.

The accounting view of material P605-100 for plant 1010 is shown.

- g) Choose *Back* (*F3*).
- a) Enter the material ID **P605-100** in the *Material* field.
- b) Choose *Select view(s)*.
- c) Choose the *Accounting 1* view
- d) Choose *Continue (Enter)*.
- e) Enter **1040** in the field *Plant* and choose *Continue (Enter)*.
The *Error* window indicates that you have no authorization to display data for plant 1010.
- f) Choose *Confirm (Enter)*.
- g) Choose *Cancel (F12)*.

4. Display the failed authorization check.

Why are you not able to display material P605-100 in plant 1040?

- a) Start transaction SU53
Menu path: → *System* → *Utilities* → *Display Authorization Check* (or transaction SU53)
- b) Analyze the result of the authorization check for object *M_MATE_WRK*.
The program required the following authorization values: *ACTVT = 03* and *WERKS = 1040* for the authorization object *M_MATE_WRK*.
- c) Check the authorizations assigned for object *M_MATE_WRK* by double-clicking the entry for object *M_MATE_WRK* in the list.
- d) Select *Authorization Object M_MATE_WRK* and choose *Expand Subtree (F6)*.
The result shows that the user master record contains authorization for object *M_MATE_WRK* (*ACTVT = 03, 08* and *WERKS = 1000, 1010, and 1020*), but not the required authorizations.

5. Log off as GR##-MM1.

- a) Choose *System* → *Log Off*
- b) Confirm the next system dialog with Yes.

Task 5: Create a Derived Role

Create a **derived** role GR##_MM_IM_POST1010 with authorizations for a warehouse supervisor in plant 1010.

1. Create a **derived** role GR##_MM_IM_POST1010 . Assign the imparting role GR##_MM_IM_POST and save your role.
Display the inheritance hierarchy of the roles (choose *Ctrl+Shift+F3* or the *Inheritance Hierarchy* icon).
- a) Start the role maintenance transaction:

SAP Menu: Tools → Administration → User Maintenance → Role Administration → Roles, (transaction code: PFCG).

- b) Enter the name for the role **GR##_MM_IM_POST1010** in the *Role* field.
 - c) Choose *Create Single Role*.
 - d) Enter description **Warehouse supervisor in plant 1010** in the *Description* field.
 - e) Enter **GR##_MM_IM_POST** in the *Derive from Role* field.
 - f) Then choose *Save (Ctrl+S)* to save your role.
2. Display the inheritance hierarchy of the roles.
- a) *Menu: → Role → Inheritance (Ctrl+Shift+F3)*
 - b) Select role **GR##_MM_IM_POST1010** and choose *Choose (F2)*.
3. Can you add other applications (menu entries, transaction codes, and reports, for example) or delete existing applications?
-
- a) Go to the *Menu* tab page.
No, since the menu of role **GR##_MM_IM_POST** is inherited from the role **GR##_MM_IM_POST1010**.
4. Maintain Authorizations - Define the organizational levels.
- Plant: 1010*
Did the system copy the authorizations of the imparting role?
-
- a) Go to the the *Authorizations* tab page.
 - b) Choose *Change Authorization Data*.
 - c) Enter the following values in the *Define Organizational Levels* window:
- *Plant: 1010*.
 - d) Choose *Save (Ctrl+S)* to save the authorization values for the organizational levels.
Did the system copy the authorizations of the imparting role?
No, they must either be maintained here directly or copied as described in the next exercise task.
 - e) Choose *Save (Ctrl+S)* to save the profile values .
 - f) In the *Assign Profile Name for Generated Authorization Profile* window, accept the proposed profile name and choose *Execute (Enter)*.
5. Maintain Authorizations - Copy the authorization data from the imparting role.
- a) Choose *Copy data (Ctrl+Shift+F7)*.
 - b) Choose *Continue (Enter)* to save the profile values .
The authorizations are then copied from the *imparting role* (reference role).
 - c) Choose *Save (Ctrl+S)* to save the profile values .

- d) Choose *Organizational levels* to check the value for the organizational level plant.
The plants 1000, 1010, and 1020 were **not** copied from the reference since this is an organizational level field which was previously set in the derived role.
- e) Choose Save (*CTRL+S*) to save the authorization values for the organizational levels.

6. Maintain Authorizations - Generate the authorization profile for your role.

- a) Choose the *Generate* icon.
- b) In the *Assign Profile Name for Generated Authorization Profile* window, accept the proposed profile name and choose *Execute (Enter)*.
- c) Choose *Back (F3)* to return to the *Change Roles* screen.
- d) Choose *Back (F3)* to return to the initial screen of the *Role Maintenance*.

Task 6: Optional: Copy a Role

In this additional exercise, you can create a single role GR##_SD_SALES by copying the predefined work center example ADM940_SD_SALES without user assignment.

1. Start the Role Maintenance transaction and create the role GR##_SD_SALES as a copy of the role ADM940_SD_SALES.
 - a) While still in the Role Maintenance transaction, enter the name for the role **ADM940_SD_SALES** in the *Role* field.
 - b) Choose *Copy Role (Shift + F11)*.
 - c) Enter **GR##_SD_SALES** in the *to role* field.
 - d) Choose *Copy All (Enter)*.
 - e) Choose *Change* on the *Role Maintenance Screen*.
2. Maintain Authorizations - Generate the authorization profile for your role.
 - a) Choose *Change Authorization Data* on the *Authorizations* tab.
 - b) Choose the *Generate* icon.
 - c) In the *Assign Profile Name for Generated Authorization Profile* window, accept the proposed profile name and choose *Execute (Enter)*.
 - d) Choose *Back (F3)* to return to the *Change Roles* screen.
3. Complete the maintenance of this role and return to the initial screen of transaction PFCG.
 - a) Choose *Back (F3)* to return to the initial screen of *Role Maintenance*.

Task 7: Optional: Create the Missing Three Single Roles of the Sample Authorization Concept

In this additional exercise, you can create the missing three single roles of the *sample authorization concept*.

After the creation of roles was carried out in detail in the previous exercises, you should now perform these exercises without a detailed solution.

Create the following roles:

Role	Transactions
GR##_FI_ACCREC_MAINT	FD01, FD02, FD03

Role	Transactions
GR##_FI_IP_POST	F-18, F-26, F-28
GR##_SD_CUST_MAINT	VD01, VD02, VD03

Restrict the requested organizational levels with the values specified here. The system **never** queries all the organizational levels listed here for a role. Use the following values for the fields used.

Organizational Level	Field Value
Company code	1010
Business area	1000
Account type	D
Controlling area	0001
Division	*
Sales organization	1010
Distribution channel	*

1. Create the role GR##_FI_ACCREC_MAINT.

a) Create the role GR##_FI_ACCREC_MAINT. Enter the role name and a short description.

b) Fill the menu with the required transaction codes:

- FD01
- FD02
- FD03

c) Restrict the requested organizational levels with the values specified here:

Role: **GR##_FI_ACCREC_MAINT**

Company code: **1010**.

d) Generate the profile and save the role.

2. Create the role GR##_FI_IP_POST.

a) Create the role GR##_FI_IP_POST. Enter the role name and a short description.

b) Fill the menu with the required transaction codes:

- F-18
- F-26
- F-28

c) Restrict the requested organizational levels with the values specified here:

Role **GR##_FI_IP_POST**

- Company code: 1010
- Business area: 1000
- Account type: D
- Controlling area: 0001
- Assign complete Authorization for the org. levels still open using the button *Full authorization*.

d) Generate the profile and save the role.

3. Create the role **Role GR##_SD_CUST_MAINT**.

a) Create the role GR##_SD_CUST_MAINT. Enter the role name and a short description.

b) Fill the menu with the required transaction codes:

- VD01
- VD02
- VD03

c) Restrict the requested organizational levels with the values specified here:

Role: **GR##_SD_CUST_MAINT**

- Company code: 1010
- Division: *
- Sales organization: 1010
- Distribution channel: *

Set full authorization for all remaining open authorization fields.

d) Generate the profile and save the role.

Task 8: Optional: Create Three Composite Roles that Correspond to the Sample Authorization Concept

In this additional exercise, you can create three composite roles, which correspond to the *sample authorization concept*.

After the creation of roles was carried out in detail in the previous exercises, you should now perform these exercises without a detailed solution

Create the following three composite roles.

Composite role	Corresponds to the work center from the <i>Sample Authorization Concept</i>
GR##_FI_ACCREC	Accounts receivable accountant (AccRec)
GR##_SD_SALCLK	Sales clerk (SClerk)
GR##_SD_SALMGR	Sales and Distribution manager (SDMan)

These composite roles should contain the following single roles:

Composite Role	Contained Roles
GR##_FI_ACCREC	GR##_MM_MAT_ANZ GR##_FI_ACCREC_MAINT GR##_FI_IP_POST
GR##_SD_SALCLK	GR##_MM_MAT_ANZ GR##_SD_CUST_MAINT GR##_SD_SALES
GR##_SD_SALMGR	GR##_MM_MAT_ANZ GR##_FI_ACCREC_MAINT GR##_SD_CUST_MAINT GR##_SD_SALES

1. Create the composite role **GR##_FI_ACCREC**.

- a) Create the composite role GR##_FI_ACCREC. Enter the role name and a short description.
- b) Go to the *Roles* tab page and select the corresponding single roles and copy them into your composite role.

Your composite role should consist of the roles of the role definition in the sample authorization concept:

- GR##_MM_MAT_ANZ
- GR##_FI_ACCREC_MAINT
- GR##_FI_IP_POST

- c) Optionally, you can further customize the menu of the composite role.

Choose *Import Menu* on the *Menu* tab page. You can move and restructure the entries with the mouse. By creating folders with the *Create folder* button, you can organize your transactions from a functional or process-oriented point of view.

- d) Save the composite role.

2. Create the composite role **GR##_SD_SALCLK**.

- a) Create the composite role GR##_SD_SALCLK. Enter the role name and a short description.
- b) Go to the *Roles* tab page and select the corresponding single roles and copy them into your composite role.

Your composite role should consist of the roles of the role definition in the sample authorization concept:

- GR##_MM_MAT_ANZ
- GR##_SD_CUST_MAINT

- GR##_SD_SALES
- c) Optionally, you can further customize the menu of the composite role.
Choose *Import Menu* on the *Menu* tab page. You can move and restructure the entries with the mouse. By creating folders with the *Create folder* button, you can organize your transactions from a functional or process-oriented point of view.
- d) Save the composite role.
3. Create the composite role **GR##_SD_SALMGR**.
- a) Create the composite role GR##_SD_SALMGR. Enter the role name and a short description.
 - b) Go to the *Roles* tab page and select the corresponding single roles and copy them into your composite role.
Your composite role should consist of the roles of the role definition in the sample authorization concept:
 - GR##_MM_MAT_ANZ
 - GR##_FI_ACCREC_MAINT
 - GR##_SD_CUST_MAINT
 - GR##_SD_SALES
 - c) Optionally, you can further customize the menu of the composite role.
Choose *Import Menu* on the *Menu* tab page. You can move and restructure the entries with the mouse. By creating folders with the *Create folder* button, you can organize your transactions from a functional or process-oriented point of view.
 - d) Save the composite role.



LESSON SUMMARY

You should now be able to:

- Implement a derived role strategy.

Outlining Subtleties of Authorization Maintenance

LESSON OVERVIEW

This lesson will describe special features in role maintenance (PFCG). These include:

- The red, yellow, and green traffic lights
- The icons in authorization maintenance
- The status texts for authorizations

Business Example

The authorization administration must understand the use of the icons and the meaning of status values for his or her daily work. Depending on the requirements in the company, the administrator may require additional display and control options for this, which are provided through expert mode or the menu.



LESSON OBJECTIVES

After completing this lesson, you will be able to:

- Describe the special features in SAP Business Role Maintenance.

Icons and Additional Information for Authorization Maintenance

When maintaining and editing authorizations in role maintenance, different terms and icons appear that are perhaps not always correctly interpreted. What task do the traffic lights perform, for example?



Traffic lights refer to authorization fields in lower branches

Group/Object/Authorization/Field	Maintain...	Value	
Object Class AAAB	Standard		
Object Class BC_A	Standard		
Object Class BC_C	Standard		
Object Class CO	Standard		
Object Class FI	Standard		
Object Class IS	Standard		
Authorization Object W_BETR_USR	Standard		
Authorization T-T108036000	Standard		
WERKS (\$WERKS)	Standard		
ACTVT	Standard		
Object Class MM_E	Standard		
Object Class MM_G	Standard		
Object Class PS	Standard		
Object Class SD	Standard		
Authorization Object V_KNA1_VKO	Standard		
Authorization T-T108036000	Standard		
VKORG (\$VKORG)	Standard		
VTWEG (\$VTWEG)	Standard		
SPART (\$SPART)	Standard		
ACTVT	Standard		
Authorization Object V_VBAK_AAT	Standard		
Authorization Object V_VBAK_VKO	Standard		

Figure 81: Authorization Maintenance: Traffic Light Legend

The traffic lights are among the most important icons for the administration of authorizations. You can use them to obtain an overview very quickly. They display the current maintenance status of the authorizations at various levels. The different icons here are Green, Yellow, and Red.

Green: All fields below this level have been filled with values.



Hint:

If your entry did **not** make the light go green, this is due to an SAP proposal.



Caution:

Regardless of the color, you must **always check all entries**. A Green traffic light does not mean that you can accept everything without checking it.

Yellow: There is at least one field (but no organizational level) below this level for which no data has been proposed or entered.

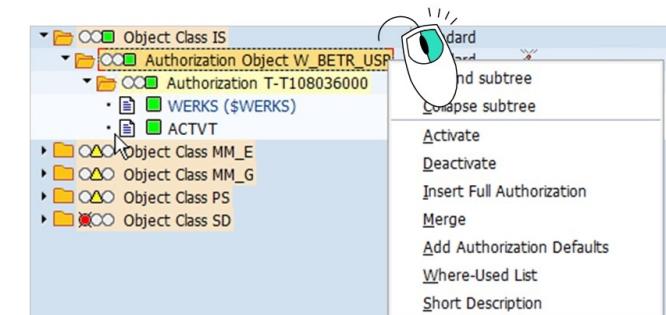
Red: There is at least one organizational level field (also known as org level) below this level for which no value has been maintained.



Caution:

Never assign organizational levels directly in the structure. This would cause the (possibly critical) status “Changed” (to be explained later in this lesson). Always use the central button *Organizational Levels* or the key combination “Ctrl + F8” to assign the values.

Authorization Maintenance: Additional Functions



The screenshot shows the SAP Authorization Maintenance interface. A context menu is open over an authorization object named 'Authorization T-T108036000'. The menu includes options like Standard, Standard subtree, and Compose subtree, followed by a separator line and then a list of functions:

- Activate
- Deactivate
- Insert Full Authorization
- Merge
- Add Authorization Defaults
- Where-Used List
- Short Description

Maintain field contents

Figure 82: Authorization Maintenance: Additional Functions

Functions that are provided by the context menu of the object classes, authorization objects, authorizations, and authorization fields are:

Assignment of authorizations: Displays the transactions that use this object.

Full authorization: You can set full authorization.

Assigning full authorization for all empty fields: If you require a role with full authorizations or want to assign "*" to all empty fields for test purposes, follow the procedure below.



Hint:

Assigning full authorization for all empty fields

If you click on a Yellow or Red traffic light in the status line, the system queries whether you want to assign the full authorization asterisk "*" for all unmaintained authorizations.

You can use the traffic lights at the level of object classes, objects, or authorizations in the same way to assign full authorization for the structure below that level. This does **not** maintain the organizational levels, and you should first use the "Organizational Levels" button to enter and assign them.

To assign full authorization for all empty fields of a role you can click on the Status icon.

Field contents: Choose the maintain icon to maintain an authorization field value.

Alternatively, you can double-click the authorization field content, or click an empty field. You enter the values in a separate input window.

Copy: If you choose copy, a complete specification for an authorization object is copied with all fields. The status of the template is retained.

Merge: You can merge identical field contents for authorization fields of an authorization object.

**Hint:**

Under certain conditions, you can merge authorizations for the same object. The merge ignores the maintenance status (Standard/Maintained/Changed/Manual) of the authorizations involved. This could result in standard authorizations being combined with authorizations with different statuses, leading to unexpected behavior of the standard authorizations.

**Caution:**

There are **new rules** here for merging. The most important and principle rule is associated with the activation status and maintenance status.

Both the activation status (Active/Inactive) and the maintenance status (Standard/Maintained/Changed/Manual) of the authorizations must match.

Exception: Changed authorizations can be merged with manual authorizations, as long as the activation status is the same.

If the activation and maintenance statuses are the same, the second condition comes into play. Authorizations can be merged only if one of the further conditions is met.

- One of the authorizations is included in the other authorization, with reference to all fields (the identity is also considered as a special case).
- Only one field is different in the two authorizations; all others are the same.

There are further exceptions here, however:

- An authorization that has empty fields cannot be merged with another authorization where at least one of these fields has content.
- An authorization that has fields with full authorization (*) cannot be merged with another authorization where at least one of these fields does not have full authorization.

Delete: Delete the content of a field or delete an inactive authorization, or delete all inactive authorizations.

Activate/Deactivate: You can technically hide authorizations and show specifications for the check in the profile (the entry is retained). Although deleting the authorization has the same effect, it is not as simple to return to the default value in that case.

**Hint:****Deactivate**

- At authorization object level: All subordinate authorizations are marked as *inactive*.
- At authorization level: This authorization is marked as *inactive*.

Note: Reactivate

This icon means that the authorization or all subordinate authorizations of an authorization object are reset to *Active*.

**Note:**

The **Inactive** and **Reactivate** function has also changed its behavior in the system.

Previously, each authorization was switched to the status “**Inactive Standard**” regardless of the original status “Standard”, “Maintained”, or “Changed”. This caused complications when merging authorizations.

The status is now always retained. If, for example, an authorization has the status “Changed”, it is now switched to “Inactive Changed”.

Authorization Maintenance: Status Texts



Status Texts for Authorizations

- **Standard:** Field values have not been changed
- **Maintained:** Value entered in field delivered empty
- **Changed:** Field delivered with content was changed
- **Manual:** Authorization object was inserted manually



Status Texts after a Comparison (such as change in menu selection)

- **Old:** No field value changed and no new authorization added
- **Updated:** The merge process led to changes in field values
- **New:** At least one new authorization added



Figure 83: Authorization Maintenance: Status Texts

Status Texts for Authorizations

Standard: All field values in the subordinate levels of the hierarchy are unchanged from the SAP defaults.


Hint:

This includes both filled and unfilled organizational level fields.

The condition for the filled fields is that the entry was made using the maintenance button “Organizational Levels”, and for unfilled fields, that the original value \$.... is displayed.

Maintained: At least one field in the subordinate levels of the hierarchy was empty by default and has since been filled with a value.

Changed: The proposed value for at least one field in the subordinate levels of the hierarchy has been changed from the SAP default value.

Manual: You maintained at least one authorization in the subordinate hierarchy levels manually (it was not proposed by Role Maintenance).

The “Yellow Traffic Light Problem”.

**Caution:**

Yellow traffic light effect. If the status jumps from *Standard/Maintained* to *Changed* due to an action in the authorizations, Role Maintenance cannot create a connection between this object entry and the menu. Therefore, for every action that requires “*Read old status and merge with new data*”, the *Standard* is read again (can also be forced in expert mode). The only exception here is when the new standard is included in the existing authorizations. For more information about this, see SAP Note 113290.

You will also see *Changed* for entries for organization levels that are not globally set (using the buttons).

**Note:**

This special feature can also lead to entries being copied into the authorizations that cannot be identified by a *Yellow* traffic light. *Red traffic lights* (uncritical, since values are missing here) or even *green traffic lights* (critical since all fields are filled in this case) can appear with new entries. Always pay attention to and consider the status *New* when processing the authorizations.

Here is the solution for this problem, so that it does not occur repeatedly when you are processing the authorizations:

**Hint:**

Before you make a change to authorizations that generates the status *Changed*, you must **first** perform the following steps:

- 1. Copy the appropriate (standard) instance.**
- 2. Set the template to inactive.**
- 3. Make the changes to the copy.**

Only by performing these steps can you avoid the default being read again and again, and ensure that you have no inexplicable values to maintain.

Status Texts After a Comparison

Old: The comparison found that all field values in the subordinate levels of the hierarchy are still current and that no new authorizations have been added.

New: The comparison found that at least one new authorization has been added to the subordinate levels of the hierarchy. If you now click *New* in the application toolbar, all new authorizations in the subordinate levels are expanded.

Display of Deleted Authorizations and Values for Merging of Authorizations

Following changes to applications in the role menu, the old authorizations are merged with the new authorization default values when authorization maintenance is started. Through this merge process, authorizations can be added, updated, or deleted.

Authorization maintenance displays which authorizations have been added or updated.

The ALV tree technology for authorization maintenance also displays which authorizations have been deleted and which authorization values have been added or deleted.

The ALV display provides the following enhancements for the merging of authorizations:

- In the column for the update status, authorization maintenance now indicates whether a value range has been added or changed at field level, too.
- In addition, a second window is displayed at the right or bottom margin, displaying deleted authorizations and values.



Note:

If you are still using the old tree display, you can switch to the new ALV display as of SAP NetWeaver 7.50.

Call transaction PFCG and navigate to the *Authorizations* tab page. Choose *Display Authorization Data* or *Change Authorization Data*. Choose *Utilities → Settings* from the menu and set the option for using the ALV tree. Note that you have to restart authorization maintenance.



Change Role: Authorizations

Role ADM940_DEMO
Maint. 0 unmant. org. levels, 0 open fields
Status: Changed

Group/Object/Authorization/Field	Maintain...	Update...	...	V...
Object Class AAAB	Maintained	Updated		
Object Class BC_A	Manual	Old		
Object Class BC_C	Standard	Old		
Object Class CO	Maintained	Old		
Object Class FI	Maintained	Updated		
Authorization Object F_BKPF_BED	Maintained	Old		
Authorization Object F_BKPF_BEK	Maintained	Old		
Authorization Object F_BKPF_BES	Maintained	Old		
Authorization Object F_BKPF_BLA	Maintained	Old		
Authorization Object F_BKPF_BUK	Standard	Old		
Authorization Object F_BKPF_BUP	Maintained	Old		
Authorization Object F_BKPF_GSB	Standard	Old		
Authorization Object F_BKPF_KOA	Standard	Old		
Authorization Object F_FAGL_LDR	Maintained	Old		
Authorization Object F_FAGL_SEG	Maintained	Old		
Authorization Object F_FICB_FKR	Standard	Old		
Authorization Object F_KNA1_BED	Maintained	Old		
Authorization Object F_KNA1_BUK	Standard	Updated		
Authorization Object F_KNA1_GEN	Standard	Old		
Authorization Object F_KNA1_GRP	Maintained	Old		
Authorization Object F_LFA1_BEK	Maintained	Old		
Authorization Object F_LFA1_BUK	Standard	Updated		
Authorization Object F_LFA1_GEN	Standard	Old		
Authorization Object F_LFA1_GRP	Maintained	Updated		
Authorization Object F_MANDATE	Standard	Old		
Object Class IS	Standard	Old		
Object Class MM_E	Maintained	Old		
Object Class MM_G	Maintained	Old		

Deleted Authorizations and Values (Merge)

Group/Object/Authorization/Field	Maintain...	Update...	'Fr...
Object Class AAAB			
Object Class BC_A			
Object Class CO			
Authorization Object K_PCAR_REP			
Authorization T-T108036000	Maintain... Deleted		
BUKRS (\$BUKRS)	Standard	*	
PRCTR (\$PRCTR)	Standard	*	
KSTAR	Maintain...	*	
ACTVT	Standard	Display i	
Object Class FI			

Figure 84: Merging of Authorizations in Role Maintenance

In addition, the ALV display supports mass changes of authorization values in role maintenance.

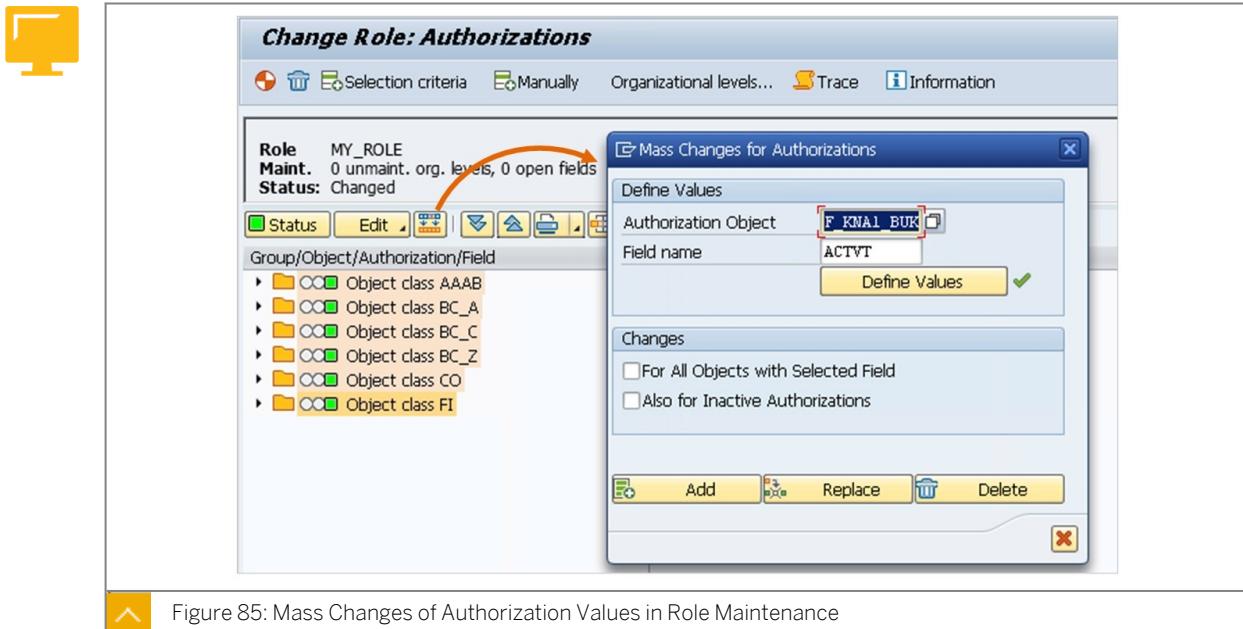


Figure 85: Mass Changes of Authorization Values in Role Maintenance

Mass Maintenance of Authorization Values in Roles

Transaction PFCGMASSVAL allows you to change the authorization values of multiple roles at the same time.

This includes the changing of organizational level values, field values of authorizations for a selected object, and cross-object field value maintenance of authorizations for a selected authorization field.

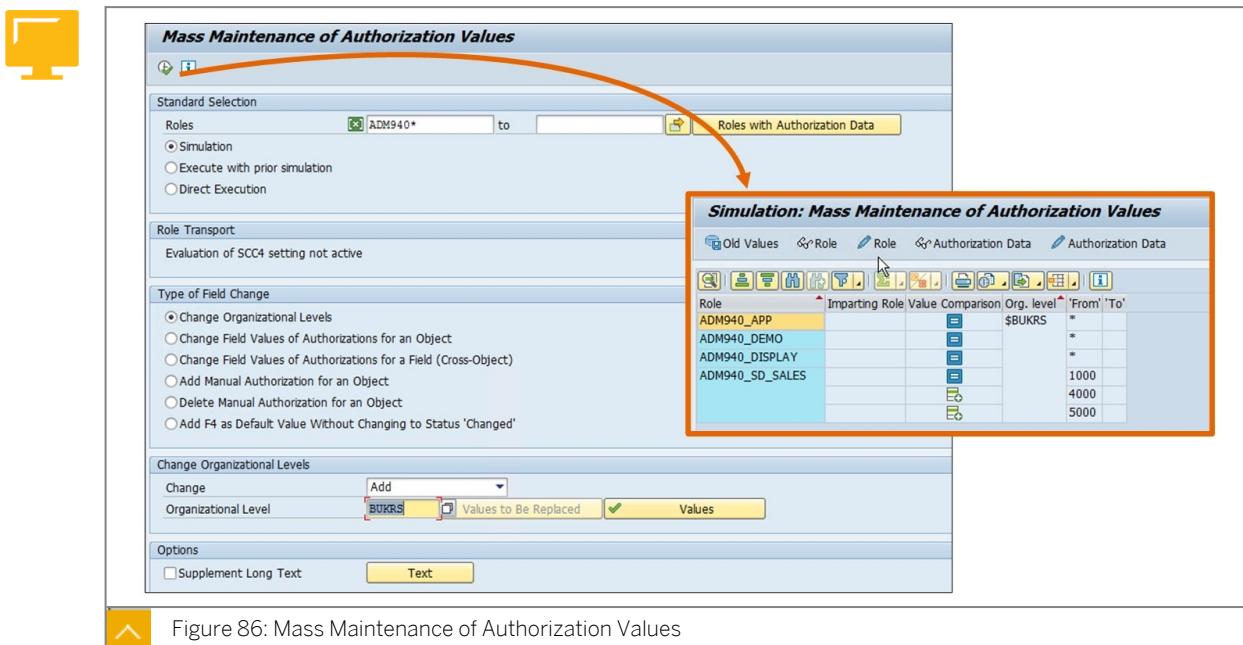


Figure 86: Mass Maintenance of Authorization Values

Note:

For details see SAP Note: 2177996 – PFCGMASSVAL: Mass maintenance of authorization values in roles.

Unit 4

Exercise 7

Practice System Exercise: Understand the Subtleties of Authorization Maintenance

Business Example

After you have used *Role Maintenance* for some time, you usually know all of the functions. However, some occurrences, such as *yellow* traffic lights that keep appearing and the status *inactive* often still cause some misunderstandings. This exercise reinforces your knowledge of the special features of *Role Maintenance*.

Task 1: Explaining Traffic Light Colors

Create the role *GR##_RGB* by copying *ADM940_RGB* without user assignments and personalization.

1. Start the *Role Maintenance* transaction and create the role *GR##_RGB* as a copy of the role *ADM940_RGB*.
2. What traffic light colors are displayed for the authorization objects used?

3. What does a **red** traffic light mean?

4. The *Profile Generator* has written a default value in the field with the field text *Plan Version*. Use the search function to find the authorization field.
Note the field value. Explain the meaning of the first character.

Result

The field you are looking for has the field name *PLVAR* (authorization object *PLOG*) and the default value *\$PLVAR*.

A “\$” character at the beginning of a field always indicates a variable for an organizational level.

5. Maintain Authorizations - Maintain authorization values for the organizational level *PLVAR*.
6. What does a **Yellow** traffic light mean, and which objects (role *GR##_RGB*) have this status?

7. What does the **Green** traffic light color mean, and what do you have to take into account here?

This must be taken into account: _____

Result

The Green traffic light indicates structures in which all fields are assigned a value. However, it is not possible to identify whether this is:

- An authorization default value
- An organizational level field that received the field value through the maintenance button
- A field for which the authorization default value was changed
- An organizational level field filled directly in the structure (not using the button)



Hint:

Take into account the fact that authorization objects with the status *Standard* and a *Green* traffic light are entirely authorization default values. *Green* does **not** mean that you do not have to check these default values.

8. Assign the following values to the field authorization object S_USER_GRP:

- CLASS = DEMO
- ACTVT = 03

Result

When changing the authorization default value for the field ACTVT, Role Maintenance automatically adds a new inactive entry for authorization object S_USER_GRP with authorization default values.

9. Generate the authorization profile for your role:

Task 2: Use Expert Mode to Merge the Existing Authorization Data

While still in the tab *Authorization*, use expert mode to merge the existing authorization data with the authorization default values again.

1. What choice must be made when starting the maintenance so that the Profile Generator reads default values again?

2. Start the role maintenance transaction to open the role GR##_RGB and add transaction FD03 to the menu.

3. Read the authorization default values again.
4. Which object class / authorization objects / has the status *New*?
Object class:

Authorization objects:

5. Generate the authorization profile for your role.
6. Delete transaction `FD03` in the role menu.
7. Read the authorization default values again.

Result

The removed authorization values are shown in the *Deleted Authorizations and Values (Merge)* area.

8. Generate the authorization profile for your role.
9. Complete the maintenance of this role and return to the initial screen of transaction `PFCG`.

Task 3: Use Mass Maintenance of Authorization Values in Roles

Add further values for the field company code in the previously created roles `GR##_*`. Use the mass maintenance of authorization values in roles.

1. Start transaction `PFCGMASSVAL`.
2. Add the values `90FR`, `90CA`, and `90US` to the values of the field company code.
3. Start the mass maintenance.

Unit 4 Solution 7

Practice System Exercise: Understand the Subtleties of Authorization Maintenance

Business Example

After you have used *Role Maintenance* for some time, you usually know all of the functions. However, some occurrences, such as *yellow* traffic lights that keep appearing and the status *inactive* often still cause some misunderstandings. This exercise reinforces your knowledge of the special features of *Role Maintenance*.

Task 1: Explaining Traffic Light Colors

Create the role **GR##_RGB** by copying **ADM940_RGB** without user assignments and personalization.

1. Start the *Role Maintenance* transaction and create the role **GR##_RGB** as a copy of the role **ADM940_RGB**.
 - a) SAP Menu:
Tools → Administration → User Maintenance → Role Administration → Roles, (transaction code **PFCG**).
 - b) Enter the name of the role **ADM940_RGB** in the *Role* field.
 - c) Choose *Copy Role* (*Shift + F11*).
 - d) Enter **GR##_RGB** in the *to role* field.
 - e) Choose *Copy All* (*Enter*).
 - f) Choose *Change* on the *Role Maintenance* screen..
2. What traffic light colors are displayed for the authorization objects used?

- a) Select the tab *Authorizations* and choose the button *Change Authorization Data*.
- b) Explore the traffic lights in the *Group/Object/Authorization/Field* column.

The following traffic light colors are displayed for the authorization objects used:

- Red
- Yellow
- Green

3. What does a **red** traffic light mean?

-
- a) A red traffic light stands for an unfilled organizational level field.
4. The Profile Generator has written a default value in the field with the field text *Plan Version*. Use the search function to find the authorization field.
Note the field value. Explain the meaning of the first character.
-
- a) Open the search option by choosing the *Search* icon or the menu path *Edit → Find*.
- b) Enter **plan version** in the “*or field text*” field in the *Find Field* area.
- c) Choose *Find Field*.
- Result**
The field you are looking for has the field name *PLVAR* (authorization object *PLOG*) and the default value *\$PLVAR*.
A “\$” character at the beginning of a field always indicates a variable for an organizational level.
5. Maintain Authorizations - Maintain authorization values for the organizational level *PLVAR*.
- a) Choose *Organizational Levels*.
- b) Enter the following value in the *Define Organizational Levels* window:
- *Plan Version: 01*,
- c) Choose *Save (Ctrl+S)* to save the authorization values for the organizational levels.
6. What does a **Yellow** traffic light mean, and which objects (role *GR##_RGB*) have this status?
-
-
-
-
-

- a) Expand the *Object Class BC_A* node.

Yellow traffic lights indicate a structure in which at least one field does not yet contain a value.

The following objects have not yet been given default values by the Profile Generator:

- *S_USER_AGR*
- *S_USER_AUT*
- *S_USER_GRP*
- *S_USER_PRO*
- *S_USER_SAS*

- *S_USER_STA*
- *S_USER_SYS*
- *S_USER_TCD*
- *S_USER_VAL*

7. What does the **Green** traffic light color mean, and what do you have to take into account here?

This must be taken into account: _____

Result

The Green traffic light indicates structures in which all fields are assigned a value. However, it is not possible to identify whether this is:

- An authorization default value
- An organizational level field that received the field value through the maintenance button
- A field for which the authorization default value was changed
- An organizational level field filled directly in the structure (not using the button)



Hint:

Take into account the fact that authorization objects with the status *Standard* and a *Green* traffic light are entirely authorization default values. *Green* does **not** mean that you do not have to check these default values.

8. Assign the following values to the field authorization object *S_USER_GRP*:

- CLASS = *DEMO*

- ACTVT = 03

- a) Open the search option by choosing the *Search* icon or the menu path *Edit → Find*.
- b) Enter **s_USER_GRP** in the *Authorization Object* field in the *Find Object* area.
- c) Choose *Find Object*.
- d) Choose the *Pencil* button on the right side of the *CLASS* field.
- e) Enter **DEMO** in the *Field values* window.
- f) Choose *Transfer (Enter)*.
- g) Choose the *Pencil* button on the right side of the *ACTVT* field.

- h) Deselect all activities excluding **03** in the *Field values* window.
- i) Choose *Transfer (Enter)*.

Result

When changing the authorization default value for the field ACTVT, Role Maintenance automatically adds a new inactive entry for authorization object **S_USER_GRP** with authorization default values.

9. Generate the authorization profile for your role:
 - a) Choose the *Generate* icon.
 - b) In the *Generate Profile* window, choose *Generate*.
 - c) In the *Assign Profile Name for Generated Authorization Profile* window, accept the proposed profile name and choose *Execute (Enter)*.
 - d) Choose *Back (F3)* to return to the *Change Roles* screen.
 - e) While still in the tab *Authorization*, go to the next task.

Task 2: Use Expert Mode to Merge the Existing Authorization Data

While still in the tab *Authorization*, use expert mode to merge the existing authorization data with the authorization default values again.

1. What choice must be made when starting the maintenance so that the Profile Generator reads default values again?

- a) On the *Authorizations* tab page, choose the *Expert Mode for Profile Generation* icon. Then, choose the mode *Read old status and merge with new data*.
- b) Choose *Back F3* to go back to the tab *Authorizations*.
- c) Choose *Back F3* to go back to the *Role Maintenance* screen.
2. Start the role maintenance transaction to open the role **GR##_RGB** and add transaction FD03 to the menu.
 - a) While still in the Role Maintenance transaction, enter the name for the role **GR##_RGB** in the *Role* field.
 - b) Choose the *Change* icon.
 - c) Open the *Menu* tab page.
 - d) Choose the *Transaction* button and enter the following transaction code in the *Transaction code* field:
 - FD03
 - e) Choose *Assign Transactions*.
 - f) Then choose *Save (Ctrl+S)* to save your role.
3. Read the authorization default values again.
 - a) Open the *Authorizations* tab page.
 - b) Choose *Expert Mode for Profile Generation* on the *Authorizations* tab.

- c) Select the radio button for the option *Read old status and merge with new data*.
 - d) Choose *Execute (Enter)*.
 - e) Choose *Cancel (F12)* on the *Define Organizational Levels* window.
4. Which object class / authorization objects / has the status *New*?
- Object class:
-
- Authorization objects:
-
- a) Search the authorizations for a line with the entry *New*:
- Object class:
- FI
- b) Expand the *Object Class FI* node.
- Authorization objects:
- F_KNA1_APP, F_KNA1_BED, F_KNA1_BUK, ...
5. Generate the authorization profile for your role.
- a) Choose the *Generate* icon.
 - b) In the *Generate Profile* window, choose *Generate*.
 - c) In the *Assign Profile Name for Generated Authorization Profile* window, accept the proposed profile name and choose *Execute (Enter)*.
 - d) Choose *Back (F3)* to return to the *Change Roles* screen.
6. Delete transaction *FD03* in the role menu.
- a) Open the *Menu* tab page.
 - b) Select the entry *FD03 - Display Customer (Accounting)* and choose the *Delete Node* icon.
 - c) Then choose *Save (Ctrl+S)* to save your role.
7. Read the authorization default values again.
- a) Open the *Authorizations* tab page.
 - b) Choose *Expert Mode for Profile Generation* on the *Authorizations* tab.
 - c) Select the radio button for the option *Read old status and merge with new data*.
 - d) Choose *Execute (Enter)*.
 - e) Choose *Cancel (F12)* on the *Define Organizational Levels* window.
- Result**
- The removed authorization values are shown in the *Deleted Authorizations and Values (Merge)* area.
8. Generate the authorization profile for your role.
- a) Choose the *Generate* icon.

- b) In the *Generate Profile* window, choose *Generate*.
 - c) In the *Assign Profile Name for Generated Authorization Profile* window, accept the proposed profile name and choose *Execute (Enter)*.
 - d) Choose *Back (F3)*, to return to the *Change Roles* screen.
9. Complete the maintenance of this role and return to the initial screen of transaction PFCG.
- a) Choose *Back (F3)* to return to the initial screen of the *Role Maintenance*.

Task 3: Use Mass Maintenance of Authorization Values in Roles

Add further values for the field company code in the previously created roles *GR##_**. Use the mass maintenance of authorization values in roles.

1. Start transaction PFCGMASSVAL.
- a) In the *OK* code field, enter the transaction code PFCGMASSVAL.
2. Add the values 90FR, 90CA , and 90US to the values of the field company code.
 - a) Enter **GR##_*** in the *Roles* field.
 - b) Select *Execute with prior simulation* in the *Standard Selection* area.
 - c) Select *Change Organizational Levels* in the *Type of field change* area.
 - d) In the *Change* field, enter *Add*.
 - e) In the *Organizational Level* field, enter BUKRS.
 - f) Choose the *Values* button, and enter the values , 90FR, 90CA and 90US.
 - g) Choose *Transfer (Enter)*.
3. Start the mass maintenance.
 - a) Choose *Execute (F8)*.

A list is displayed which shows a simulation of the respective changes.

Then choose *Execute (F8)* to perform the changes.

Result

Now the values are added to the field company code in the roles *GR##_** .



LESSON SUMMARY

You should now be able to:

- Describe the special features in SAP Business Role Maintenance.

Learning Assessment

1. Which of the following are views offered by Role Maintenance in SAP?

Choose the correct answers.

- A Basic maintenance
- B Advanced view
- C Complete view
- D Customization view

2. When using composite roles, if the contents of the assigned single roles are changed, these changes are automatically visible in the composite role menu.

Determine whether this statement is true or false.

- True
- False

3. If you assign a number of single roles to a user, multiple listings of individual menu entries can occur.

Determine whether this statement is true or false.

- True
- False

4. Derived roles inherit the menu structure and the functions included (transactions, reports, Web links, and so on) from the referenced role.

Determine whether this statement is true or false.

- True
- False

5. Which of the following statements are true about the traffic light colors used for authorizations?

Choose the correct answers.

- A Green indicates that all fields below this level have been filled with values.
- B Yellow suggests that all fields have been properly filled.
- C Red signifies that at least one organizational level field below this level lacks a maintained value.
- D Yellow means at least one field (not an organizational level) below this level has no proposed or entered data.

6. Organizational levels should be directly assigned in the structure to prevent any potential issues related to the status “Changed.”

Determine whether this statement is true or false.

- True
- False

Learning Assessment - Answers

1. Which of the following are views offered by Role Maintenance in SAP?

Choose the correct answers.

- A Basic maintenance
- B Advanced view
- C Complete view
- D Customization view

Role Maintenance offers both Basic maintenance and Complete view as part of its features.

2. When using composite roles, if the contents of the assigned single roles are changed, these changes are automatically visible in the composite role menu.

Determine whether this statement is true or false.

- True
- False

The statement is false.

3. If you assign a number of single roles to a user, multiple listings of individual menu entries can occur.

Determine whether this statement is true or false.

- True
- False

The statement is true.

4. Derived roles inherit the menu structure and the functions included (transactions, reports, Web links, and so on) from the referenced role.

Determine whether this statement is true or false.

True

False

The statement is true.

5. Which of the following statements are true about the traffic light colors used for authorizations?

Choose the correct answers.

A Green indicates that all fields below this level have been filled with values.

B Yellow suggests that all fields have been properly filled.

C Red signifies that at least one organizational level field below this level lacks a maintained value.

D Yellow means at least one field (not an organizational level) below this level has no proposed or entered data.

The following statements are true: Green indicates that all fields below this level have been filled with values. Red signifies that at least one organizational level field below this level lacks a maintained value. Yellow means at least one field (not an organizational level) below this level has no proposed or entered data.

6. Organizational levels should be directly assigned in the structure to prevent any potential issues related to the status "Changed."

Determine whether this statement is true or false.

True

False

Organizational levels should not be directly assigned in the structure to avoid causing the (possibly critical) status "Changed." Always use the central button Organizational Levels or the key combination "Ctrl + F8" to assign values.

Lesson 1

Investigating Installation and Upgrade Tasks	192
Exercise 8: Practice System Exercise: Maintain Authorization Default Values	203

Lesson 2

Maintaining Access Control and User Administration	211
--	-----

Lesson 3

Implementing User and Authorization Management Strategies	227
Exercise 9: Practice System Exercise: Access Control and User Administration	237

UNIT OBJECTIVES

- Manage installation and upgrade tasks in SAP Business Role Maintenance.
- Manage access control configuration.
- Implement user and authorization management strategies.

Investigating Installation and Upgrade Tasks

LESSON OVERVIEW

This lesson provides an overview of the steps required to install the Role Maintenance. The Role Maintenance has been activated since SAP R/3 4.6.

The lesson also explains which steps are to be performed after an upgrade, and how you can continue to use profiles that you have already created manually.

Business Example

Before the Role Maintenance can be used, you must activate it in the system and link it with default tables for the delivered SAP transaction codes.

If the customer performs an upgrade, various postprocessing is required in connection with the Role Maintenance and existing combinations of authorizations. This includes manually created authorization concepts that are to be migrated.



LESSON OBJECTIVES

After completing this lesson, you will be able to:

- Manage installation and upgrade tasks in SAP Business Role Maintenance.

Basic Settings for Using Role Maintenance

Activating Role Maintenance after a **new installation** requires two steps.

Required Steps for Operating Role Maintenance



- The SAP system profile parameter *auth/no_check_in_some_cases* has the value "Y"
- The default tables are filled, which control the behavior of Role Maintenance when a transaction is selected in a role.

Both steps are described in detail in this lesson.



Hint:

The parameter *auth/no_check_in_some_cases* is already set to "Y" in the default settings. You only need to create the customer default tables.

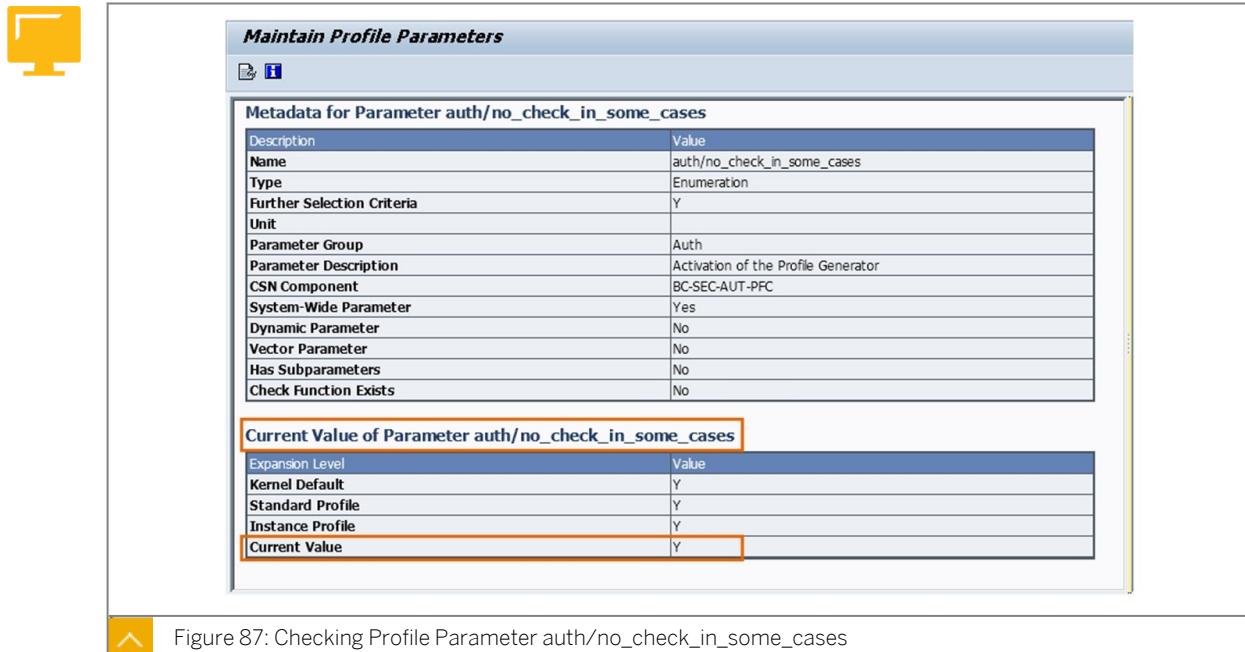


Figure 87: Checking Profile Parameter auth/no_check_in_some_cases

You only need to check that the profile parameter is set to the correct value.

To check this, use transaction RZ11. The figure shows transaction RZ11 after you have entered the parameter name (*auth/no_check_in_some_cases*). For *Current value*, Y must be entered.

To check this, use transaction RZ11. The figure shows transaction RZ11 after you have entered the parameter name (*auth/no_check_in_some_cases*). For *Current value*, Y must be entered.

You can find more details on the currently selected parameter by choosing *Documentation*.

Alternatively, you can select and check the parameter setting using report RSPFPAR.



Hint:

If the parameter has the value "N", it must have been set to this value in the default profile or in the instance profiles of the SAP system. Transaction RZ10 is used to maintain and manage these profiles (you can call this transaction by choosing *Tools* → *CCMS* → *Configuration* → *Profile Maintenance* → *System Profiles*). You should use this transaction to delete the parameter from both the default and the instance profiles. The parameter is then set to its default value "Y".

Where do the Default Values Come From?

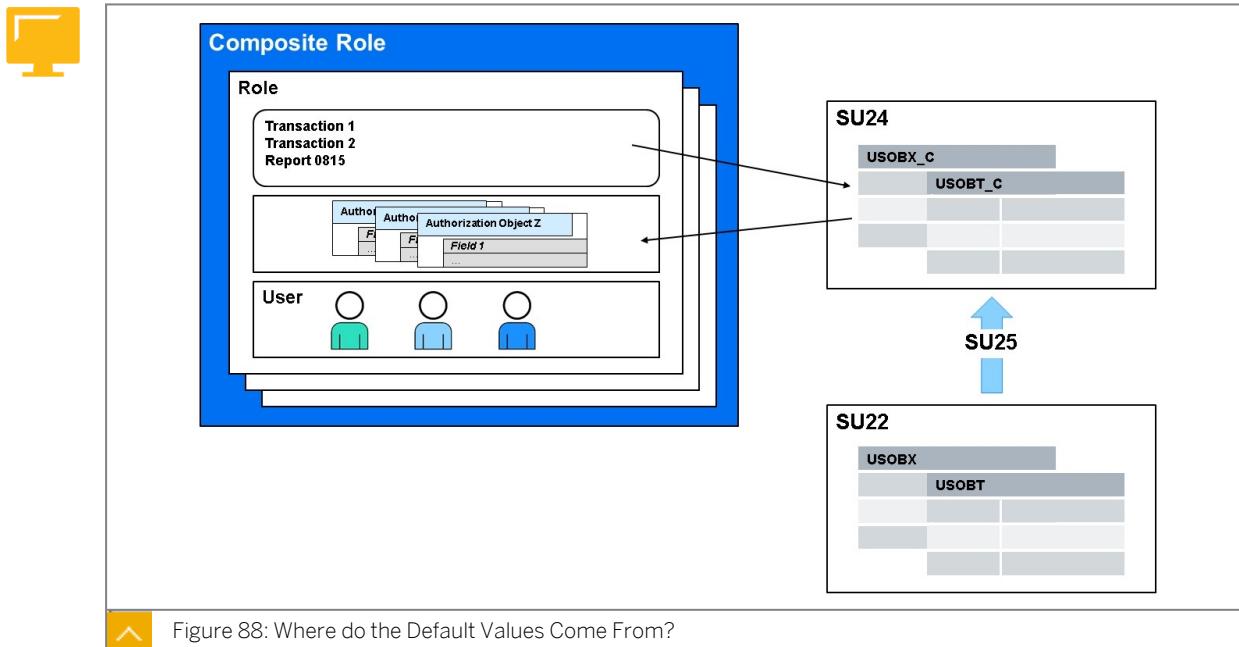


Figure 88: Where do the Default Values Come From?

If an administrator selects a transaction while creating a role, Role Maintenance selects the authorization objects that are checked in this transaction and maintained in Role Maintenance. Four cases can occur:

- For an authorization object against which the check is performed in the selected transaction, Role Maintenance has default values for the authorization content so that full authorization can be provided. The traffic light beside the authorization is **green**.
- For an authorization object against which the check is performed in the selected transaction, Role Maintenance does not have default values for the authorization content. In the example on the slide, the SAP Office transaction S001 has been selected, from which you can access files at operating system level. For security reasons, no specifications are made as to which files can be accessed in read-only or in write mode. The traffic light beside the authorization is **yellow**.
- For an authorization object against which the check is performed in the selected transaction, Role Maintenance does not have default values for the authorization content, and this field is an “organizational level field”. The traffic light beside the authorization is therefore **red**.
- It may be the case that some authorization checks during transaction processing were not maintained in Role Maintenance. The corresponding authorization objects do not appear in the profile overview.



Hint:

This should, however, only occur as an exception. It is usually sensible to maintain the missing authorization objects in the tables using transaction SU24.

Tables *USOBX_C* and *USOBT_C* control the behavior of Role Maintenance after the transaction has been selected. After a new installation, these tables are empty and must be

filled with values before Role Maintenance is used for the first time. The next step, shown on the next slide is required to do this.

Initial Fill of the Default Tables

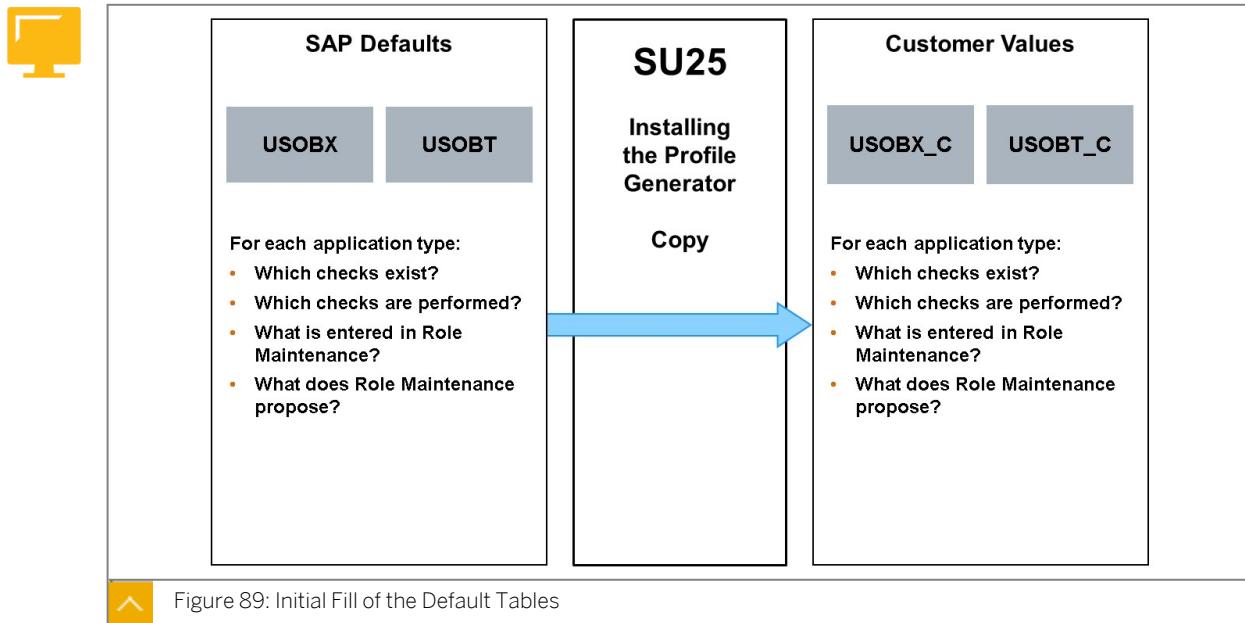


Figure 89: Initial Fill of the Default Tables

SAP delivers the tables `USOBX` and `USOBT`. These tables are filled with default values and are used for the initial fill of the customer tables `USOBX_C` and `USOBT_C`. After the initial fill, you can modify the customer tables, and therefore the behavior of Role Maintenance, if required.

Table `USOBX` defines which authorization checks are to be performed within a transaction and which are not (despite programmed *authority-check* command). This table also determines which authorization checks are maintained in Role Maintenance.

Table `USOBT` defines for each transaction and for each authorization object which default values an authorization created from the authorization object should have in Role Maintenance.

Under menu item 1, *Initially Fill the Customer Tables*, transaction `SU25` copies the SAP defaults from `USOBX` and `USOBT` to the customer tables `USOBX_C` and `USOBT_C`. You can use Role Maintenance as of this point.



Caution:

If you call transaction `SU25` and there are already values for date/time and user entered under **Point 1**, filling the table again would delete the changes that you have made and overwrite them with the SAP values.

For a full description of the functions of “`SU25`”, choose the *Information about this transaction* button.

Adjusting Authorization Default Status

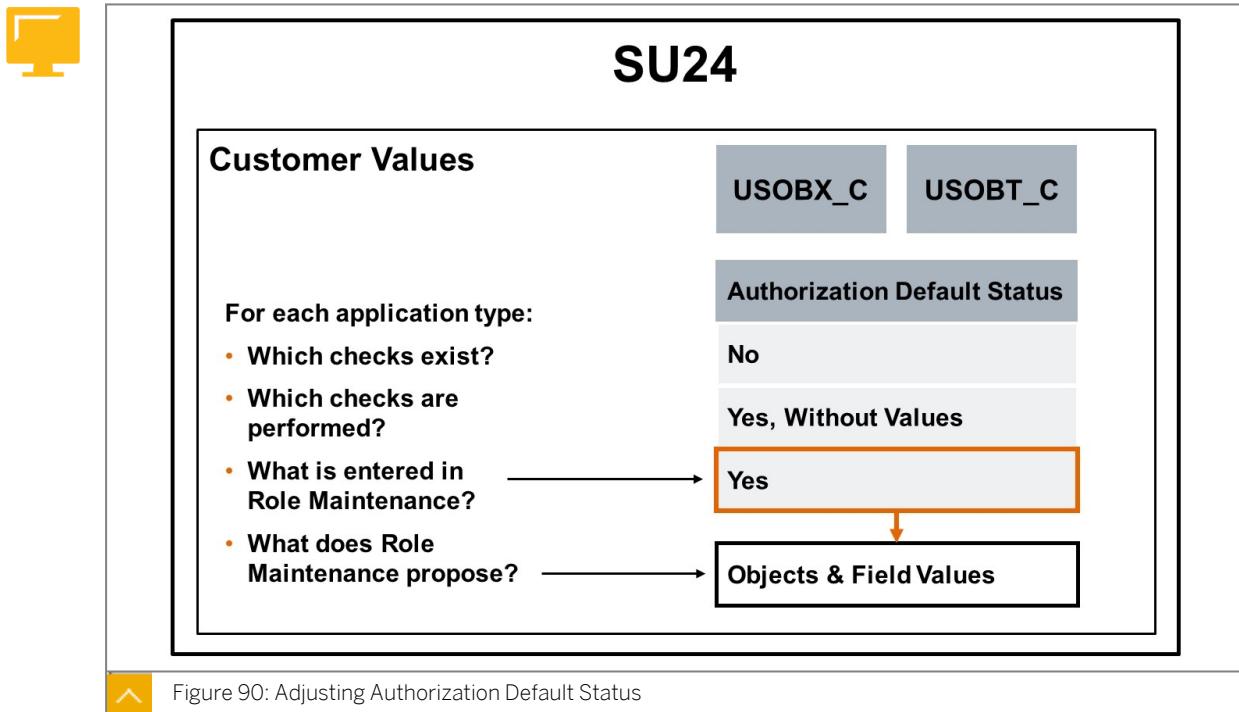


Figure 90: Adjusting Authorization Default Status

After the customer tables *USOBX_C* and *USOBT_C* have been filled, you can maintain them to adjust the behavior of Role Maintenance and the authorization checks to be performed for each transaction. The tables are maintained in transaction *SU24*.

This transaction displays the authorization default values of a transaction.



Note:

As of SAP NetWeaver 2004s, the check status (check or do not check) is separated from the default authorization status. The display and maintenance options in transaction *SU24* have been modified accordingly.

The behavior of objects is governed by the maintenance status of the authorization object and the check indicator.

1. Authorization Default Status

Possible values for the authorization default status are as follows.

Authorization Default Status:

- Yes

By setting this default status, developers inform administrators that the user requires an authorization for this object to execute the core functionality of the application.

If this application is added to a role, the Profile Generator adds an authorization for this object in the role. The fields of the authorizations are predefined with the proposed values.

- Yes, Without Values

By setting this default status, developers inform administrators that the user requires an authorization for this object to execute the core functionality of the application. However, the developers cannot specify any values, since these are only determined in the customer system.

If the administrator adds the application to a role, the Profile Generator places an empty authorization for this object in the role.

- **No**

By setting this authorization default status, developers inform administrators that a user does not require an authorization for this object to execute the core functionality of this application.

If this application is added to a role, the Profile Generator does not place an authorization for this object in the role.



Hint:

To edit the preset check indicators and default values (in SU24), you need the authorization object S_DEVELOP with the following values:

- ACTVT: 03 (Display) or 02 (Change)
- DEVCLASS: Any
- OBJTYPE:
 - SUSK (assignment of transaction to authorization object in customer systems)
 - SUST (assignment of transaction to authorization object in SAP systems)
- OBJNAME: Name of the transaction
- P_GROUP: Any

2. Check Indicator

The following check indicator values are supported.

Check Indicator

- **Check**

Default check indicator.

The appropriate authorization object is always checked.

- **Do Not Check**

The authorization check for this authorization object is deactivated. The system does not check whether the user has a suitable authorization.

This indicator cannot be chosen for HR and Basis authorization objects.



Caution:
Authorization check is suppressed during runtime.

3. Maintenance status of authorization object

The maintenance status of an authorization object indicates whether authorization default data has been maintained correctly for the object.

Possible values are

- 'Maintained' (green icon) - *Default status* (and any authorization field values) have been maintained completely.
- 'Not maintained' (red icon) - The authorization default status has not yet been maintained or another priority 1 error has occurred.
- 'Maintained with warning' (yellow icon) - Authorization field values have not been maintained correctly for the object; a priority 2 (or lower) warning exists.
- 'Do not check' (gray icon) - The authorization check has been disabled for the object (*Check Indicator* is set to "Do not check").



Caution:
If you change the field values, these are distributed by Role Maintenance as new defaults during role maintenance. This affects all roles for which the affected transaction is in the menu, and the authorization values are read again (*Read old status and merge with new data*).

This is the case regardless of whether the change in the role is for this transaction or a different transaction.



Hint:

In the SAP Standard, there is currently no restore function for the data of the SU24. For a smaller volume, you can manually reset the changes to the data of the change document (the data basis is in accordance with report SU2X_SHOW_HISTORY or it can be taken from the tables USOBT_CD and USOBX_CD).

If the data of the SU24 seems to be inconsistent in your system, you can analyze the data and repair it using the report SU24_AUTO_REPAIR. This report automatically detects and repairs inconsistencies that have a negative influence to the PFCG or the upgrade post-processing steps (transaction SU25).

For details about these reports, see SAP note 1539556 - Administration of authorization default values.

Upgrading Role Maintenance

After an upgrade, transactions that were selected in the menu of existing roles can be protected using additional authorization objects in the target release. This means that tables USOBT_C and USOBX_C have to be updated as well as the existing roles.

The authorization checks added in the target release require that tables *USOBX_C* and *USOBT_C* as well as the roles created in the source release be updated to the latest version. To do this, you can use the transaction SU25, step *Postprocess of Settings After Upgrading to Higher Release*.

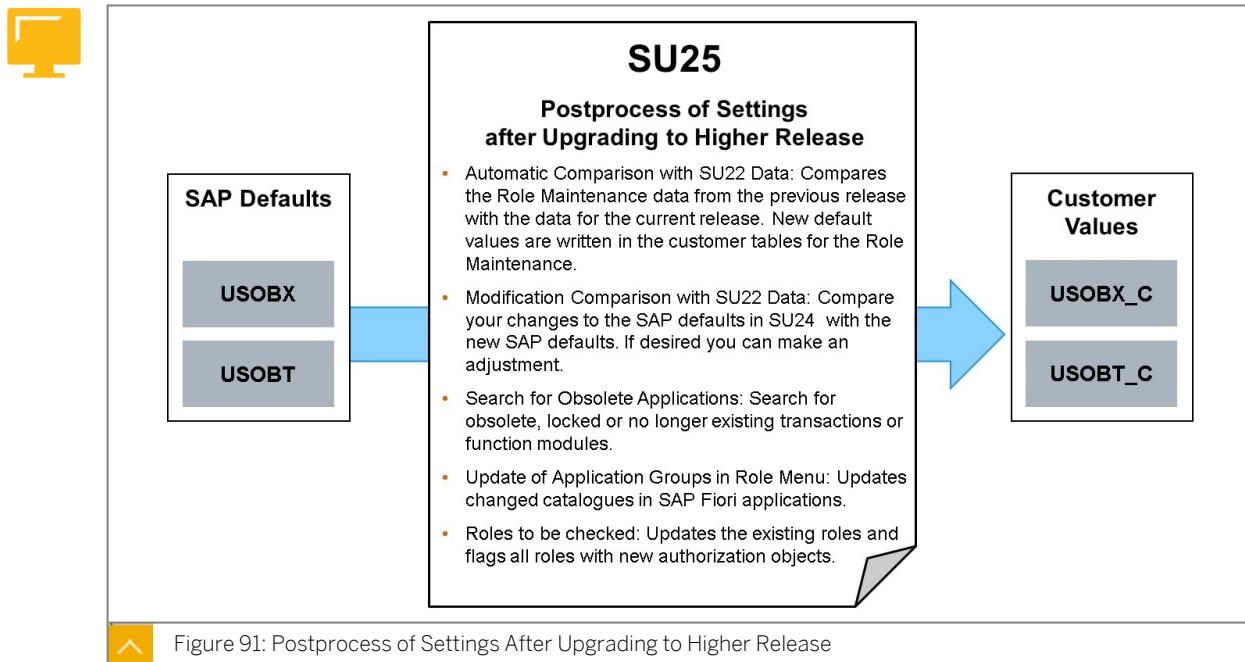


Figure 91: Postprocess of Settings After Upgrading to Higher Release



Caution:

When executing transaction SU25, you should keep in mind that the customer may have changed table *USOBX_C* or *USOBT_C* in the source release. The step *Installing the Profile Generator* in transaction SU25 **may not** be executed for this reason as it would completely overwrite the tables.

Consequently, a comparison procedure is required, which is performed using the step *Postprocess the Settings After Upgrading to a Higher Release*.

Automatic Comparison with SU22 Data

This compares Role Maintenance data from the previous release with the data for the current release. New default values are written in the customer tables for Role Maintenance. You only need to perform a manual adjustment later (in step 2B) for transactions in which you changed the settings for authorization default values. You can also display a list of the roles to be checked (step 2C).

Modification Comparison with SU22 Data

If you have made changes to the authorization values in transaction SU24, you can compare these with the new SAP defaults. You can see the values delivered by SAP and the values that you changed next to each other, and you can make an adjustment, if desired. You can assign the authorization default values by double-clicking the relevant line.

Search for Obsolete Applications

This step searches for obsolete, locked, or no-longer-existing transactions or function modules so you are able to adapt PFCG roles for correct authorization in the new SAP release.

Update of Application Groups in Role Menu

You have inserted application groups (for example, SAP Fiori tile catalogs) into the menu of roles. The applications contained in the application groups were also included in the role menu as sub nodes of the groups. If you add applications to a group or delete applications from a group, you must update the role menu.

Roles to be Checked

This step guides you through all the roles that are affected by newly-added authorization checks and that have to be changed to correspond. You can jump directly to Role Maintenance.



Hint:

Steps *Automatic Comparison with SU22 Data* and *Modification Comparison with SU22 Data* make changes to the customer tables of Role Maintenance. If you want to transport these changes, choose step *Transport of Customer Tables* in transaction SU25.

New Functionality in SU25: Deactivating Merge Mode in Step “Roles to be Checked”

Transaction SU25 is required after an upgrade to update the customer-specific authorization default values and roles. Step *Roles to be Checked* provides a list of roles which are affected by the newly added or changed authorization default values. The roles that authorization data must be merged with get the "Profile comparison required" status (merge mode) and are marked with red traffic lights. The merge mode triggers an automatic merging when we go into Role Maintenance in transaction PFCG. This automatic merging is often undesired because role administrators may want to display the original authorization data first before the merge process.

With the new functionality in Step *Roles to be Checked*, you can now select a set of roles that have a red status and deactivate the merge mode using function key F7. All the roles that you process in this manner get a new yellow status. When you now navigate back to transaction PFCG, the system no longer merges the roles automatically, but displays the relevant authorization data. To take advantage of this new feature, import the relevant Support Package, see SAP Note 1417883.

As long as one role has a yellow status, the function key F8 can be used to reactivate the merge mode. You can change between the active and inactive mode as many times as required. Whenever step *Roles to be Checked* is called again, roles with an inactive merge mode are automatically transferred to active mode.

Additional information related to this new function enhancement:

- Meaning of the Statuses

The role statuses in Step *Roles to be Checked* are not identical to the authorization statuses of roles in the Authorizations of Role Maintenance. Step *Roles to be Checked* refers only to whether or not the authorization data should or can be merged. The status of the related authorization profiles in PFCG is irrelevant. The exact status definitions are as follows:

- Red: The authorization data must and can be merged (merge mode is active).
 - Yellow: The authorization data must be merged, but this is not possible (merge mode is inactive)
 - Green: The authorization data has already been merged.
- Role Lock

During a status change, the roles are temporarily locked. Roles that cannot be locked remain in their old status.
 - Roles that Have a Green Status

For roles which the authorization data has already been merged, you can never change the status. Selecting these roles does not have any effect. Once you have transferred all the roles in the list to green status by merging the authorization data, you do not have to perform any further activities in step *Roles to be Checked*. As a result, the functions for changing the merge mode and the selection functions are not available.

Generate Standard Role SAP_NEW

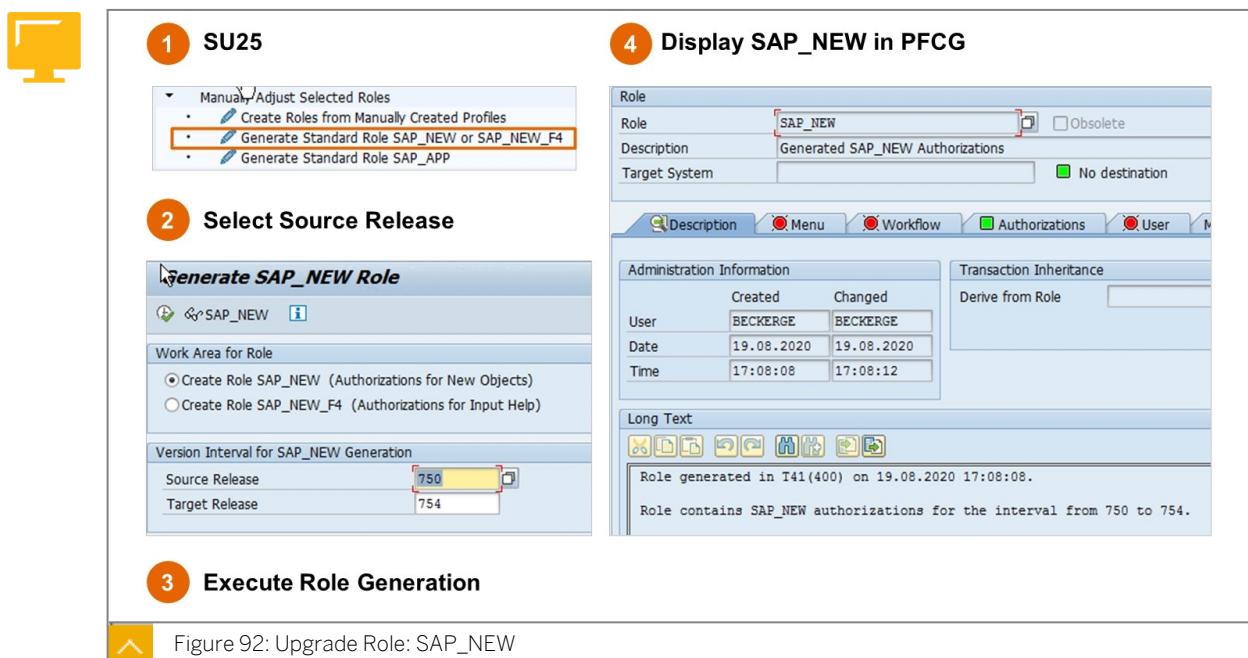


Figure 92: Upgrade Role: SAP_NEW

If you use a very large number of roles, it can be useful for reasons of time, to do without the postprocessing initially, and to assign the role SAP_NEW to the users manually. The role SAP_NEW is used to bridge the differences in releases in the case of new or changed authorization checks for existing functions, so that your users can continue to work as normal.

The role SAP_NEW must be generated in accordance with the system environment in transaction SU25 *Manually Adjust Selected Roles* → *Generate Standard Role SAP_NE or SAP_NEW_F4* or using the report **REGENERATE_SAP_NEW**.

After generation, the role SAP_NEW contains authorizations for all new checks in existing transactions.

The role SAP_NEW guarantees backward compatibility of the authorizations if a new release or an update or authorization checks introduce checks for previously unprotected functions.

**Caution:**

This role contains very extensive authorizations, since, for example, organizational levels are assigned with the full authorization asterisk ("*").

Once you have included the new authorization checks in your authorization concept, delete the role SAP_NEW from each of the corresponding master records. Do not wait until you have finished processing everything, but do it immediately, "user for user", to avoid retaining authorizations that are too extensive.

**Hint:**

In older SAP releases, where the report GENERATE_SAP_NEW is not available, you still require the profile SAP_NEW. Therefore, you must use transaction SU02 for the profile administration and to assign the SAP_NEW profile to the users manually.

This composite profile contains very extensive authorizations, since, for example, organizational levels are assigned with the full authorization asterisk ("*").

Either temporarily assign the previously adjusted composite profile SAP_NEW or the relevant single profiles contained in it, SAP_NEW_“Release”. You require all single profiles between the old release and the new release.

**Note:**

The role SAP_NEW_F4 contains the full authorization for all objects with the field ACTVT and the fixed value F4 and further directly registered objects. This role is not part of XPRA and should, in general, only be used if required.

Workbench for Switchable Authorization Scenarios

A central switchable authorization check is needed for different application scenarios and as a requirement for security-relevant corrections to the authorization concept.

If SAP delivers new authorization checks in already established business processes via corrections delivered in a Note or Support Package, these checks should be available in the customer's landscape, but they should not affect production processes. You can identify new authorization checks with scenario names in the delivered code. A scenario groups together the new or changed authorization checks of a business process. The switchable authorization scenario construct is a simple way of introducing tighter security requirements scenario-by-scenario, according to customer requirements. The cross-application solution of switchable authorization checking creates the necessary transparency about the degree of conversion of tighter authorization concepts.

For details on this Switchable Authorization Scenarios, refer to SAP notes 1908870 - SACF: Workbench for switchable authorization scenarios and 1922808 - SACF: FAQ - Supplementary application information.

Unit 5

Exercise 8

Practice System Exercise: Maintain Authorization Default Values

Business Example

This exercise reinforces the topics of default values for Role Maintenance, proposal values, and the steps to perform after an upgrade.

Task 1: Display the Authorization Default Values

Display the authorization default values for transaction FD03.

1. Start the *Maintain Authorization Default Values* transaction (SU24).
2. Display the authorization default values for transaction FD03 and check the following:
Are there any authorization objects with the default status
 - Yes
 - Yes, *Without Values*
 - No

To which authorization objects is the default status “Yes” assigned?

Result

There are authorization objects with the default status Yes and Yes, *Without Values* shown.

The default status “Yes” is assigned to the following authorization objects:

- B_BUPA_RLT
- F_KNA1_APP
- F_KNA1_BED
- F_KNA1_BUK
- F_KNA1_GEN
- F_KNA1_GRP
- F_MANDATE

3. Which default values are assigned to the authorization fields of the authorization object *F_KNA1_APP* → ?

Fill in the following table.

Object	Field	Value (Interval)
F_KNA1_BUK		

Object	Field	Value (Interval)

4. To which authorization objects is the default status “No” assigned?

Task 2: Compare the Automatically Entered Authorizations in a Role with Authorization Default Values

Create a role GR##_FI_FD03 and compare the automatically entered authorizations with the authorization default values from the previous task.

1. Start the role maintenance transaction and create the predefined role. Enter a short description, and save.
2. Add the transaction FD03 to the role menu.
3. Go to the Authorizations tab page and define the organizational levels.

Define the organizational level:

- Organizational level: Company Code= 1010

Why do you have to enter an authorization value for the company code?

4. Answer the following questions.

For which authorization objects did the system automatically generate authorizations?

Why is the status of the authorization objects F_KNA1_APP, F_KNA1_BUK, and F_KNA1_GEN set to Standard and why is the traffic light symbol status set to green?

Result

The system automatically generates authorizations for the following authorization objects:

Green light:

- S_TCODE
- F_KNA1_APP
- F_KNA1_BUK
- F_KNA1_GEN

Yellow light:

- B_BUPA_RLT
- F_BNKA_MAN
- F_BNKA_MAO
- F_KNA1_AEN
- F_KNA1_BED
- F_KNA1_GRP
- F_MANDATE

The status of the authorization objects F_KNA1_APP, F_KNA1_BUK, and F_KNA1_GEN are set to *Standard* and why is the traffic light symbol status set to *green*.

All fields of the authorization objects F_KNA1_APP and F_KNA1_GEN could be filled with default values.

The organization level field of F_KNA1_BUK is interpreted as an authorization default value.

5. Maintain Authorizations - Set all open authorization values to full authorization (top set of traffic lights).
6. Maintain Authorizations - Generate the authorization profile for your role.

Practice System Exercise: Maintain Authorization Default Values

Business Example

This exercise reinforces the topics of default values for Role Maintenance, proposal values, and the steps to perform after an upgrade.

Task 1: Display the Authorization Default Values

Display the authorization default values for transaction FD03.

1. Start the *Maintain Authorization Default Values* transaction (SU24).
 - a) In the OK code field, enter transaction code SU24.



Note:

You can also start the *Maintain Authorization Default Values* transaction in the SAP Reference Implementation Guide (SPRO):

- SAP Menu: Tools → Customizing → IMG → Execute Project, (transaction code: SPRO).
- IMG path: SAP Customizing Implementation Guide → SAP NetWeaver → Application Server → System Administration → Users and Authorizations → Maintain Authorizations and Profiles Using Profile Generator → Work on SAP Check Indicators and Field Values.
- Choose Change Check Indicators.

2. Display the authorization default values for transaction FD03 and check the following:

Are there any authorization objects with the default status

- Yes
- Yes, *Without Values*
- No

To which authorization objects is the default status "Yes" assigned?

- a) Enter FD03 in the *Transaction Code* field.
- b) Choose *Execute (F8)*.

Result

There are authorization objects with the default status Yes and Yes, *Without Values* shown.

The default status “Yes” is assigned to the following authorization objects:

- B_BUPA_RLT
- F_KNA1_APP
- F_KNA1_BED
- F_KNA1_BUK
- F_KNA1_GEN
- F_KNA1_GRP
- F_MANDATE

3. Which default values are assigned to the authorization fields of the authorization object *F_KNA1_APP* → ?

Fill in the following table.

Object	Field	Value (Interval)
F_KNA1_BUK		

- a) The authorization default values are listed in the *Authorization Default Values* area.
 b) Check the entries in the line with authorization object *F_KNA1_APP*.

Object	Field	Value (Interval)
F_KNA1_APP	ACTVT	03
	ACTVT	C2
	APPKZ	F

- c) Choose *Back (F3)* to return to the initial screen of the *Maintain Authorization Default Values* transaction.
 4. To which authorization objects is the default status “No” assigned?

- a) Choose the *Complete Object List* icon.

There are further authorization objects with the default status No shown.

Task 2: Compare the Automatically Entered Authorizations in a Role with Authorization Default Values

Create a role GR##_FI_FD03 and compare the automatically entered authorizations with the authorization default values from the previous task.

1. Start the role maintenance transaction and create the predefined role. Enter a short description, and save.
 - a) SAP Menu:
Tools → Administration → User Maintenance → Role Administration → Roles (transaction code PFCG).
 - b) Enter the name for the role **GR##_FI_FD03** in the *Role* field.

- c) Choose *Create Single Role*.
 - d) Enter description **Check authorization default values** in the *Description* field.
 - e) Then choose *Save (Ctrl+S)* to save your role.
2. Add the transaction **FD03** to the role menu.
- a) Go to the *Menu* tab page.
 - b) Choose the *Transaction* button and enter the following transaction code in the *Transaction code* field:
- FD03
 - c) Choose *Assign Transactions*.
 - d) Then choose *Save (Ctrl+S)* to save your role.
3. Go to the *Authorizations* tab page and define the organizational levels.
Define the organizational level:
- Organizational level: *Company Code= 1010*
Why do you have to enter an authorization value for the company code?
-
- a) Go to the *Authorizations* tab page.
 - b) Choose *Change Authorization Data*.
 - c) Enter the following values in the *Define Organizational Levels* window:
- *Company code: 1010*,
 - d) Why do you have to enter an authorization value for the company code?
The field *company code* has been created as an organizational level.
 - e) Choose *Save (Ctrl+S)* to save the authorization values for the organizational levels.

4. Answer the following questions.

For which authorization objects did the system automatically generate authorizations?

Why is the status of the authorization objects **F_KNA1_APP**, **F_KNA1_BUK**, and **F_KNA1_GEN** set to *Standard* and why is the traffic light symbol status set to *green*?

- a) Expand *Object Class AABB* and *Object Class FI*.

Result

The system automatically generates authorizations for the following authorization objects:

Green light:

- S_TCODE
- F_KNA1_APP
- F_KNA1_BUK
- F_KNA1_GEN

Yellow light:

- B_BUPA_RLT
- F_BNKA_MAN
- F_BNKA_MAO
- F_KNA1_AEN
- F_KNA1_BED
- F_KNA1_GRP
- F_MANDATE

The status of the authorization objects F_KNA1_APP, F_KNA1_BUK, and F_KNA1_GEN are set to *Standard* and why is the traffic light symbol status set to *green*.

All fields of the authorization objects F_KNA1_APP and F_KNA1_GEN could be filled with default values.

The organization level field of F_KNA1_BUK is interpreted as an authorization default value.

5. Maintain Authorizations - Set all open authorization values to full authorization (top set of traffic lights).
 - a) Choose the *Status* button.
 - b) Choose *Execute (Enter)* in the *Assign Full Authorization of Subtree* window.
6. Maintain Authorizations - Generate the authorization profile for your role.
 - a) Choose the *Generate* icon.
 - b) In the *Assign Profile Name for Generated Authorization Profile* window, accept the proposed profile name and choose *Execute (Enter)*.
 - c) Choose *Back (F3)* to return to the *Change Roles* screen.



LESSON SUMMARY

You should now be able to:

- Manage installation and upgrade tasks in SAP Business Role Maintenance.

Maintaining Access Control and User Administration

LESSON OVERVIEW

This lesson provides an overview of the password rules and special users, and introduces scenarios for user and authorization administration. The authorization objects that are used in transactions SU01 and PFCG are very important for the principles of dual and treble control. This lesson will describe how these and other frequently used objects are used.

Business Example

In order to protect your SAP system against unauthorized access, you must define password rules, set the relevant profile parameters and change the initial passwords of the special users.

In addition to these parameters, there are general authorization objects, which must often be specified. These are also introduced in this context.

You must also define areas of responsibility for user and authorization administration. The organizational areas of responsibility must be clearly defined technically using authorizations. The principle of dual or treble control can be created.



LESSON OBJECTIVES

After completing this lesson, you will be able to:

- Manage access control configuration.

Profile Parameters and Password Rules for User Logon

The following slides show you the most important settings, and the profile parameters with which you can control password and logon rules. Control using these values should protect your system against any type of misuse by users.

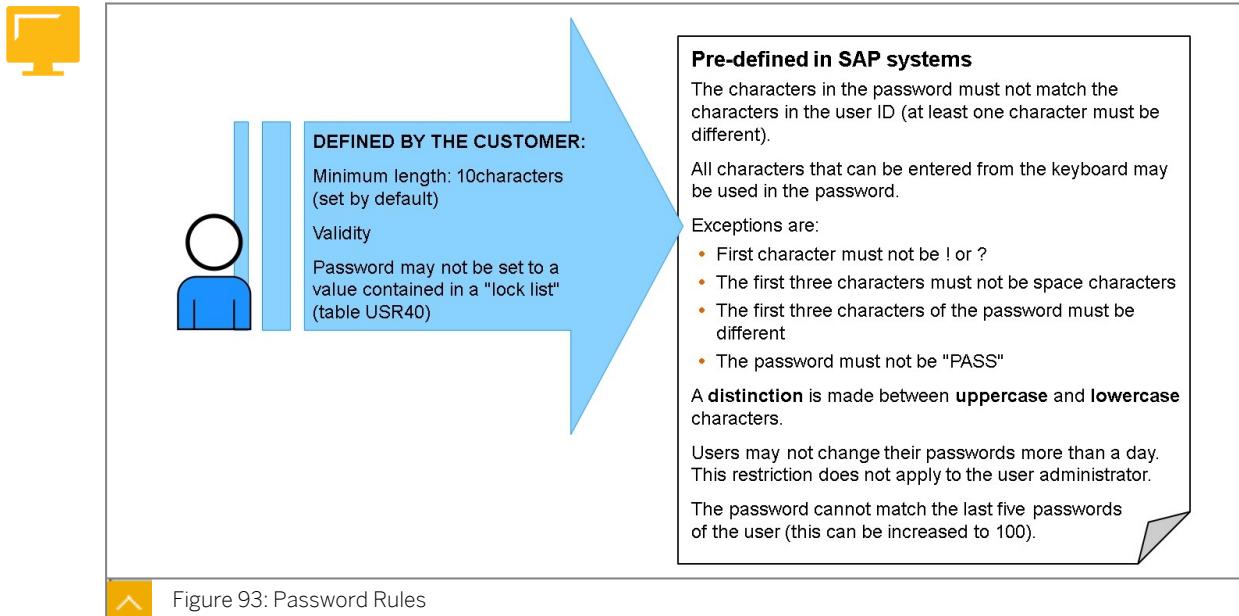


Figure 93: Password Rules

There are two ways in which you can control the choice of user passwords:

- You can use the system profile parameters to assign a minimum length for passwords and define how often users must set new passwords.
- Invalid passwords can be entered in the table of reserved passwords, *USR40*. This table is maintained with transaction *SM30*. The entries can also be made generically:
 - "?" denotes a single character
 - "*" denotes a character string

Example:

- If you enter "123*" in table *USR40*, passwords may not begin with the character string "123*".
- If you define "*ABC*", passwords cannot contain the character string "ABC" in any position.

There are general rules for passwords that cannot be deactivated. A password:

- Must be at least six characters long (by default)
- Must not begin with "?" or "!"
- Must not be "pass"
- The new password must differ from the old one by at least one character



Hint:

The setting that determines if users must create a new password that differs from the previous five passwords they have entered is no longer mandatory. You can use the *login/password_history_size* parameter to set the history from between 1 and 100. The proposed standard value remains 5.

There are also a number of predefined password rules, which are shown on the next slide.



System Profile Parameters	Default	Value Range
Minimum password length <i>login/min_password_lng</i>	10*	1-40 chars
Validity period for passwords <i>login/password_expiration_time</i>	0	0-1000 days
Validity period for unused initial passwords <i>login/password_max_idle_initial</i>	0	0-24000 days
Validity period for unused user passwords <i>login/password_max_idle_productive</i>	0	0-24000 days
Minimum difference in password characters <i>login/min_password_diff</i>	1	1-40 chars

Figure 94: Password Checks with System Profile Parameters (1)

There are now around 30 profile parameters in the SAP system that start with “login”. Due to the large number of parameters, only a few have been listed here as examples. For more information, see the parameter descriptions (for transaction RZ11) or the online documentation.

login/min_password_lng

You can set the minimum length for passwords with the parameter *login/min_password_lng*. By default, the password must be at least “6” and no more than “40” characters long. The parameters *login/min_password_digits*, *login/min_password_letters*, *login/min_password_lowercase*, *login/min_password_uppercase*, and *login/min_password_specials* specify the minimum number of **digits**, **letters (number of upper and lower case)** or **special characters** that a password must contain. The value range is 1 to 40.

login/password_expiration_time

The parameter *login/password_expiration_time* specifies the number of days after which a user must set a new password. If the parameter is set to 0, the user does not need to change his or her password.

login/password_max_idle_initial

The parameter *login/password_max_idle_initial* indicates the maximum length of time during which an initial password (a password selected by the user administrator) remains valid if it is not used. Once this period has expired, the password can no longer be used for authentication. The user administrator can reactivate the password logon by assigning a new initial password.

login/password_max_idle_productive

This parameter indicates the maximum length of time a productive password (a password chosen by the user) remains valid when it is not used. Once this period has expired, the password can no longer be used for authentication. The user administrator can reactivate the password logon by assigning a new initial password.

login/min_password_diff

With the parameter *login/min_password_diff*, the administrator can determine the number of different characters a new password must possess in comparison with the old

one when users change their passwords. This parameter does not take effect when a new user is created or passwords are reset (==> initial password).



System Profile Parameters		Default	Value Range
	End the logon procedure <i>login/fails_to_session_end</i>	3	1-99
	Maximum number of failed logon attempts <i>login/fails_to_user_lock</i>	5*	1-99
	Deactivation of automatic unlocking <i>login/failed_user_auto_unlock</i>	0*	0-1
	Deactivation of multiple dialog logon <i>login/disable_multi_gui_login</i>	0	0-1
	Special users (multiple logon) <i>login/multi_login_users</i>	Alphanumeric	

Figure 95: Password Checks with System Profile Parameters (2)

login/fails_to_session_end

You can set the number of failed logon attempts after which SAP GUI is terminated using the parameter *login/fails_to_session_end*. If the user wants to try again, he or she must restart SAP GUI.

login/fails_to_user_lock

You can set the number of failed logon attempts after which a user is locked in the SAP system using the parameter *login/fails_to_user_lock*. An entry is written in the system log at the same time. The failed logon counter is reset after a successful logon attempt.

login/failed_user_auto_unlock

At midnight (server time), the users that were locked as a result of incorrect logon attempts are **no longer automatically** unlocked by the system (default value since SAP NetWeaver 7.0). You reactivate this automatic unlocking with the parameter *login/failed_user_auto_unlock* = 1.

The administrator can unlock, lock, or assign a new password to users in user maintenance (transaction SU01).

login/disable_multi_gui_login

If the parameter *login/disable_multi_gui_login* is set to 1, a user cannot log on to a client more than once. This can be desirable for system security reasons. This parameter applies to SAP GUI logons. If the parameter is set to 1, the user has the following options when he or she logs on again: "Continue with this logon and end any other logons in the system" or "Terminate this logon". Users to whom this should not apply should be specified in the parameter *login/multi_login_users*, separated with commas, and with no spaces.

The following parameters add a new level of detail to the implementation of the password policy in the SAP system.

login/min_password_lowercase

login/min_password_lowercase: In accordance with the parameter value, the password must contain at least “x” lowercase letters. The default value is “0”.

login/min_password_uppercase

login/min_password_uppercase: The parameter value defines the minimum number of uppercase letters a password must have. The default value is “0”.

login/password_change_waittime

login/password_change_waittime: Users can change their passwords again only after waiting for a specified amount of time. The default value is “1”, which means the user must wait a day to change his or her password again. User administrators, however, can change or reset the password of users as many times in a day as they need.

login/password_charset

login/password_charset: The default value is “1”. This parameter is used only if downward compatible passwords need to be generated. It specifies which characters can be used in the password. All Unicode characters are allowed, by default.

login/password_downwards_compatibility

login/password_downwards_compatibility: The system generates downward compatible password hashes, which correspond to an “8” character long password. Downward compatibility is required for RFC communication with older SAP releases. The default value is “1”.

Special Users



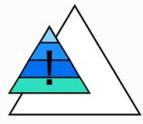
Initial Logon Procedure in SAP Clients				
Client	000	001	066	Client (new)
User	SAP*	DDIC	EarlyWatch	SAP*
Initial Password	Set during installation		support	pass
 Since these users are public information, they must be protected against unauthorized access. You are prompted for SAP* and DDIC during the installation.				

Figure 96: Special Users

Essentially, there are two types of special users: those created by installing the SAP system and those created when you copy clients.

During the installation of the SAP system, client 000 is created. Depending on the SAP system that is installed clients 001 and 066 are created in addition. Special users are predefined in the clients. Since there are standard names and standard passwords for these users, which are known to other people, you must protect them against unauthorized access.

SAP System Special User, SAP*

*SAP** is the only user in the SAP system for which no user master record is required, since it is defined in the system code. *SAP** has, by default, the password “PASS”, and unrestricted access authorizations for the system.

When you install the SAP system, a user master record is automatically created for *SAP** in client 000 (and in 001 if it exists). At first, this still has the initial password “06071992”. The administrator is required to reset the password **during** installation. The installation can continue only after the password has been changed correctly. The master record created here deactivates the special properties of *SAP**, so that only the authorizations and password defined in the user master record now apply.

DDIC User

This user is responsible for maintaining the ABAP Dictionary and the software logistics.

When you install the SAP system, a user master record is automatically created in client 000 [001] for the user *DDIC*. With this user too, you are requested to change the standard password of “19920706” during the installation (similar to the user *SAP**). Certain authorizations are predefined in the system code for the *DDIC* user, meaning that it is, for example, the only user that can log on to the SAP system during the installation of a new release.



Caution:

To protect the system against unauthorized access, SAP recommends that you assign these users to the user group *SUPER* in the client 000 [001]. This user group is only assigned to superusers.

EarlyWatch User

The EarlyWatch user is delivered in client 066 and is protected with the password “*SUPPORT*”. The EarlyWatch experts at SAP work with this user. This user should not be deleted. Change the password. This user should only be used for EarlyWatch functions (monitoring and performance).



Hint:

Special features for the user “*SAP**”

If you copy a client, the user “*SAP**” is always available. This user does not have a user master record, and is programmed into the system code. To protect your system against unauthorized access, you should create a user master record for this special user. Create a “superuser” with full authorization.

If you now delete the user master record “*SAP**”, the initial password “*PASS*” with the following properties becomes valid again:

- The user has full authorization since no authorization checks are made.
- The standard password “*PASS*” cannot be changed.

How can you counter this problem to protect the system against misuse?

- You can deactivate the special properties of *SAP**. To do this, you must set the system profile parameter `login/no_automatic_user_sapstar` to a value greater than zero. If the

parameter is active, SAP* no longer has any special properties. If the user master record SAP* is deleted, the logon with PASS no longer works.

- If you want to reinstate the old behavior of SAP*, you must first reset the parameter and restart the system.

Security Policy and Restricting the Log On of Users

Security Policy

Sometimes users require a different security policy for log on and passwords than the default values. For example, powerful users such as administrators should have passwords with a higher level of protection than standard users. Such users should be forced to change their passwords more often or have more complex rules for their passwords. However, such requirements, if applied widely, can cause an increase in help desk requests if you force standard users to comply with such requirements.

Use this field to choose a security policy for the user. Otherwise, the user uses the standard security policy.

Defining Security Policies

With this procedure, you create security policies with attributes, for which you explicitly do not want to use the default value. For example, you assign a new security policy called Digits, and change, as described below, the standard value for the attribute MIN_PASSWORD_DIGITS from 0 to 4. The new security policy Digits then uses the standard values for all security policy attributes, with the exception of the attribute MIN_PASSWORD_DIGITS. You can, however, also create a security policy without defining attributes. This policy then uses the default values for all security policy attributes.

Procedure:

1. Start the maintenance tool for security policies (transaction SECPOL).
2. In change mode, choose *New Entries*.
3. Enter a name in the *Security Policy* field and a description in the *Short Text* field.
4. Double-click the *Attributes* node.
5. Select the security policy, and double-click the *Attributes* node again. The change view for attributes appears.
6. Choose *New Entries*.
7. In the field *Policy Attribute Name*, enter, for example using the input help, a security policy attribute and, in the *Attribute Value* field, a value.



Hint:

Once you have specified all of the attributes to be changed, you can display the attribute values that actually apply for the policy. To do this, choose the *Effective* button. The system displays both the attributes that you changed and the attributes that have been retained with default values in the security policy.

8. Save your entries.

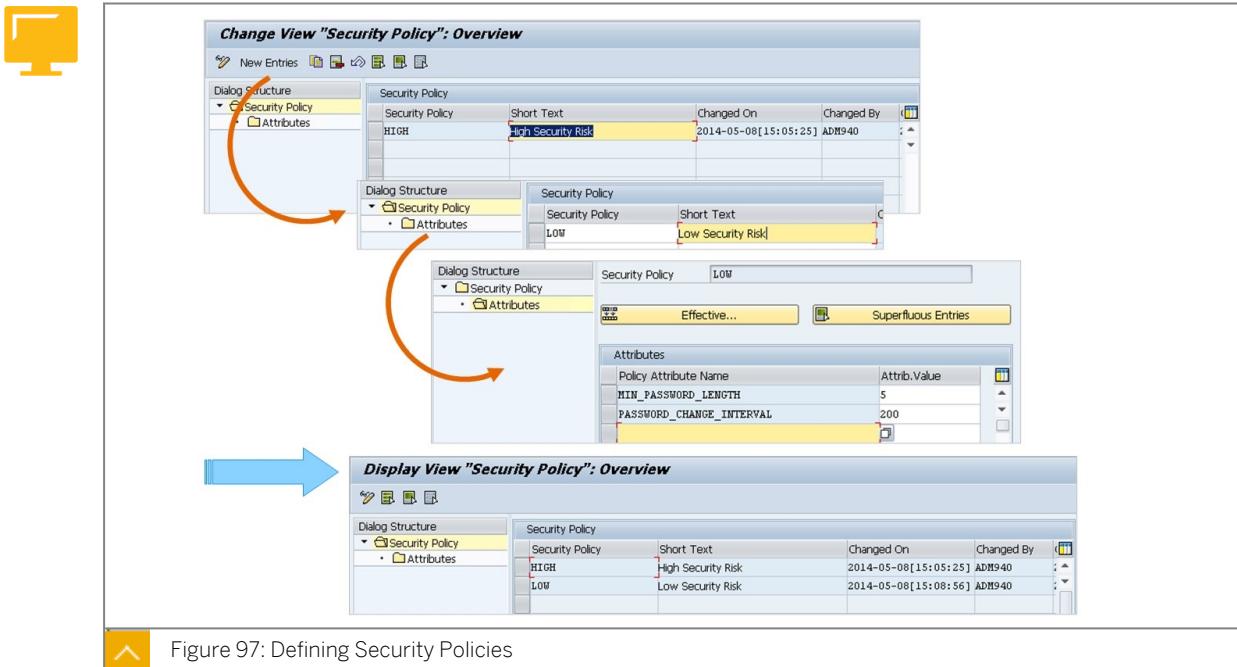


Figure 97: Defining Security Policies

Assigning Security Policies to Users

The security policy could be assigned to a user by using the user maintenance tool (transaction SU01), or assign it to multiple users using mass user maintenance (transaction SU10). On the *Logon Data* tab, enter a security policy for the user, in the *Security Policy* field.

Restricting the Users' Log On While Maintenance Work is Performed in the System

During maintenance work, only certain administrators should be able to log on to the system. The logon of users to the application server could be restricted by setting the new profile parameter *login/server_logon_restriction*.

The following values are possible:

- 0: No restriction.
All users can log on to the application server.
- 1: A logon to the application server is allowed only with special rights.
Only those users whose assigned security policy contains the new attribute SERVER_LOGON_PRIVILEGE with the value 1 can log on to the system. To change the security policy, use transaction SECPOL. Change the relevant security policy that you have assigned only to your administrators. Include the guideline attribute SERVER_LOGON_PRIVILEGE in the security policy and set the value to 1. Users who log on to the system without special rights see the following error message: Server is currently not generally available (restricted logon).
- 2: No logon is allowed to the application server.
Users who log on to the system see the following error message: Server is currently not available (logon not permitted).
- 3: An external logon to the application server is allowed only with special rights.
Only those users whose assigned security policy contains the attribute SERVER_LOGON_PRIVILEGE with the value 1 can log on to the system externally. Users

who try to log on to the system externally without special rights see the following error message: Server is currently not generally available (restricted logon).

- 4: No external logon to the application server is allowed.

Users who try to log on to the system externally without special rights see the following error message: Server is currently not available (logon not permitted).



Hint:

If you set the dynamic profile parameter, no users are logged off the application server. Use transaction RZ10 to save the value permanently. The where-used list in the user information system lets you determine which users have been assigned a security policy or policy attribute. To use it, call transaction SUIM and choose *Where-Used List → Security Policies → In Users*.



Caution:

If you have activated the emergency user, SAP*, then a logon to the system with the SAP* user is always possible. The emergency user is active if the profile parameter *login/no_automatic_user_sapstar* is set to 0 and the SAP* user is not defined in transaction SU01.

Restricting the Logon of Users (*/login/server_logon_restriction*)

Locking Inactive Users

To lock all inactive users, use the report RSUSR_LOCK_USERS with which you can automatically select and lock. On the selection screen of the report RSUSR_LOCK_USERS, select the criteria that you want to apply for locking the user. You have the option to check the result of the selection and display the users that you found or to lock the users immediately. Bear in mind that only a local user lock is set. You can execute the report online and in the background.

Special Authorization Objects

In the area of authorizations, there are a few objects that occur regularly, and are used and specified for daily queries. To clarify their use, some of these objects are described in the following pages.

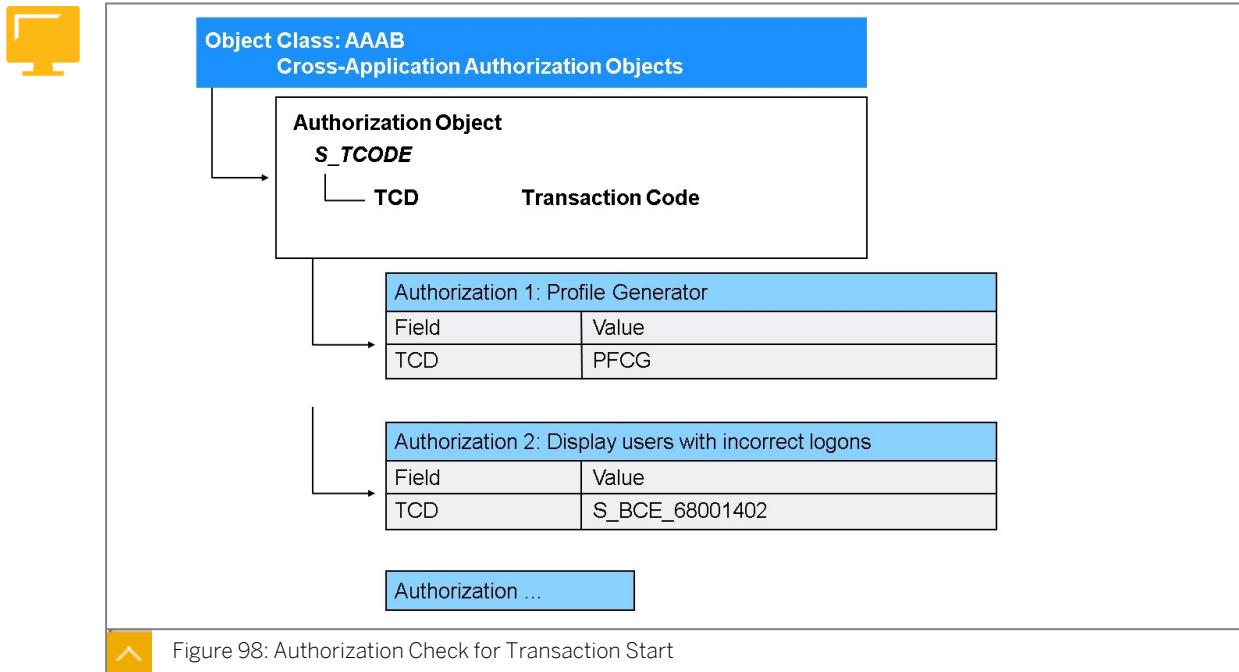


Figure 98: Authorization Check for Transaction Start

**Hint:**

Each time a transaction is started, the kernel always automatically checks the transaction code (TCD) as a value against the authorization object S_TCODE. This also applies for customer-developed transaction codes.

Example:

- *Authorization 1:*

The user calls transaction PFCG (Role Maintenance). He or she can only call Role Maintenance if he/she has authorization for this transaction code.

- *Authorization 2:*

The user calls report "Display users with incorrect logons" from the area menu. Transaction code S_BCE_68001402 is assigned to this report. The user can only execute this report if he or she has authorization for this transaction code.

All the objects of an area menu are checked with authorization object S_TCODE since a transaction code is assigned to each executable menu entry (reports, transactions). This was implemented during the migration of report trees to area menus.

**Hint:**

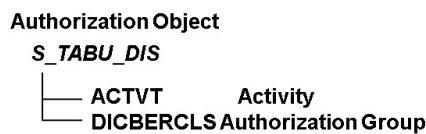
However, there is no rule without exception. Some user/participants know about a backdoor with which this kernel check can be avoided.

If a transaction is called indirectly, that is, from another transaction, no authorization check is performed. This means, for example, that authorizations are not checked, if a transaction calls another with the statement CALL TRANSACTION.

To ensure that the called transactions are also subjected to an authorization check, you must use transaction SE97 to set the check indicator check in tables TCDCOUPLES for the entry of the pair of calling and called transactions (see SAP Note 358122).



Object Class: BC_A
Basis: Administration

**Possible Activities**

- ACTVT:**
- 02 Add, change, or delete table entries
 - 03 Only display table entries

Authorization 1: Maintenance for sales tables

Field	Value
ACTVT	02
DICBERCLS	V*

Authorization 2: Maintenance for materials tables

Field	Value
ACTVT	02
DICBERCLS	M*

Authorization ...

Figure 99: Table Maintenance Authorization for Groups of Tables

Authorization object **S_TABU_DIS** defines which table contents may be maintained by which employees.

The authorization object **S_TABU_DIS** controls only complete accesses, which are made using standard table maintenance (SM31), advanced table maintenance (SM30), or the Data Browser (SE16). These group assignments are defined in table **TDDAT**.

The object consists of the following fields:

- **DICBERCLS:** Authorization group for ABAP Dictionary objects (description - maximum of 4 characters)
- **ACTVT:** Activity (02, 03).

Example:**Authorization 1:**

In this case, table entries may be added, changed or deleted (ACTVT:=02), but only tables/views assigned to authorization group "V*" (DICBERCLS=V*) may be maintained.

SAP standard tables are assigned to authorization groups. These assignments can be changed ("SM30"). **You should consider this carefully, however.** Depending on the setting, some maintenance dialogs could produce data inconsistencies thereafter.

The important tables are:

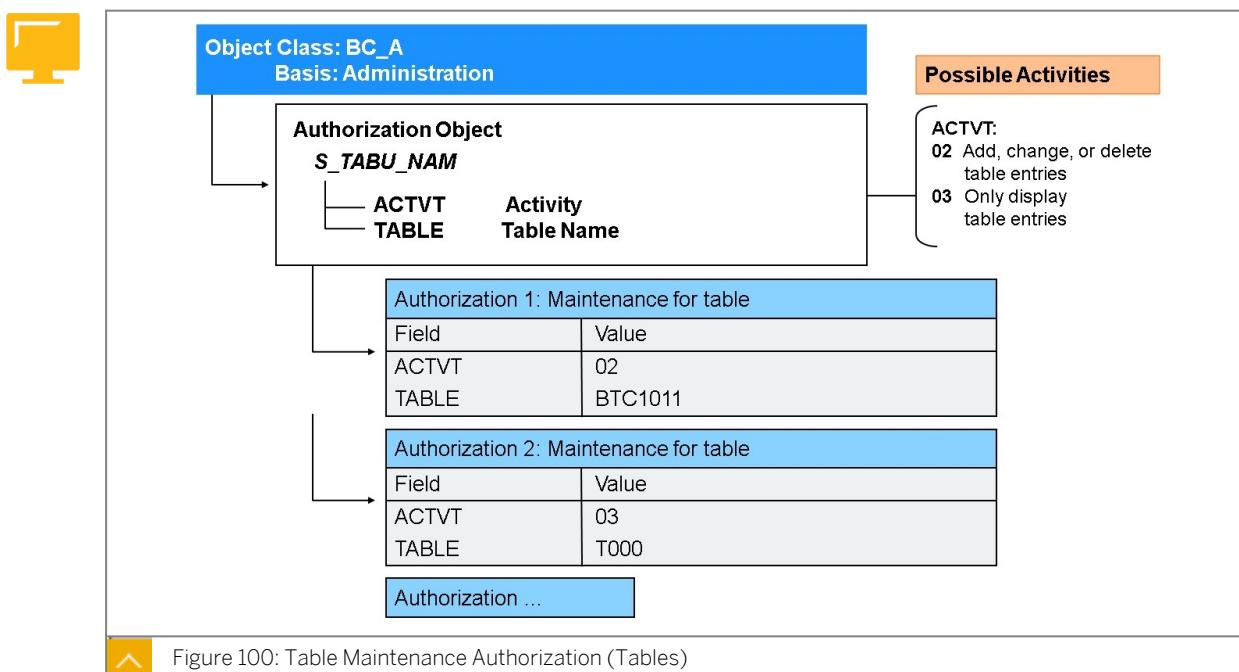
- *V_DDAT_54*: Assignment of authorization group to tables/view.
- *V_BRG_54*: Assignment of authorization groups to tables/views.

The table authorization group of a table or maintenance view can be assigned using transaction *SE11* or *SE54*. The permitted table authorization groups are defined using transaction *SE54* or those defined in the maintenance dialog *V_BRG_54*.

The maximum length of a table authorization group name is only four characters. It is therefore very difficult to represent a meaningful name concept. Using a parameter namespace is not possible.

In addition to the previous maintenance tools for the authorization groups based on the table *TBRG*, a central maintenance environment (transactions *STBRG* and *STBRG_OBJ*) is provided. As well as the ability to define authorization groups independently of the client, these can now also be provided as workbench objects (transport object *SUCU*) across clients. As part of this enhancement, the authorization field for table authorization groups was extended from four to fourteen characters, so that namespace-based authorization groups could be defined and assigned for the authorization object *S_TABU_DIS* as of this maintenance level (see SAP note 1645260 - Enhanced maintenance of table authorization groups).

The authorization concept for generic table access using such standard transactions as *SE16*, *SE17*, *SM30*, *SM31* or *SM34* was previously only bound to the authorization object *S_TABU_DIS*. With SAP note 1481950 - New authorization check for generic table access, the authorization concept was enhanced with the authorization object *S_TABU_NAM* that checks access at the table name level. If a user does not have any *S_TABU_DIS* authorization for a certain table, the system also checks whether the user has an *S_TABU_NAM* authorization. The access is permitted if the user has an *S_TABU_NAM* authorization.



The authorization object *S_TABU_NAM* contains the fields:

- ACTVT: Activity (02, 03).
- TABLE: Name of table or view to be checked

With this object, the system checks the view names or table names directly so that an exact authorization check is possible.



Note:

Authorization check for the display or maintenance of table contents with generic table access tools is performed with the use of function module `VIEW_AUTHORITY_CHECK` for the authorization check.

Function module `VIEW_AUTHORITY_CHECK` checks if the authorization is granted by object `S_TABU_DIS`. If the check for object `S_TABU_DIS` failed, the check is performed for object `S_TABU_NAM`.

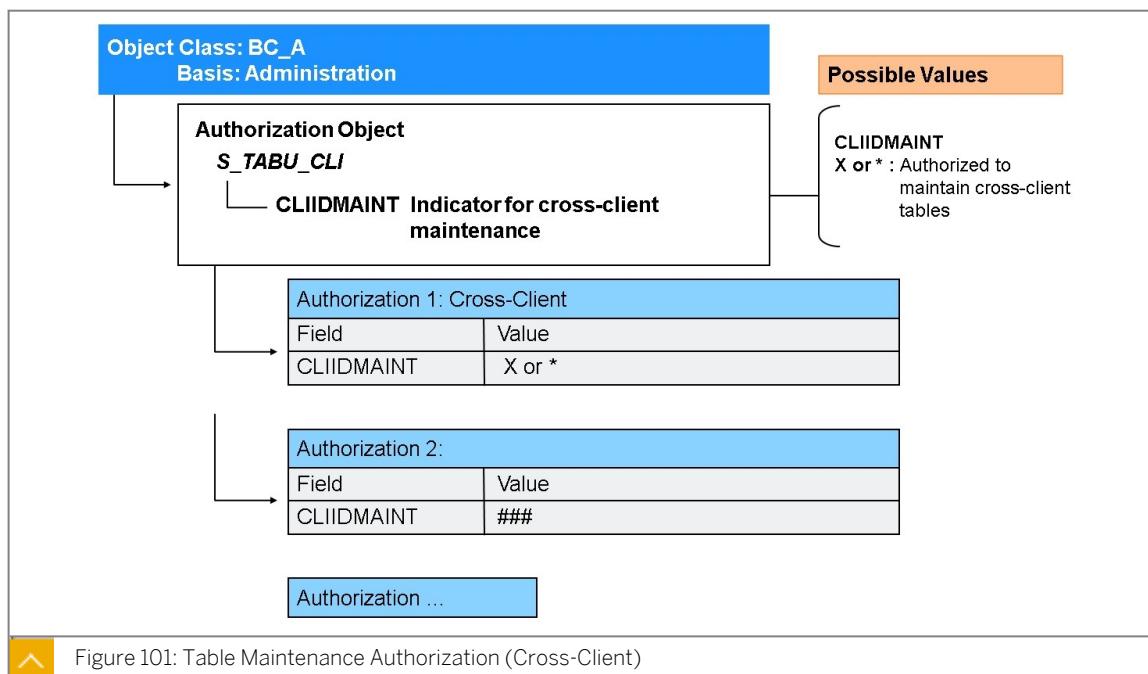
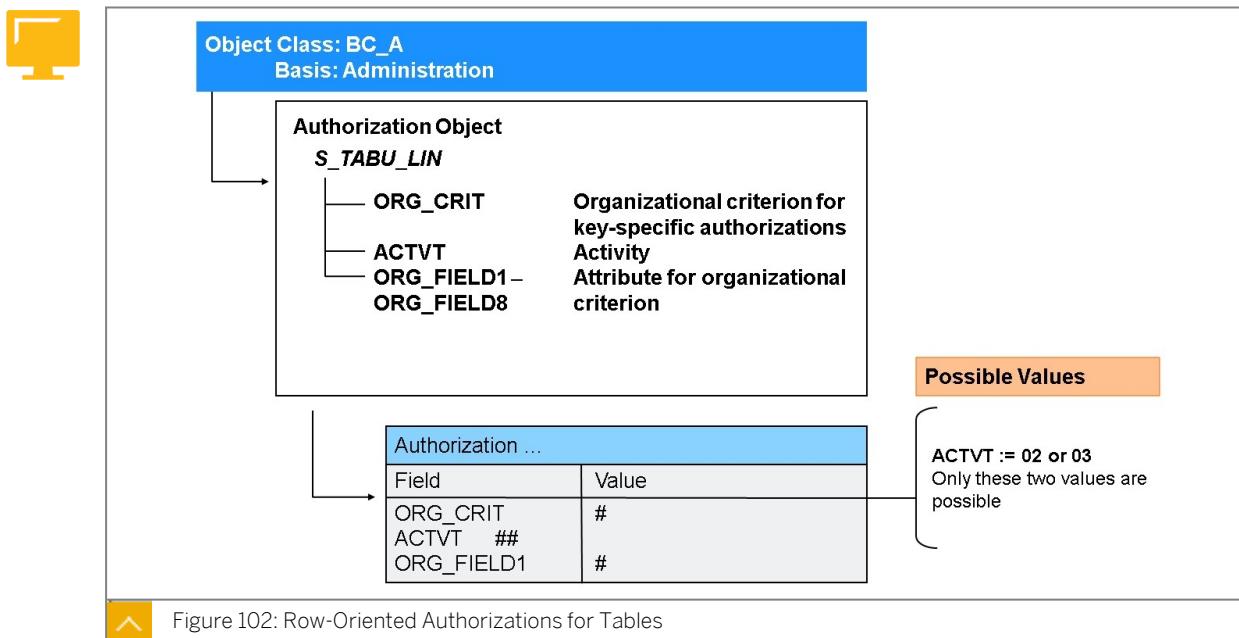


Figure 101: Table Maintenance Authorization (Cross-Client)

Authorization object `S_TABU_CLI`: Grants authorization to maintain cross-client tables with the standard table maintenance transaction (`SM31`), extended table maintenance transaction (`SM31`), and the Data Browser, and also in the Customizing system. It also acts as an additional security measure for cross-client tables and enhances the general table maintenance authorization `S_TABU_DIS`.

The object has the following field:

`CLIIDMAINT`: If identifier “**X**” or “*****” is set, cross-client tables can be maintained.



By introducing organization criteria, you can restrict a user's access rights to specific parts of a table. A possible use for S_TABU_LIN is to display and to change content for only a certain work area, such as a country or a plant.

As you can see in the graphic, the object consists of fields.

Activity:

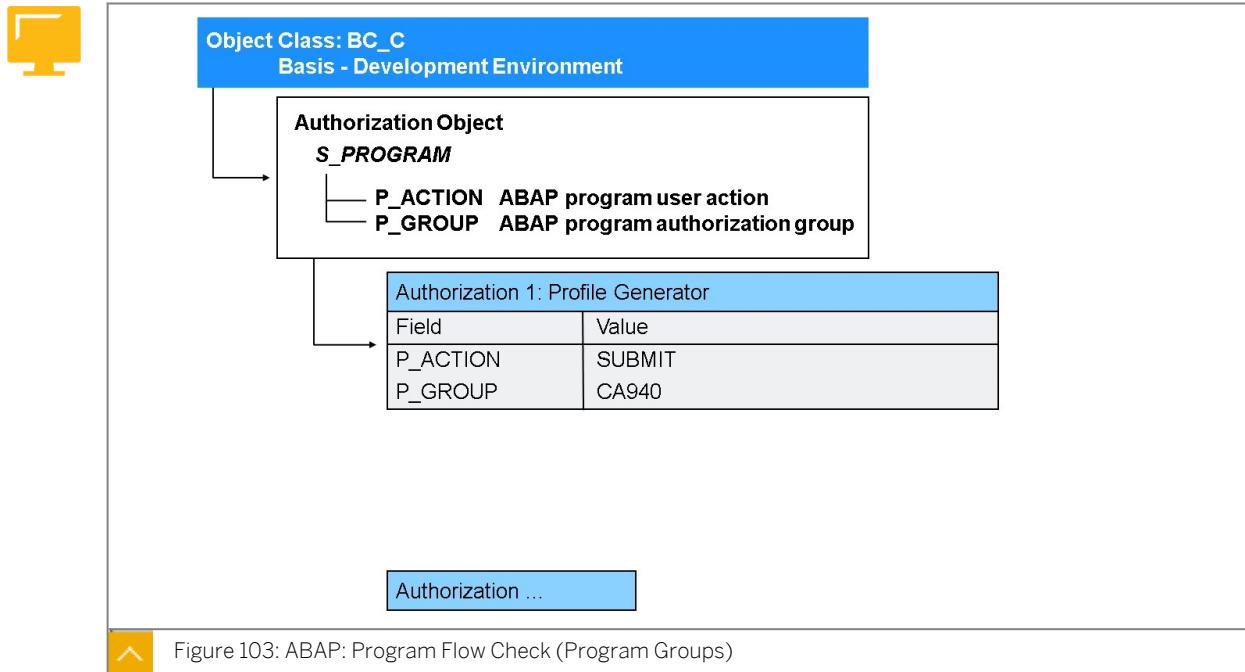
- 02: Add, change, or delete table entries
- 03: Only display table contents.

Organizational Criterion:

Table key fields/row authorization, such as organizational criteria (defined in Customizing)

Attribute for Organizational Criterion:

Attributes 1 to 8 for the organizational criterion; each attribute for a certain table key field.



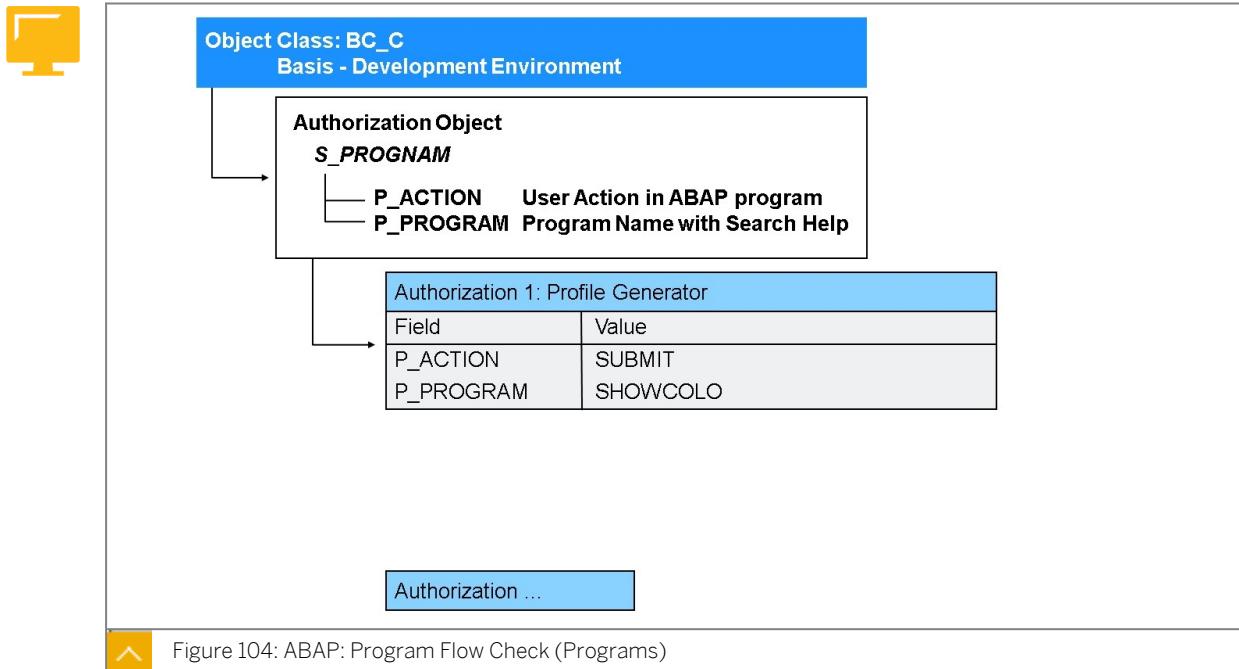
As is familiar from previous releases, it is possible to check programs using the authorization object *S_PROGRAM*.

The programs (reports) are combined into program authorization groups and can be protected against unauthorized access using the groups. The authorization group is stored in the properties of the programs.

You can also store your own authorization groups in SAP programs (without making modifications).

You can assign authorizations for the following activities by program groups:

- Starting a program (*SUBMIT*)
- Scheduling a program as a background job (*BTCSUBMIT*)
- Variant maintenance (*VARIANT*)



The object `S_PROGNAM` is used to supplement the start authorization check for programs. Authorizations for this object are checked exclusively with method `CL_SABE=>AUTH_CHECK_PROGNAM()` in the context of scenarios for switchable authorizations (maintenance transaction `SACF`). The check does not take place with each submit command, but only if it is called explicitly. If the associated scenario is activated, all programs are checked in addition to the existing authorization checks (for example, with authorization groups).



LESSON SUMMARY

You should now be able to:

- Manage access control configuration.

Implementing User and Authorization Management Strategies



LESSON OBJECTIVES

After completing this lesson, you will be able to:

- Implement user and authorization management strategies.

User and Authorization Administration

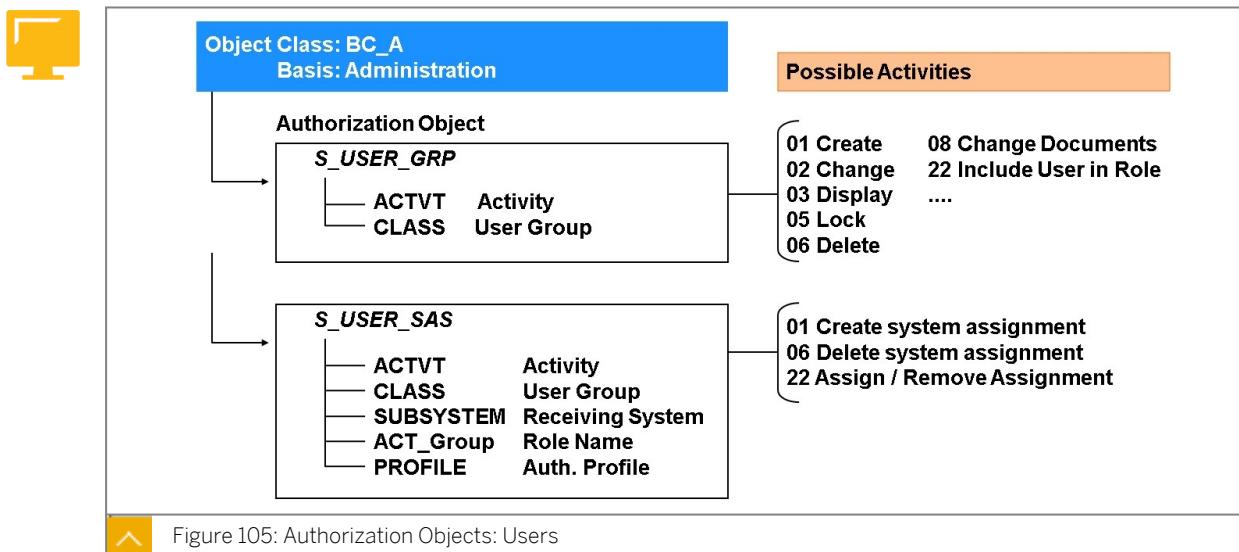
In today's system landscapes, an administrator has many tasks to perform to structure and maintain user master records and roles. These activities should also be subjected to an authorization check and should not all be available to one administrator. You can use the object presented on the following pages to flexibly create a principle of dual or treble control.

Daily Tasks and Activities of an Administrator



- Create, maintain, lock and unlock users, and change passwords
- Create and maintain roles
- Maintain transaction selections and authorization data in roles
- Generate authorization profiles
- Assign roles and profiles
- Transport roles
- Monitor using the Information System
- Archive change documents

The administrator uses the transactions SU01 and PFCG for the activities listed above. When these transaction codes are used, the following objects are checked in the program code.



The object User Master Record Maintenance: User Groups (*S_USER_GRP*) defines the user groups for which an administrator has authorization and the activities that are allowed.

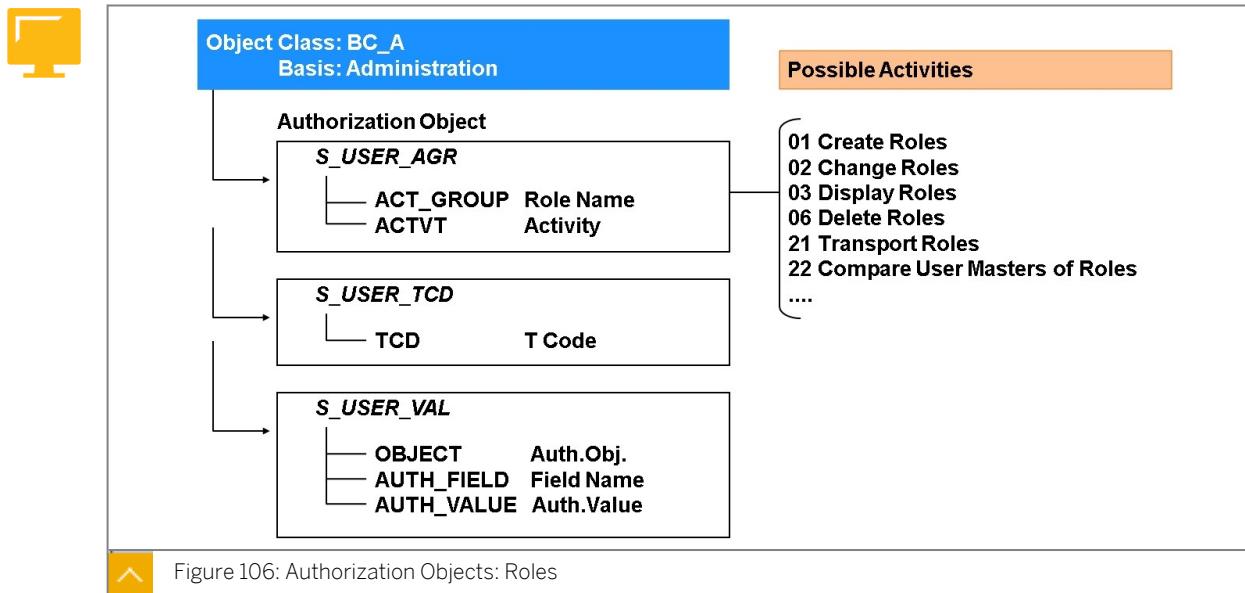
The object *S_USER_GRP* can be used to grant administration rights for only a certain user group in decentralized administration.

Authorization object *S_USER_SAS* is checked in transactions SU01, SU10, PFCG, and PFUD when roles, profiles, and systems are assigned to users. It is a further development of the authorization objects *S_USER_GRP*, *S_USER_AGR*, *S_USER_PRO*, and *S_USER_SYS*, which were previously checked when authorizations were made.

The checking of authorization object *S_USER_SAS* is activated by default and can be deactivated using a Customizing switch. To deactivate, use transaction SM30 to create an entry in table *PRGN_CUST* with the ID **CHECK_S_USER_SAS** and the value **NO**. This means that the authorization objects *S_USER_GRP*, *S_USER_AGR*, *S_USER_PRO*, and *S_USER_SYS*, are used again.

Only one of the Role and Authorization Profile fields is ever checked. The other field can be left empty in the definition of the authorizations.

The previous object *S_USER_SYS* can be used in decentralized administration to grant administration rights for only users in a certain system from the central user administration. The object *S_USER_SYS* defines which system a user administrator can access from the central user administration and the activities that are allowed.



The object Authorization: Role Check (*S_USER_AGR*) defines the role names for which an administrator is authorized and the activities that are allowed.

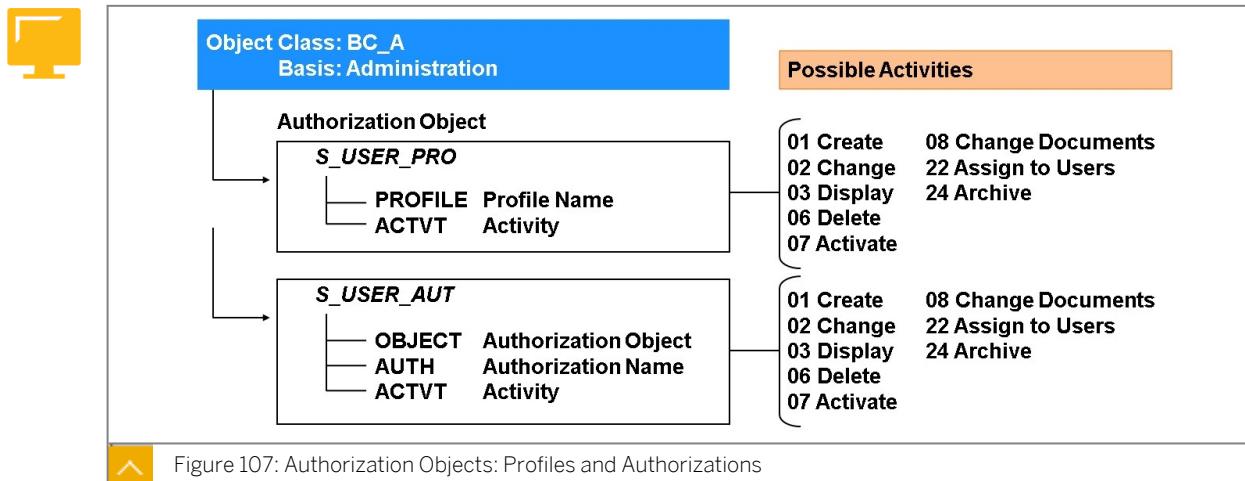
The object *S_USER_AGR* can be used in decentralized administration to grant an administrator authorization access to only certain roles (such as for a module or an organizational unit).

The object Authorizations: Transactions in Roles (*S_USER_TCD*) defines the transactions that an administrator may include in a role.

The object *S_USER_TCD* can be used to grant an administrator authorization to include only certain transactions in roles and thus prevent critical transactions from being included in roles.

The object Authorizations: Field Values for Roles (*S_USER_VAL*) defines the field values an administrator may enter in roles for a particular authorization object and particular fields.

The object *S_USER_VAL* can be used to grant an administrator authorization to assign only certain authorizations in roles and thus prevent critical authorizations from being included in roles.

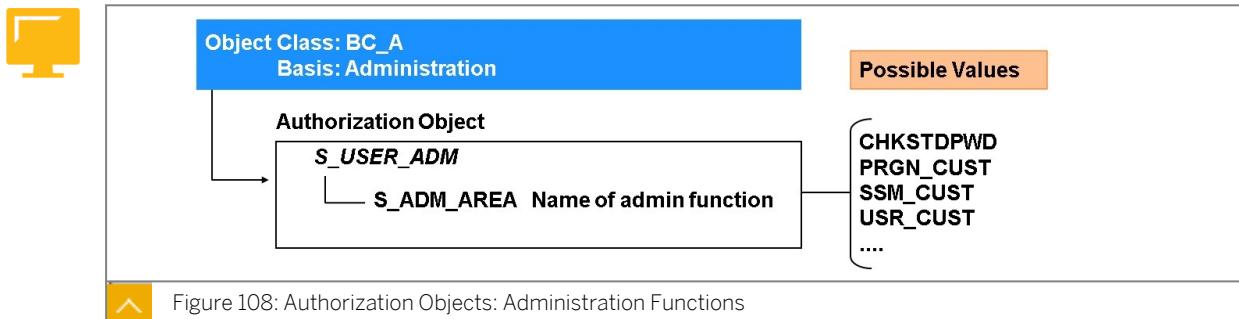


The object User Master Record Maintenance: Authorization Profile (*S_USER_PRO*) defines the profile names for which an administrator has authorization and the activities that are allowed.

The object *S_USER_PRO* can be used to grant an administrator authorization to assign only certain profiles in a decentralized administration (such as for a module or an organizational unit).

The object User Master Record Maintenance: Authorizations (*S_USER_AUT*) defines the authorization object name and the authorization name for which an administrator has authorization and the activities that are allowed.

The object *S_USER_AUT* can be used to grant an administrator authorization to create only certain authorizations in roles and thus prevent critical authorizations from being created in roles.



This authorization object *S_USER_ADMIN* checks access to general administration functions for user and authorization administration.

The object contains exactly one authorization field with the name of the administration functions. The field *S_ADMIN_AREA* can have the following values:

- *CHKSTDPWD*: Display special users (such as SAP*) with default passwords.
- *PRGN_CUST*: Change the Customizing table *PRGN_CUST*.
- *SSM_CUST*: Change the Customizing table *SSM_CUST*.
- *USR_CUST*: Change the Customizing table *USR_CUST*.
- *USR_CUST_S*: Change the Customizing table *USR_CUST_SYSTEM*.
- *ID_MODEL*: Change the identity model.
- *SNC4*: Check canonical SNC names.

Each administration function includes the area to be administered and the activity required to do this.

Options for Decentralization of User Administration

Options for Decentralization of User Administration

Security Requirements



- An administrator may not administer users **and** maintain authorizations **and** generate authorization profiles
- Solution by separating functions

Principle of dual control

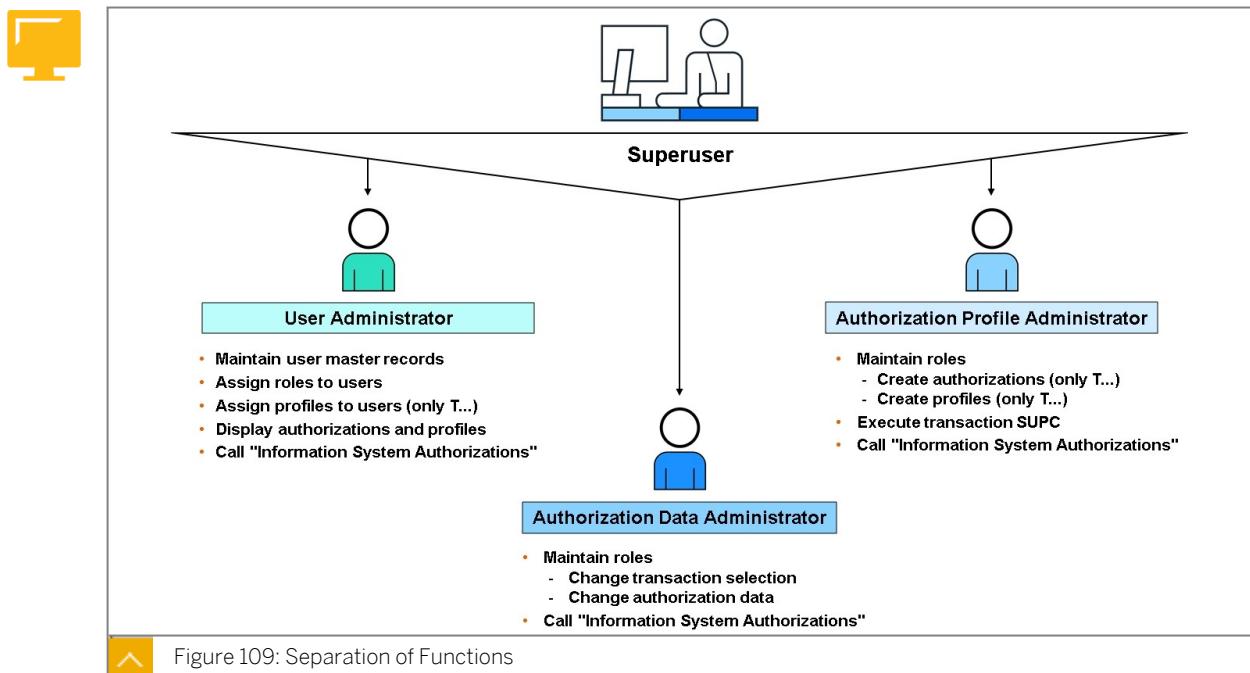
- User administration
- Authorization maintenance and generation

Principle of treble control

- User administration
- Authorization maintenance
- Authorization generation

The authorization system can be used to flexibly organize maintenance of the user master records, profiles, and authorizations.

- If your company is small and is organized centrally, all the tasks connected with maintaining the user master records and the authorization components can be handled by a single user called the superuser.
- If you want to ensure that your system maintains a higher level of security, you can share the responsibility for maintaining the user master records and the authorizations among a user administrator and an authorization administrator, each having limited responsibility (principle of dual control).
- For maximum system security you can share the responsibility for maintaining the user master records and the authorizations among a user administrator, an authorization data administrator and an authorization profile administrator, each having limited responsibility (principle of treble control).
- Since you can assign specific authorizations for the user and administrator maintenance, the administrators need not be privileged users in your IT department. Normal users can be responsible for maintaining the user master records and authorizations.



Sharing the administrative tasks among three administrators is called the **principle of treble control**.

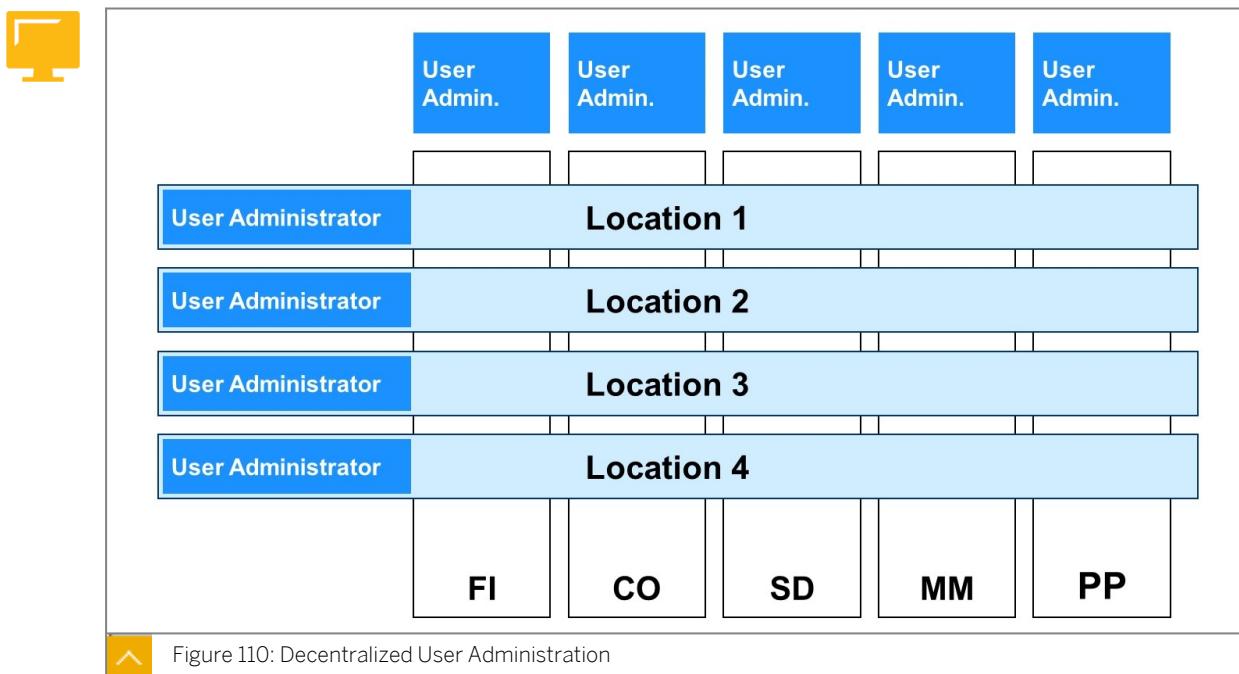
The superuser sets up all the user master records, profiles, and authorizations for the administrator.

The **authorization data administrator** creates the roles, selects transactions, and maintains the authorization data. He or she simply saves the data in Role Maintenance since he or she does not have the necessary authorization for generating the profile. He or she accepts the proposed profile name "T-...". The **authorization data administrator** may not change users, nor generate profiles.

The **authorization profile administrator** starts transaction **SUPC** and chooses *All Roles*. He or she then restricts his or her selection, for example by entering the ID of the role to be edited. On the next screen, he or she chooses *Display Profile* to check the data. If all the data is correct, he or she generates the authorization profile. The **authorization profile administrator** may not change users, change the data for roles, nor generate profiles containing authorization objects beginning with **S_USER***.

The **user administrator** then assigns this role to a user (from the user maintenance transaction **SU01**). The profile is entered for the user. The **user administrator** may not change data for roles, nor change or generate profiles.

The principle of dual control combines the tasks and authorizations of the authorization data administrator and those of the authorization profile administrator.



With decentralized user administration, there are several user administrators each responsible for administration of a certain group of users.

The administration tasks in decentralized user administration can be shared according to different criteria:

- **Application Area / Module**

The users are assigned to decentralized user administrators, each of whom is responsible for a business application or an SAP module.

- **Locations**

The users are assigned to decentralized user administrators, each of whom is responsible for all users at that location.

- **Departments**

The users are assigned to decentralized user administrators, each of whom is responsible for all the users in the department.

Technically, decentralization is implemented by grouping users to form user groups. Each decentralized user administrator may only administer the users assigned to the user group for which he or she is responsible. Accordingly, each decentralized user administrator may only assign the roles needed for his or her application module, location, or department.

Scenario 1, Principle of Dual Control



- **Central User Administration**
 - One user administrator for all users
 - Unlimited authorizations for all user administration tasks of the user administrator
- **Central Maintenance of Roles and Profiles**

One administrator performs both roles

 - Authorization data administrator
 - Authorization profile administrator
 - All authorizations for maintaining the roles and profiles



	DEVELOPMENT		PRODUCTION
	User Administrator	Authorization Data Administrator and Authorization Profile Administrator	User Administrator
S_USER_GRP			
ACTVT	*	03, 08	*
CLASS	*	*	*
S_USER_AGR			
ACTVT	03, 22	*	03, 22
ACT_GROUP	*	*	*
S_USER_TCD		*	
TCD			
S_USER_VAL			
OBJECT		*	
AUTH_FIELD		*	
AUTH_VALUE		*	
S_USER_PRO			
ACTVT	03, 08, 22	*	03, 08, 22
PROFILE	*	*	*
S_USER_AUT			
ACTVT	03, 08	*	03, 08
NAME	*	*	*

Figure 111: Authorization Management: Scenario (1)

In this scenario, there is one central user administrator for the development system and one for the production system.

The development system also has a central administrator responsible for authorization data administration and authorization profile administration.

Scenario 2, Principle of Treble Control



- Decentralized User Administration (Production System)

One user administrator for each application area (FI, MM):

- Authorized to maintain a certain user group
- Authorized to assign a certain number of roles and profiles
- No other restrictions in the specific user administration tasks

- Central Maintenance of Roles and Profiles

Separation of responsibilities:

- One authorization data administrator
- One authorization profile administrator
- No other restrictions with regard to specific roles or profiles for both administrators



	DEVELOPMENT			PRODUCTION	
	User Administrator	Authorization Data Administrator	Authorization Profile Administrator	FI User Administrator	MM User Administrator
S_USER_GRP					
ACTVT	*	03, 08	03, 08	*	*
CLASS	*	*	*	FI_USER	MM_USER
S_USER_AGR					
ACTVT	03, 22	01, 02, 03, 06	03, 64	03, 22	03, 22
ACT_GROUP	*	*	*	*	*
S_USER_TCD					
TCD		*			
S_USER_VAL					
OBJECT		*			
AUTH_FIELD		*			
AUTH_VALUE		*			
S_USER_PRO					
ACTVT	03, 08, 22	01, 02, 03, 06, 08	03, 07, 08	03, 08, 22	03, 08, 22
PROFILE	*	*	*	FI*	MM*
S_USER_AUT					
ACTVT	03, 08	01, 02, 03, 06, 08, 22	03, 07, 08	03, 08	03, 08
NAME	*	*	*	*	*

Figure 112: Authorization Management: Scenario (2)

This scenario has two user groups, each of which is administered by its own user administrator in the production system.

- The group of FI users (*FI_USER*) is administered by the FI user administrator.
- The group of MM users (*MM_USER*) is administered by the MM user administrator.

The decentralized user administrators must be restricted as follows:

- Administration of the user group for which they are responsible (*S_USER_GRP*)
- Assignment of the relevant roles and profiles for the user group (*S_USER_AGR*, *S_USER_PRO*)

The users must be assigned to the appropriate groups (*FI_USER*, *MM_USER*).

Caution: Users not belonging to any group can be administered by both user administrators.

Scenario 3, Principle of Treble Control, Decentralized User Administration in PRD



- Central Creation and Deletion for All Users (prod.)
- Decentralized User Administration (Production System)

One user administrator for each application area (FI, MM):

- Authorized to maintain a certain user group
- Authorized to assign a certain number of roles and profiles
- Authorized for only certain user administration tasks (change, lock/unlock, reset password)

• Central Maintenance of Roles and Profiles

Separation of responsibilities:

- One authorization data administrator
- One authorization profile administrator
- No other restrictions with regard to specific roles or profiles for both administrators



	DEVELOPMENT			PRODUCTION		
	User Administrator	Authorization Data Administrator	Authorization Profile Administrator	FI User Administrator	MM User Administrator	Central User Administrator
S_USER_GRP						
ACTVT	*	03, 08	03, 08	02, 03, 05, 22	02, 03, 05, 22	01, 03, 06, 08
CLASS	*	*	*	FI_USER	MM_USER	*
S_USER_AGR						
ACTVT	03, 22	01, 02, 03, 06	03, 64	03, 22	03, 22	03
ACT_GROUP	*	*	*	*	*	*
S_USER_TCD						
TCD	*					
S_USER_VAL						
OBJECT	*					
AUTH_FIELD	*					
AUTH_VALUE	*					
S_USER_PRO						
ACTVT	03, 08	01, 02, 03, 06, 08	03, 07, 08	03, 08, 22	03, 08, 22	03, 08
PROFILE	*	*	*	FI*	MM*	*
S_USER_AUT						
ACTVT	03, 08	01, 02, 03, 06, 08, 22	03, 07, 08	03, 08	03, 08	03, 08
NAME	*	*	*	*	*	*

Figure 113: Authorization Management: Scenario (3)

This scenario has two user groups, each of which is administered by its own user administrator in the production system:

- The group of FI users (*FI_USER*) is administered by the FI user administrator.
- The group of MM users (*MM_USER*) is administered by the MM user administrator.

In contrast to scenario 2, the user administrators may only perform the following activities for users in their group:

- Lock / unlock users
- Change passwords

- Assign roles and profiles

A central user administrator creates and deletes the users.

The decentralized user administrators must be restricted as follows:

- Administration of the user group for which they are responsible (*S_USER_GRP*)
- Activities in user administration (*S_USER_GRP*)
- Assignment of the relevant roles and profiles for the user group (*S_USER_AGR*, *S_USER_PRO*)

The users must be assigned to the appropriate groups (*FI_USER*, *MM_USER*).

Unit 5

Exercise 9

Practice System Exercise: Access Control and User Administration

Business Example

As part of their daily work, they check the security settings. You can refine these by setting up a security policy.

Task 1: Check Security Settings

You are the data protection officer and want to check the SAP system's assignment of authorizations and security.

1. Display all the users *GR##** according to logon date and password change.

Which of your users *GR##** are not in use?

Which of your users *GR##** do not have a valid password?

When did the user *GR##-ADM* log on to the system?

Result

The users which are not in use are displayed in the *Date of Last Logon* column.

The users who do not have a valid password are displayed in the *Password Status* column.

The logon date and time of the user *GR##-ADM* is displayed in the *Date of Last Logon* and *Last Logon Time* columns.

2. Check the logon rules and settings for special users in the system. How can you request this information?

How many characters are set for the minimum password length?

After how many incorrect logons is the user locked?

Is the user automatically unlocked?

Result

System parameter to define the minimum password length: *login/min_password_lng := "5"*

System parameter to define the number of incorrect logons is the user locked: *login/fails_to_user_lock := "5"*

System parameter to define if users are automatically unlocked: *login/failed_user_auto_unlock := "0 (no)"*

You can view the descriptions of the system parameters in transaction **RZ11**.

Task 2: Create a Security Policy

Create a security policy with the following restrictions: MIN_PASSWORD_LENGTH = 8 and PASSWORD_CHANGE_INTERVAL = 100.

1. Start the transaction **SECPOL**.
2. Create a new security policy **GR##-SECPOL**.
3. Assign the security policy to the users you have created using the *User Mass Maintenance* transaction.

User Name
GR##-FI1
GR##-FI2
GR##-SD1
GR##-SD2
GR##-MM1
GR##-MM2

Task 3: Explore Authorization Objects for Table Maintenance Using Standard Tools

Create authorizations so that a user can view specific tables in transaction **SE16**. The user must be able to display two tables. Those table names are **USR40** and **PRGN_CUST**.

1. Which authorization objects give access for the display or maintenance of table contents with generic table access tools?

Result

The following authorization objects give access for the display or maintenance of table contents with generic table access tools?

- **S_TABU_DIS**
- **S_TABU_NAM**

2. Explore authorization object **S_TABU_DIS**.

Display the documentation for the authorization object **S_TABU_DIS**.

What is the main function of this authorization object?

3. Which fields does authorization object S_TABU_DIS contain?
-
-

4. Explore authorization object S_TABU_NAM.

Display the documentation for the authorization object S_TABU_NAM.

What is the main function of this authorization object?

5. Which fields does authorization object S_TABU_NAM contain?
-
-

Task 4: Find the Authorization Group Assigned to a Table

Find the authorization group assigned to table USR40.

Then, find all tables assigned to authorization group SUSR.

1. Find the authorization group assigned to table USR40.

Table group assigned to table USR40:

2. How many tables are assigned to authorization group SUSR?
-

Task 5: Create a Role for Reading Tables USR40 and PRGN_CUST

Create a role for reading tables USR40 and PRGN_CUST. Access to table USR40 should be assigned by authorization object S_TABU_DIS and access to table PRGN_CUST should be assigned by authorization object S_TABU_NAM.

1. Start Role Maintenance, create the role GR##_TAB_ANZ, and write a short description.
2. Add the transaction SE16 to the role menu.
3. Go to the Authorizations tab page and define the authorizations.

Define the following authorizations:

Object	Field	Value (Interval)
S_TABU_DIS	DICBERCLS	SUSR
	ACTVT	Display

Object	Field	Value (Interval)
S_TABU_NAM	TABLE	PRGN_CUST
	ACTVT	Display

4. If necessary: Maintain Authorizations - Set all open authorization values to full authorization.
5. Maintain Authorizations - Generate the authorization profile for your role.
6. Assign the role to your user *GR##-FI1*. Perform a user master comparison and exit role maintenance.

Task 6: Log On as GR##-FI1 and Check the Table Authorizations

Log on as *GR##-FI1*. Call transaction *SE16*, and answer the following questions:

Use the password automatically generated in the exercise for the *user master record* or assign a new initial password in user maintenance.

Change the password when you log on: _____

1. Log on to the system as user *GR##-FI1*.
2. Can you display table *USR40*? Why?

Result

Yes, you can display table *USR40*. When this table is displayed, authorization group *SUSR*, which is in the user master record, is checked.

3. Can you display table *USREFUSVAR*? Why?

Result

Yes, you can display table *USREFUSVAR*. This table is also assigned to the authorization group *SUSR*.

4. Can you display table *PRGN_CUST*? Why?

Result

Yes, you can display table *PRGN_CUST*. When this table is displayed, authorization is checked by authorization object *S_TABU_NAM*.

Unit 5 Solution 9

Practice System Exercise: Access Control and User Administration

Business Example

As part of their daily work, they check the security settings. You can refine these by setting up a security policy.

Task 1: Check Security Settings

You are the data protection officer and want to check the SAP system's assignment of authorizations and security.

1. Display all the users **GR##*** according to logon date and password change.

Which of your users **GR##*** are not in use?

Which of your users **GR##*** do not have a valid password?

When did the user **GR##-ADM** log on to the system?

- a) Navigate to the User Information System in the SAP Menu.

SAP Menu: → *Tools* → *Administration* → *User Maintenance* → *Information System*

- b) Expand the structure for the *User* node, and select the report *By Logon Date and Password Change* (RSUSR200) by double-clicking it.
- c) Enter **GR##*** in the *User* field.
- d) Choose *Execute (F8)*.

Result

The users which are not in use are displayed in the *Date of Last Logon* column.

The users who do not have a valid password are displayed in the *Password Status* column.

The logon date and time of the user **GR##-ADM** is displayed in the *Date of Last Logon* and *Last Logon Time* columns.

2. Check the logon rules and settings for special users in the system. How can you request this information?

How many characters are set for the minimum password length?

After how many incorrect logons is the user locked?

Is the user automatically unlocked?

- a) Start the *Display Profile Parameter* transaction (RSPFPAR).

In the *OK* code field, enter the transaction code RSPFPAR.

- b) Enter **login*** in the *Profile Parameters* field.

- c) Choose *Execute (F8)*.

Result

System parameter to define the minimum password length: *login/min_password_lng := "5"*

System parameter to define the number of incorrect logons is the user locked: *login/fails_to_user_lock := "5"*

System parameter to define if users are automatically unlocked: *login/failed_user_auto_unlock := "0 (no)"*

You can view the descriptions of the system parameters in transaction RZ11.

Task 2: Create a Security Policy

Create a security policy with the following restrictions: MIN_PASSWORD_LENGTH = 8 and PASSWORD_CHANGE_INTERVAL = 100.

1. Start the transaction SECPOL.

- a) In the *OK* code field, enter the transaction code SECPOL.

2. Create a new security policy GR##-SECPOL.

- a) Choose the *Display → Change (Ctrl+F1)* icon.

- b) Choose *New Entries*.

- c) Enter **GR##-SECPOL** in the *Security Policy* column and enter **Policy ##** in the *Short Text* column.

- d) Choose *Save (Ctrl+S)*.

- e) Select a transport request or create a new one:

To create a new transport request choose *Create*.

Enter a short description and choose *Save (Enter)*.

Enter a short description and choose *Save*.

- f) Select the line with your security policy GR##-SECPOL.

- g) Double-click *Attributes* in the *Dialog Structure* area.

- h) Choose *New Entries*.

- i) Enter **MIN_PASSWORD_LENGTH** in the *Policy Attribute Name* column and enter **8** in the *Attrib. Value* column.

- j) Enter **PASSWORD_CHANGE_INTERVAL** in the *Policy Attribute Name* column and enter **100** in the *Attrib. Value* column.
 - k) Choose Save (*Ctrl+S*).
 - l) Choose Back (*F3*) twice.
3. Assign the security policy to the users you have created using the *User Mass Maintenance* transaction.

User Name
GR##-FI1
GR##-FI2
GR##-SD1
GR##-SD2
GR##-MM1
GR##-MM2

- a) Start the *User Mass Maintenance* transaction.
SAP Menu: → Tools → Administration → User Maintenance → User Mass Maintenance (transaction code **SU10**).
- b) Choose *Address Data* in the *User selection* area.
- c) Enter **GR##*** in the *Users* field.
- d) Choose *Execute (F8)*.
- e) Choose the *Select All* icon on the top left of the resulting table (*Ctrl+A*).
- f) Choose *Transfer*.
- g) Choose *Change (Shift+F6)*.
- h) Enter **GR##-SECPOL** in the *Security Policy* field.
- i) Choose *Change*.
- j) Choose Save (*Ctrl+S*).
- a) Choose Back (*F3*) twice.

Task 3: Explore Authorization Objects for Table Maintenance Using Standard Tools

Create authorizations so that a user can view specific tables in transaction **SE16**. The user must be able to display two tables. Those table names are **USR40** and **PRGN_CUST**.

1. Which authorization objects give access for the display or maintenance of table contents with generic table access tools?
-
-

Result

The following authorization objects give access for the display or maintenance of table contents with generic table access tools?

- S_TABU_DIS
- S_TABU_NAM

2. Explore authorization object *S_TABU_DIS*.

Display the documentation for the authorization object *S_TABU_DIS*.

What is the main function of this authorization object?

- a) Navigate to the User Information System in the SAP Menu.

SAP Menu: → *Tools* → *Administration* → *User Maintenance* → *Information System*

- b) Expand the structure for the *Authorization Objects* node, and select the report *Authorization Objects - By Object Name, Text* by double-clicking it.

- c) Enter **s_TABU_DIS** in the *Authorization Object* field.

- d) Choose *Execute (F8)*.

- e) Double-click object *S_TABU_DIS*.

- f) Choose *Display Object Documentation*.

This authorization object checks authorizations for displaying or maintaining table contents.

3. Which fields does authorization object *S_TABU_DIS* contain?

- a) Take the fields of *S_TABU_DIS* from the *Defined fields* in the documentation:

- DICBERLCS (Authorization Group)
- ACTVT (activity)

Authorization object *S_TABU_DIS* provides access for all tables of an authorization groups.

- b) Choose *Close*.

- c) Choose *Cancel (F12)*.

- d) Choose *Back (F3)* to return to the *Authorization Objects by Complex Selection Criteria* screen.

4. Explore authorization object *S_TABU_NAM*.

Display the documentation for the authorization object *S_TABU_NAM*.

What is the main function of this authorization object?

- a) Navigate to the User Information System in the SAP Menu.

SAP Menu: → *Tools* → *Administration* → *User Maintenance* → *Information System*

b) Expand the structure for the *Authorization Objects* node, and select the report *Authorization Objects - By Object Name, Text* by double-clicking it.

c) Enter **S_TABU_NAM** in the *Authorization Object* field.

d) Choose *Execute (F8)*.

e) Double-click object **S_TABU_NAM**.

f) Choose *Display Object Documentation*.

This authorization object checks authorizations for displaying or maintaining table contents.

5. Which fields does authorization object S_TABU_NAM contain?
-
-

a) Take the fields of S_TABU_NAM from the *Defined fields* in the documentation:

- TABLE (table or view name)

- ACTVT (activity)

Authorization object S_TABU_DIS provides access for a table or a view. The object is only checked if the authorization check for object S_TABU_DIS failed.

b) Choose *Close*.

c) Choose *Cancel (F12)*.

d) Choose *Back (F3)* to return to the *Authorization Objects by Complex Selection Criteria* screen.

Task 4: Find the Authorization Group Assigned to a Table

Find the authorization group assigned to table USR40.

Then, find all tables assigned to authorization group SUSR.

1. Find the authorization group assigned to table USR40.

Table group assigned to table USR40:

a) **Start the Generate Table Maintenance Dialog transaction (SE54).**

SAP Menu: Tools → ABAP Workbench → Development → Other Tools → General Table Maintenance Dialog, (transaction code: SE54).

b) Select “Assign Authoriz. Group” and choose *Display*.

c) Enter **USR40** in the *Table/View* field.

d) Choose *Execute (F8)*.

Table USR40 is assigned to the authorization group **SUSR**

e) Choose *Back (F3)* twice to return to the start screen of transaction SE54.

2. How many tables are assigned to authorization group SUSR?
-

a) **Start the Generate Table Maintenance Dialog transaction (SE54).**

SAP Menu: *Tools* → *ABAP Workbench* → *Development* → *Other Tools* → *General Table Maintenance Dialog* (transaction code: SE54).

b) Select “Assign Authoriz. Group” and choose *Display*.

c) Enter **SUSR** in the *Authorization Group* field.

d) Choose *Execute (F8)*.

52 tables are assigned to the authorization group *SUSR*.

e) Choose *Back (F3)* twice to return to the start screen of transaction SE54.

Task 5: Create a Role for Reading Tables USR40 and PRGN_CUST

Create a role for reading tables USR40 and PRGN_CUST. Access to table USR40 should be assigned by authorization object S_TABU_DIS and access to table PRGN_CUST should be assigned by authorization object S_TABU_NAM.

1. Start Role Maintenance, create the role **GR##_TAB_ANZ**, and write a short description.

a) SAP Menu:

Tools → *Administration* → *User Maintenance* → *Role Administration* → *Roles* (transaction code PFCG).

b) Enter the name for the role **GR##_TAB_ANZ** in the *Role* field.

c) Choose *Create Single Role*.

d) Enter description **Display tables** in the *Description* field.

e) Then choose *Save (Ctrl+S)* to save your role.

2. Add the transaction SE16 to the role menu.

a) Go to the *Menu* tab page.

b) Choose the *Transaction* button and enter the following transaction code in the *Transaction code* field:
- SE16

c) Choose *Assign Transactions*.

d) Then choose *Save (Ctrl+S)* to save your role.

3. Go to the *Authorizations* tab page and define the authorizations.

Define the following authorizations:

Object	Field	Value (Interval)
S_TABU_DIS	DICBERCLS	SUSR
	ACTVT	Display

Object	Field	Value (Interval)
S_TABU_NAM	TABLE	PRGN_CUST
	ACTVT	Display

- a) Go to the *Authorizations* tab page.
 - b) Choose *Change Authorization Data*.
 - c) Expand *Object Class BC_A*.
 - d) Expand *Authorization Object S_TABU_DIS*.
 - e) Expand *Authorization Authorizat. OO*.
 - f) Choose the *Pencil* icon to the right of the *DICBERCLS* field..
 - g) Enter **SUSR** in the *Field values* window.
 - h) Choose *Transfer (Enter)*.
 - i) Expand *Authorization Object S_TABU_NAM*.
 - j) Expand *Authorization Authorizat. OO*.
 - k) Choose the *Pencil* icon to the right of the *TABLE* field.
 - l) Enter **PRGN_CUST** in the *Field values* window.
 - m) Choose *Transfer (Enter)*.
4. If necessary: Maintain Authorizations - Set all open authorization values to full authorization.
- a) Choose the *Status* button.
 - b) Choose *Execute (Enter)* in the *Assign Full Authorization of Subtree* window.
5. Maintain Authorizations - Generate the authorization profile for your role.
- a) Choose the *Generate* icon.
 - b) In the *Assign Profile Name for Generated Authorization Profile* window, accept the proposed profile name and choose *Execute (Enter)*.
 - c) Choose *Back (F3)* to return to the *Change Roles* screen.
6. Assign the role to your user **GR##-FI1**. Perform a user master comparison and exit role maintenance.
- a) Go to the *User* tab page.
 - b) Enter **GR##-FI1** in the *User ID* column.
 - c) Choose *Save (Ctrl+S)*.
 - d) Choose *User Comparison*.
 - e) Choose *Full Comparison* on the *Compare Role User Master Record* window.
 - f) Choose *Cancel (F12)* on the *Compare Role User Master Record* window.
 - g) Choose *Back (F3)* to return to the *Role Maintenance* screen.

Task 6: Log On as GR##-FI1 and Check the Table Authorizations

Log on as **GR##-FI1**. Call transaction **SE16**, and answer the following questions:

Use the password automatically generated in the exercise for the *user master record* or assign a new initial password in user maintenance.

Change the password when you log on: _____

1. Log on to the system as user GR##-FI1.
 - a) Start SAP Logon.
 - b) Select system *T41* and choose *Log On*.
 - c) Enter the user name **GR##-FI1** in the *User* field.
 - d) Enter the generated password in the *Password* field.
Use the password automatically generated in the exercise for the *user master record* or assign a new initial password in user maintenance.
 - e) Choose *Enter*.
 - f) Enter a new productive password of your choice in the *New Password* and the *Repeat Password* fields.
New password : _____
 - g) Choose *Transfer (Enter)*.
 - h) Choose *Continue (Enter)*.

2. Can you display table USR40? Why?

- a) Start transaction SE16 (Data Browser) from the *User menu*.
- b) Enter **USR40** in the *Table Name* field.
- c) Choose *Table Contents (F7)*.
- d) Choose *Execute (F8)*.
- e) Choose *Back (F3)* twice, to return to the *Data Browser: Initial Screen*.

Result

Yes, you can display table USR40. When this table is displayed, authorization group *SUSR*, which is in the user master record, is checked.

3. Can you display table USREFUSVAR? Why?

- a) Start transaction SE16 (Data Browser) from the *User menu*.
- b) Enter **USREFUSVAR** in the *Table Name* field.
- c) Choose *Table Contents (F7)*.
- d) Choose *Execute (F8)*.
- e) Choose *Back (F3)* twice, to return to the *Data Browser: Initial Screen*.

Result

Yes, you can display table USREFUSVAR. This table is also assigned to the authorization group *SUSR*.

4. Can you display table PRGN_CUST? Why?

-
-
- a) Start transaction SE16 (Data Browser) from the *User menu*.
 - b) Enter **PRGN_CUST** in the *Table Name* field.
 - c) Choose *Table Contents (F7)*.
 - d) Choose *Execute (F8)*.
 - e) Choose *Back (F3)* twice, to return to the *Data Browser: Initial Screen*.
 - f) Log off the system.

Result

Yes, you can display table PRGN_CUST. When this table is displayed, authorization is checked by authorization object S_TABU_NAM.



LESSON SUMMARY

You should now be able to:

- Implement user and authorization management strategies.

Learning Assessment

1. What color is the traffic light for the following case? For an authorization object against which the check is performed in the selected transaction, Role Maintenance has default values for the authorization content.

Choose the correct answer.

- A Red
- B Yellow
- C Green

2. What color is the traffic light for the following case? For an authorization object against which the check is performed in the selected transaction, Role Maintenance does not have default values for the authorization content, and this field is an “organizational level field”.

Choose the correct answer.

- A Red
- B Yellow
- C Green

3. Which user is the only user that can access the SAP system without a user master record?

Choose the correct answer.

- A SAP*
- B DDIC
- C EarlyWatch

4. Which user should only be used for monitoring and performance functions?

Choose the correct answer.

- A SAP*
- B DDIC
- C EarlyWatch

5. An administrator may not administer users and maintain authorizations and generate authorization profiles when implementing decentralized user administration.

Determine whether this statement is true or false.

True

False

Learning Assessment - Answers

1. What color is the traffic light for the following case? For an authorization object against which the check is performed in the selected transaction, Role Maintenance has default values for the authorization content.

Choose the correct answer.

- A Red
- B Yellow
- C Green

The traffic light is green in this case.

2. What color is the traffic light for the following case? For an authorization object against which the check is performed in the selected transaction, Role Maintenance does not have default values for the authorization content, and this field is an “organizational level field”.

Choose the correct answer.

- A Red
- B Yellow
- C Green

The traffic light is red in this case.

3. Which user is the only user that can access the SAP system without a user master record?

Choose the correct answer.

- A SAP*
- B DDIC
- C EarlyWatch

SAP* is the only user in the SAP system for which no user master record is required, since it is defined in the system code.

4. Which user should only be used for monitoring and performance functions?

Choose the correct answer.

- A SAP*
- B DDIC
- C EarlyWatch

The EarlyWatch user should only be used for monitoring and performance functions.

5. An administrator may not administer users and maintain authorizations and generate authorization profiles when implementing decentralized user administration.

Determine whether this statement is true or false.

- True
- False

The statement is true.

UNIT 6

Using Traces

Lesson 1

Troubleshooting Authorization Checks	256
Exercise 10: Practice System Exercise: Troubleshoot and Administer Aids	265

Lesson 2

Using Traces to Maintain Role Menus and Authorizations	269
Exercise 11: Practice System Exercise: Use Authorization Trace	273

UNIT OBJECTIVES

- Trace and analyze SAP ABAP authorization checks.
- Utilize authorization trace data.

Troubleshooting Authorization Checks

LESSON OVERVIEW

In this lesson, you will obtain an overview of the options for analyzing authorization checks. The lesson will also deal with the information system for user maintenance and the Audit Information System.

Business Example

Missing authorizations can be found with the analysis functions. The results established in this way are usually combined in new combinations of authorizations. However, if you use existing authorizations that fulfill the requirements, you have improved the clarity of the authorization concept. This is an information system and various evaluation functions for this purpose.



LESSON OBJECTIVES

After completing this lesson, you will be able to:

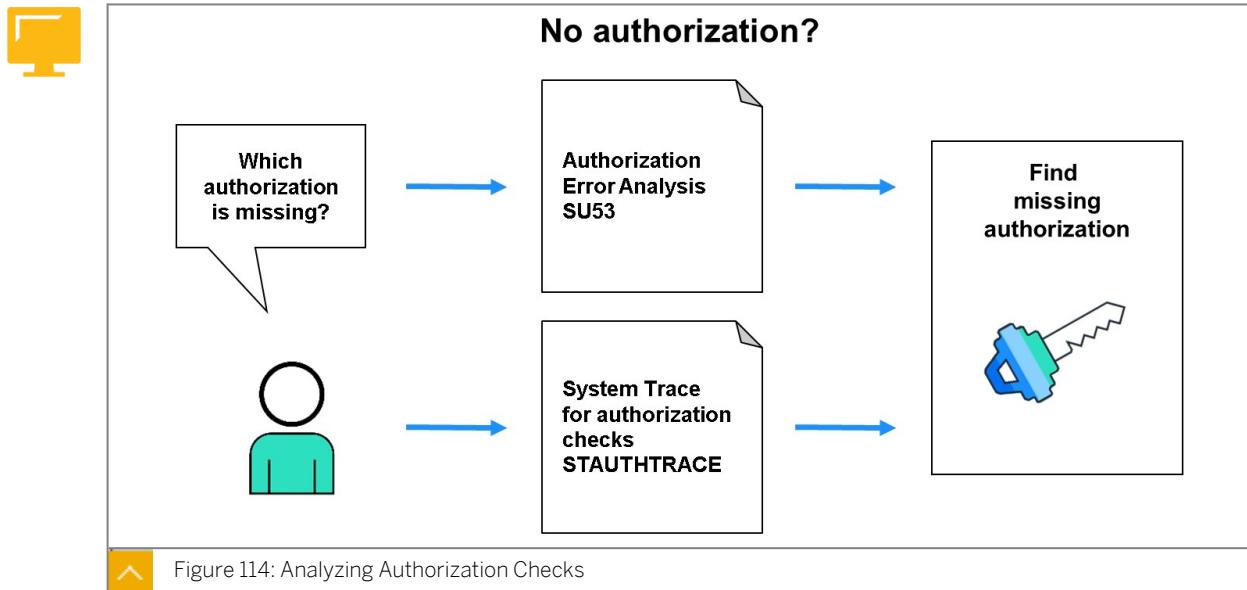
- Trace and analyze SAP ABAP authorization checks.

Error Analysis for Authorization Problems

If you cannot find documentation about authorization for a transaction, or if a *failed authorization check* is always reported when you execute a transaction, there are two ways in which you can determine the required authorizations:

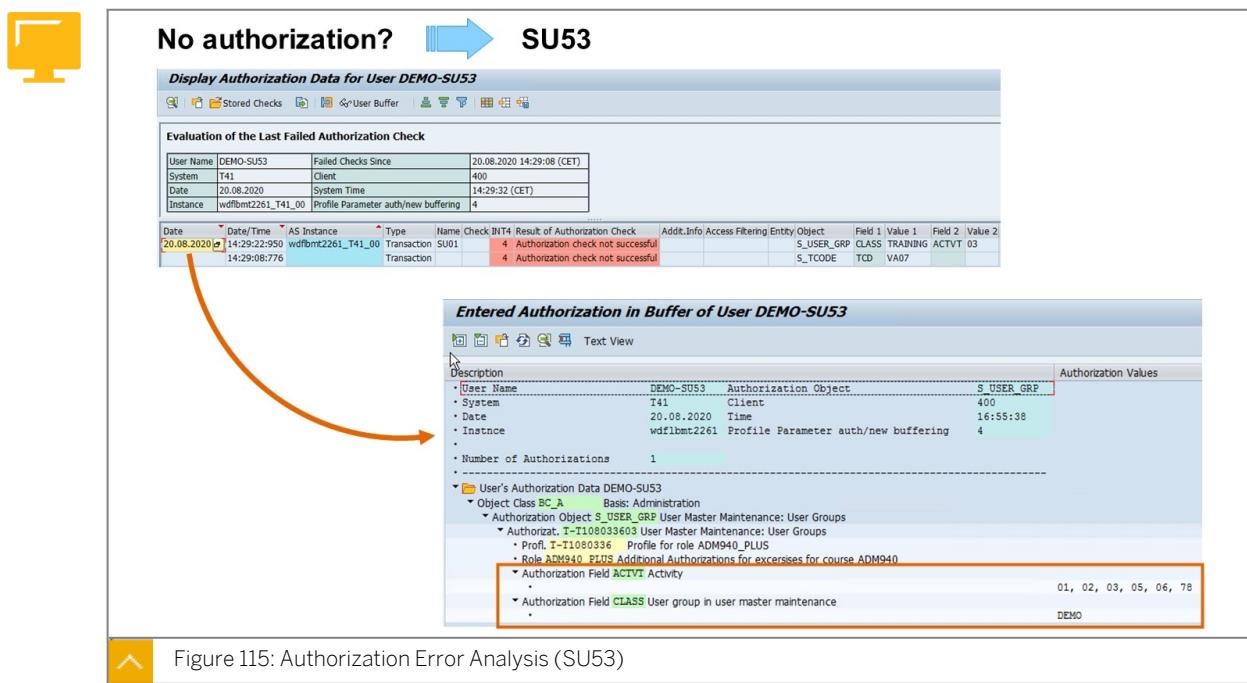
1. With the authorization error analysis and transaction code SU53.
2. With the system trace for authorization checks STAUTHTRACE.

Analyzing Authorization Checks



In the next example, a transaction from the *F1* area was executed and terminated due to a missing authorization. The system message is: You are not authorized for this function.

To analyze this error, choose the menu path *System → Utilities → Display Authorization Check* or enter transaction code **SU53** in the command field.



You can now analyze the last error in your system that occurred due to a missing authorization. You can call transaction **SU53** in any session, not just in the session in which the error occurred.

Example: In the previous figure, the user calls transaction **VA07**. The message “You are not authorized for transaction **VA07**” appears.

Then, the user calls transaction SU01 and will display the user data of another user. In this case, the authorization object S_USER_GRP is checked. The authorization object is assigned to the user, but the required authorization values (activity "03" and user group "Training") are not assigned.

To analyze the missing authorization, the user enters transaction code SU53 in the command field and the system displays the authorization object that caused the last failed authorization checks. The system displays the value of the authorization object that the program required.

In the case of missing authorization values for a specific authorization object, you can check which other authorization values are assigned to the user.

Transaction SU53 displays the maximum of 100 failed authorization checks for each user in the upper area. It displays these for the last three hours at most. If there are very many active users and very many failed authorization checks, the number of checks and the period that is covered can also be smaller for a user. In addition, it displays the context in which the check occurred (that is, the transaction, RFC function module, or service). In the lower area, the authorizations of the user are displayed for all of the authorization objects that are displayed.

The system uses a ring buffer in the shared memory of the application server for saving failed authorization checks. Web Dynpro applications can also access this memory area.

The size of the buffer depends on the number of work processes, which is defined by profile parameters. It consists of 100 authorization checks for each work process in the standard system. This number can be changed by setting the profile parameter *auth/su53_buffer_entries*. The profile parameter can be maintained using transactions RZ11 and RZ10.

The user can also use transaction SU56 to view which authorizations are currently in his or her buffer.



Hint:

If the user was prevented from executing an action, and the authorization error analysis shows: *All authorization checks have so far been successful*, the problem is **not** an authorization problem. The problem has another cause.

If transaction SU53 does not provide a satisfactory result, you can still use the system trace for authorization checks (STAUTHTRACE).

System Trace for Authorization Checks

If you do not know the required authorization, you can use the system trace or the authorization error analysis to determine them. You can use the system trace function to record authorization checks in your own and in external sessions using the system trace function : System Trace for Authorization Checks STAUTHTRACE. As an alternative, you can also use the system trace: Tools → Administration → Monitor → Traces → System Trace (transaction ST01).

The trace records each authorization object that is tested, along with the object's fields and the values tested.

**Note:**

The system trace allows the recording of internal SAP system activities. The system trace is primarily used when an authorization trace is required. Besides authorization checks, the following components can be monitored using the system trace: kernel functions, kernel modules, database accesses, table buffers, RFC calls, and lock operations.

The system trace for authorization checks (transaction STAUTHTRACE) provides an optimized user interface to trace authorization checks. It works in the same way as the system trace (transaction ST01). However, it only evaluates authorization checks.

The evaluation of the system trace for authorization checks can be performed for the current server. It is also possible to start and stop the system trace for authorization checks on all servers or on selected servers of a system. When you display the authorization checks that were performed, the system displays an additional column containing the name of the server.



Date	Data/Time	User	Type	Application Name	Program	Chkd	Result	Result of Authorization Check	Addit.Info Object	Field 1	Value 1	Field 2	Value 2
07.05.2014	08:31:45:385	ADM940	Transaction	SESSION_MANAGER	SAPLUS	0	0	Authorization check successful	S_TCODE	TCD	SU01		
07.05.2014	08:31:45:399	ADM940	Transaction	SESSION_MANAGER	SAPLUS	0	0	Authorization check successful	S_USER_GRP_CLASS		ACTVT		

Result := Return code 0: Authorization check successful; 1: Missing authorizations

Figure 116: System Trace for Authorization Checks (STAUTHTRACE)

You can analyze authorizations using the system trace for authorization checks as follows:

1. If necessary, set *Trace Only for User* and start the trace by choosing *Activate Trace*. The system writes the trace data in the current trace file.
2. Execute the application as fully as possible in a separate session on the same application server.
3. Deactivate the trace by choosing *Deactivate Trace*.
4. You can optionally restrict the results display with the options under *Restrictions*.
5. Choose *Evaluate*.

The system trace (transaction ST01) offers a variety of tracing options. Among others, you can trace authorization checks. For evaluation of the system trace, it is necessary that the trace and the transaction to be traced are running on the same application server.

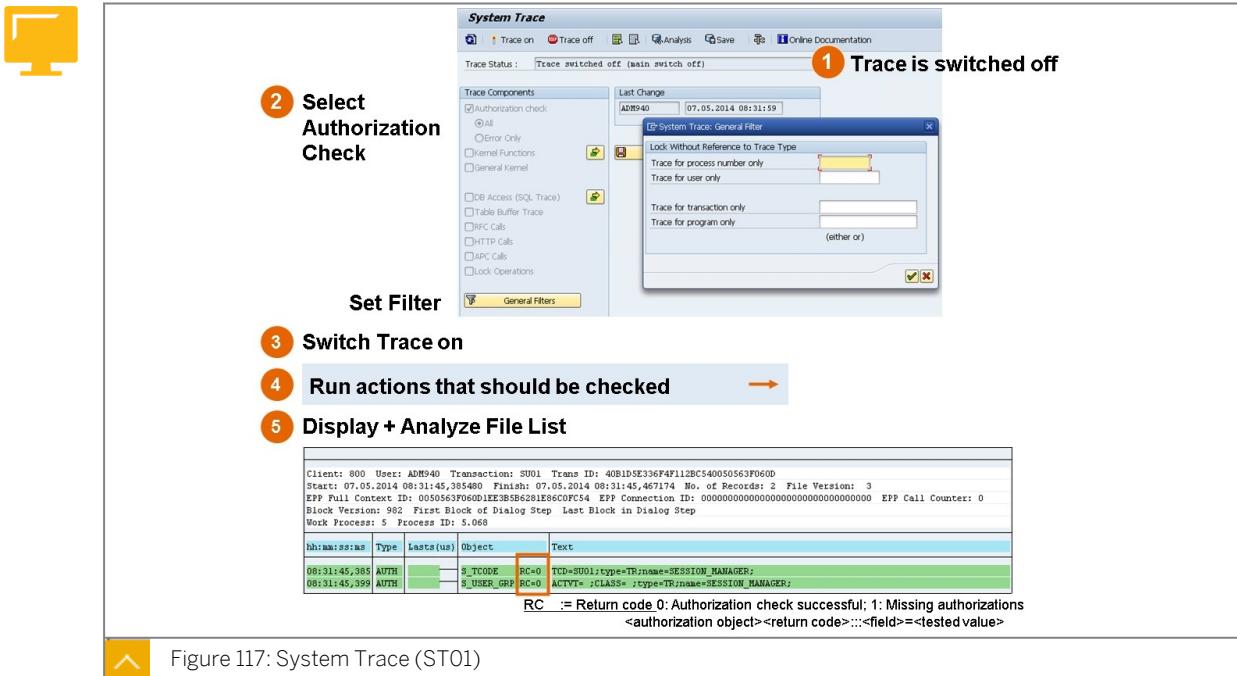


Figure 117: System Trace (ST01)

You can analyze authorizations as follows:

1. Choose *Tools → Administration → Monitor → Traces → System Trace* or transaction ST01.
2. Choose the *Authorization Check* trace component.
3. To restrict the trace function to your own sessions, choose *Edit → Filter → Shared*. Enter your user ID in the *Trace for user only* field in the displayed dialog box.
4. Start the trace by choosing the *Trace on* button. The trace is automatically written to the hard disk.
5. Execute the relevant system actions.
6. Once you have completed the analysis, choose *Trace off*.
7. To display the results of the analysis, choose *Goto → Analysis* or the *Analysis* button. Select the desired file and choose *Start Reporting*.

The results of the authorization check are displayed in the following format (see also the previous figure):

<authorization object><return code>:::<field>=<tested value>

The return code shows whether or not the authorization code was successful.



Hint:

The return code "0" (dark green) means that the check at this point was "successful". Any other result means that an error occurred, which may have various causes, depending on the programming (see SAP Note 209899).

Information Systems for Administrators and Audit

You should not immediately implement the result of a trace or of transaction SU53 as new roles or profiles. First, analyze the system for existing settings. The *Information System* and

the *Audit Info System* (which is used by auditors) are available to the administrator for this purpose.

You can use the User Information System to obtain an overview of the authorizations and users in your SAP system at any time using search criteria that you specify. In particular, you can display lists of users to which authorizations classified as critical are assigned. You can also use the User Information System to do the following.

Examples from the User Information System



- Compare roles and users
- Display change documents for the authorization profile of a user
- Display the transactions contained in a role
- Create where-used lists

We recommend that you regularly check the various list that are important for you. Define a monitoring procedure and corresponding checklists to make sure that you continually review your authorization plan. We especially recommend that you determine which authorizations you consider critical and regularly review which users have these authorizations in their profiles.



Figure 118: Information System

You can start the Information System from the SAP Menu by choosing *Tools → Administration → User Maintenance → Information System*. You can also branch to the Information System authorizations from the User Maintenance transaction (SU01) by choosing the menu path *Information → Information System*.

You can find elements of the authorization system using different selection criteria.

The Information System (RSUSR998) and parts of the Information System can be called as executable reports using transaction SA38. Here are a few examples:

- RSUSR002; Users by complex selection criteria

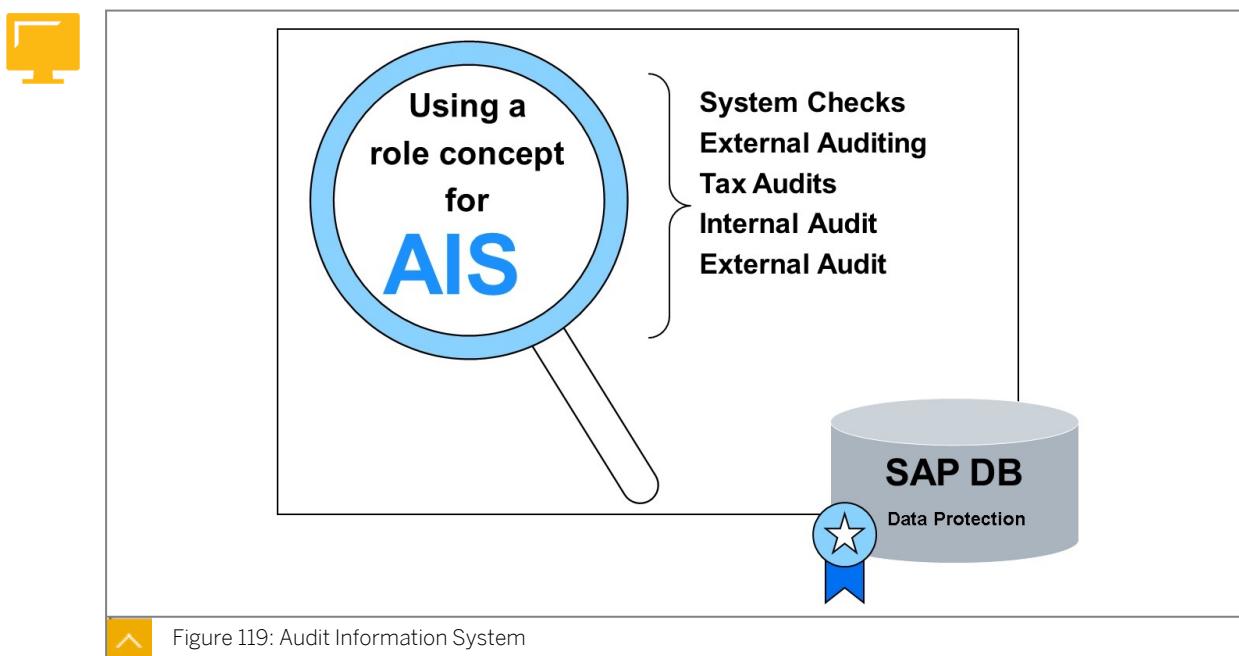
- RSUSR008; By critical combinations of authorizations at transaction start
- RSUSR008_009_NEW; List of users with critical authorizations
- RSUSR020; Profiles by complex selection criteria
- RSUSR030; Authorizations by complex selection criteria
- RSUSR040; Authorization objects by complex selection criteria
- RSUSR070; Roles by complex selection criteria
- RSUSR100; Change Documents for Users
- RSUSR101; Change Documents for Profiles

More detailed analyses can also be started using Reports:

- RSUSR003; Check the Passwords of Users "SAP*" and "DDIC" in All Clients
- RSUSR200; List of Users by Logon Data and Password Change

Another way to read information from the system is a special role concept for auditing (previously done using *Audit Information System*).

The content of the concept has been revised by the auditing and risk management working group of the German-Speaking SAP User Group e.V. (DSAG), in cooperation with customers and partners. This group has considered a wide range of information from external and internal auditors, IT specialists, and consultants who examine SAP applications or whose companies implement SAP software. For more information, see <http://www.sap.com/germany/discsap/revis/index.htm>.



The **Audit Information System (AIS)** is a checking tool for:

- System checks
- Audit (business audit)
- Tax audits

- Internal auditing
- External auditing

The AIS role concept improves the **flow** and **quality of the check**.

The Audit Information System is a tool used by auditors to optimize a system and examine any weak points. The old menu-based version (AUDIT area menu) was replaced by a role-based environment. The role concept used now includes the same collections, structuring, and defaults for standard SAP programs, but is easier to scale. The content is defined using the transaction PFCG (→ Tools → Administration → User Maintenance → Role Administration); the old transaction SECR is no longer used.



Hint:

For more information about the technology behind the program, see SAP Note 451960. 451960.

The roles are constructed to match the flow of the check for different check fields with default control data/evaluation programs for the area “**Business**” and “**System Audit**”. The roles can be found in PFCG with the ID “SAP*AUDITOR*”.

The screenshot shows the SAP Fiori interface. On the left, there is a navigation tree for the Audit Information System (AIS) under the System Audit and Business Audit categories. To the right, a callout box labeled "SAP Note: 451960" points to the "Role Maintenance (PFCG)" screen. The PFCG screen displays a search results table for the role name "SAP*AUDITOR*". The results are categorized into "Single roles" and "Composite roles". Under "Single roles", several roles are listed, including SAP_AUDITOR_A, SAP_AUDITOR_ADMIN, SAP_AUDITOR_ADMIN_A, SAP_AUDITOR_BA_A, SAP_AUDITOR_BA_CFM, and SAP_AUDITOR_BA_GFM_A. A yellow highlight bar is placed over the first result, SAP_AUDITOR_A, which is described as "AIS - Central Authorizations".

Figure 120: Excerpt from the Search Results SAP*AUDITOR* in Role Maintenance

The delivered single roles are split into two groups:

1. Authorization roles
2. Transaction roles

The authorization roles are easy to identify. The role names always end with the suffix “*_A”. This means that all roles that do not end with a simple “A” are the corresponding menu roles.

Accordingly, the following condition applies:

- The authorization roles contain (manual) authorization values, but do not have a menu (such as SAP_AUDITOR_BA_SD_A).

- The transaction roles contain a menu, but do not have any authorization values (such as SAP_AUDITOR_BA_SD).

If you are now asking yourself "Why not use a single role with menu and authorizations?", there is a simple explanation.

What happens when you enter a transaction code in the role menu and then display the authorization data? Correct. Default authorization values are displayed for objects and fields. In many cases, however, there are too many defaults for auditing purposes, since the authorization goes far beyond just "**Display Authorization**". If you were to modify these defaults for your own requirements, the time and effort needed to make changes to the content would be much too high (note: maintenance status "Changed").



Hint:

Finally, note again the following: As an administrator, remain focused on your authorization concept every time you receive a new request from the user departments.

- Avoid an unnecessarily large number of roles or profiles.
- Not every error that is displayed is connected to authorizations.
- When you receive requests, first search for authorizations to see if they have already been created.
- Clarify whether these can be reused.
- Only create something new in response to a requested authorization if nothing suitable already exists.

Unit 6

Exercise 10

Practice System Exercise: Troubleshoot and Administer Aids

Business Example

During your daily work as an administrator, you will regularly search for special settings, authorization values, roles, and other important things. You can find these in the user information system.

Compare the Settings of the Authorizations Between Two Users

You are authorization administrator and are in the consolidation phase after the start of production.

1. Compare the settings of the authorizations between user `GR##-ADM` and user `GR##-FI1`.
Are there differences?

Result

Any authorization values that are not the same are indicated by a red light. Navigate in the detail view by double-clicking and look at the different authorization values.

2. Find out which users may execute transaction `MB1C`.

Result

The resulting list shows the users who may execute transaction `MB1C`.

3. Display all the users assigned to the role `GR##_MM_MAT_ANZ`.

Result

The resulting list shows the users assigned to the role `GR##_MM_MAT_ANZ`.

4. Display an overview of all the users you created (`GR##*`) with their assigned roles.

Result

The resulting list shows the roles that are assigned to users `GR##*`.

Unit 6 Solution 10

Practice System Exercise: Troubleshoot and Administer Aids

Business Example

During your daily work as an administrator, you will regularly search for special settings, authorization values, roles, and other important things. You can find these in the user information system.

Compare the Settings of the Authorizations Between Two Users

You are authorization administrator and are in the consolidation phase after the start of production.

1. Compare the settings of the authorizations between user **GR##-ADM** and user **GR##-FI1**.
Are there differences?

-
- a) Navigate to the User Information System in the SAP Menu.

SAP Menu: → Tools → Administration → User Maintenance → Information System

- b) Expand the structure for the Comparisons node, and select the report - Of Users by double-clicking it.
- c) Enter **GR##-ADM** in the User A field.
- d) Enter **GR##-FI1** in the User B field.
- e) Choose Execute (F8).

Result

Any authorization values that are not the same are indicated by a red light. Navigate in the detail view by double-clicking and look at the different authorization values.

2. Find out which users may execute transaction **MB1C**.

- a) Navigate to the User Information System in the SAP Menu.

SAP Menu: → Tools → Administration → User Maintenance → Information System

- b) Expand the structure for the User → Users by Complex Selection Criteria node, and select the report - By Authorization Values by double-clicking it.
- c) Enter **s_TCODE** in the Authorization Object field.
- d) Choose Input Values.
- e) Enter **MB1C** in the Value field.
- f) Choose Execute (F8).

Result

The resulting list shows the users who may execute transaction MB1C.

3. Display all the users assigned to the role **GR##_MM_MAT_ANZ**.

- a) Navigate to the User Information System in the SAP Menu.

SAP Menu: → Tools → Administration → User Maintenance → Information System

- b) Expand the structure for the *User → Users by Complex Selection Criteria* node, and select the report - *By Role* by double-clicking it.

- c) Enter **GR##_MM_MAT_ANZ** in the *Role* field.

- d) Choose *Execute (F8)*.

Result

The resulting list shows the users assigned to the role **GR##_MM_MAT_ANZ**.

4. Display an overview of all the users you created (**GR##***) with their assigned roles.

- a) Navigate to the User Information System in the SAP Menu.

SAP Menu: → Tools → Administration → User Maintenance → Information System

- b) Expand the structure for the *Roles → Roles by Complex Selection Criteria* node, and select the report - *By User Assignment* by double-clicking it.

- c) Enter **GR##*** in the *User(s)* field.

- d) Choose *Execute (F8)*.

Result

The resulting list shows the roles that are assigned to users **GR##***.



LESSON SUMMARY

You should now be able to:

- Trace and analyze SAP ABAP authorization checks.

Using Traces to Maintain Role Menus and Authorizations

LESSON OVERVIEW

This lesson shows how to use the system trace to maintain the menu and authorization data for roles, and to maintain authorization default values.

Business Example

When creating roles, the most difficult part is to define the transactions needed for this role and to maintain the authorization data. Based on the recorded activities in the system trace, the trace evaluation supports the maintenance of the menu and authorization data for roles.



LESSON OBJECTIVES

After completing this lesson, you will be able to:

- Utilize authorization trace data.

Overview

Based on a trace evaluation, it is easier to maintain the menu and the authorization data of a role, as well as authorization default values for applications.

You can use a system trace or an authorization trace to record authorization checks and their values. This function supports you when maintaining authorization default values (transactions SU22 and SU24) and when maintaining the menu and authorization data for roles (transaction PFCG).

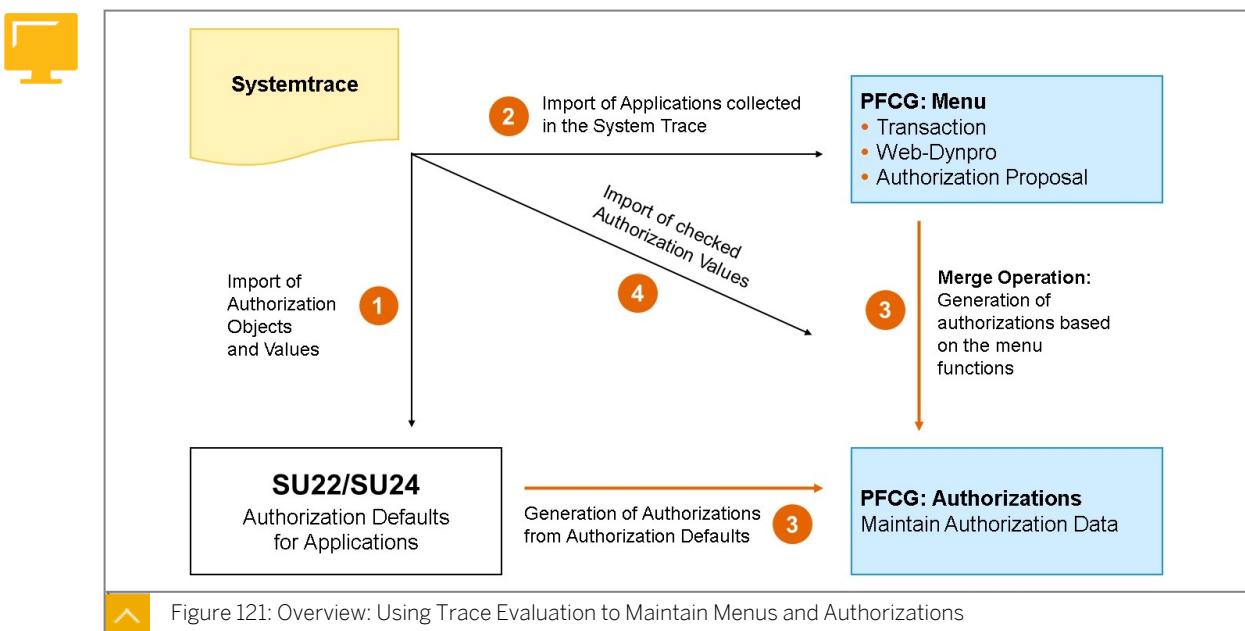
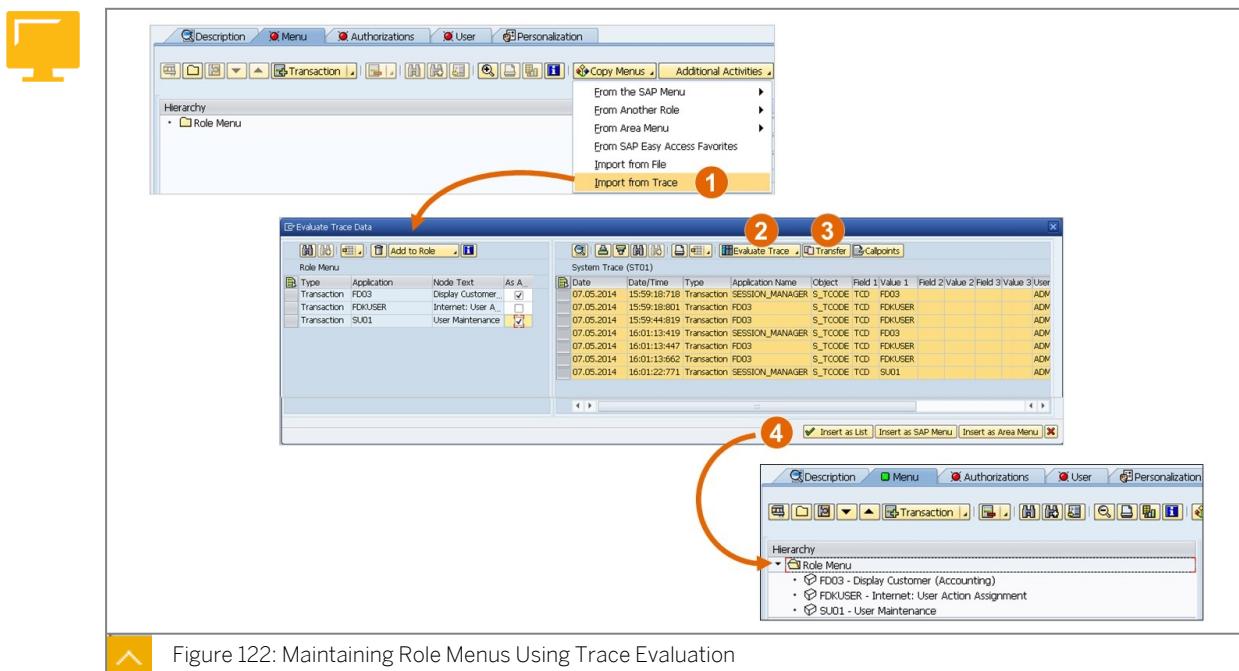


Figure 121: Overview: Using Trace Evaluation to Maintain Menus and Authorizations

Maintaining Role Menus Using Trace Evaluation

In the role maintenance screen (transaction PFCG), the trace evaluation can be used to maintain the role menu. To add applications (transactions, WEB-DYNPROS, and so on) to the role menu, you collect these applications in the system trace (transaction ST01 or STAUTHTRACE). During its runtime, the tracing uses the start authorization checks to log which applications were called. The administrator can then copy these applications to the role menu.

Call transaction PFCG for a role and go to change mode. On the *Menu* tab, choose *Copy Menus* → *Import from Trace*. The upper-left half of the dialog box that the system displays contains the *Information* button. You can obtain all of the information about the use by selecting this button.



Maintaining Authorization Fields Using Trace Evaluation

In Role Maintenance (transaction PFCG), trace evaluation can also be used to maintain the authorization fields. You can complete the authorization fields of a role with values that you collect in the authorization trace or the system trace. To do this, navigate to authorization data maintenance for a role. Expand the authorizations and choose the *Trace* symbol at the authorization level. The system then displays a similar dialog box to that for menu maintenance and you can again choose *Information* to obtain information about the usage.



Hint:

If the trace for your applications occurred on another application server, you must configure an RFC destination for the target system or application server to transfer the trace results to transaction PFCG.

Start Trace Evaluation

Change Role: Authorizations

Role ADM940_DEMO
Maint. 1 unmaint. org. levels, 55 open fields
Status: Changed

Group/Object/Authorization/Field	Maintain...	Value	Text
Object Class AAAA	Standard		Cross-application Authorization Objects
Object Class BC_A	Standard		Basis: Administration
Authorization Object S_SECPOL	Standard		Security Policy
Authorization Object S_USER_AGR	Standard		Authorizations: Role Check
Authorization Object S_USER_AUT	Standard		User Master Maintenance: Authorizations
Authorization Object S_USER_GRP	Standard		User Master Maintenance: User Groups
Authorization Object T-T108036000	Standard		User Master Maintenance: User Groups
CLASS	Standard	01, 02, 03, 05, 06, 78	User group in user master maintenance
ACTVT	Standard		Activity
Authorization Object S_USER_PRO	Standard		User Master Maintenance: Authorization Profile
Authorization Object S_USER_SAS	Standard		User Master Maintenance: System-Specific Assign...
Authorization Object S_USER_SYS	Standard		User Master Maintenance: System for Central User ...
Object Class BC_C	Standard		Basis - Development Environment
Object Class CO	Standard		Controlling
Object Class FI	Standard		Financial Accounting
Object Class HR	Standard		Human Resources
Object Class IS	Standard		Industry Solutions
Object Class MM_E	Standard		Materials Management: Purchasing
Object Class MM_G	Standard		Materials Management: Master Data
Object Class PS	Standard		Project System
Object Class SD	Standard		Sales and Distribution

Figure 123: Maintaining Authorization Fields Using Trace Evaluation (1)

Evaluate Trace Data

Authorization Object: S_USER_GRP | User Master Maintenance: User Groups

Authorization: T-ZE55213500

Evaluate Trace Data

Authorization Object: F_KNA1_BUK | Customer: Authorization for Company Codes

Authorization: T-ZE55213500

Figure 124: Maintaining Authorization Fields Using Trace Evaluation (2)

Maintaining Authorization Default Values Using Trace Evaluation

You can also complete the authorization default values with values that you collect in the authorization trace or the system trace. Call transaction SU24 and display the authorization data for an application. Choose the *Trace* function.

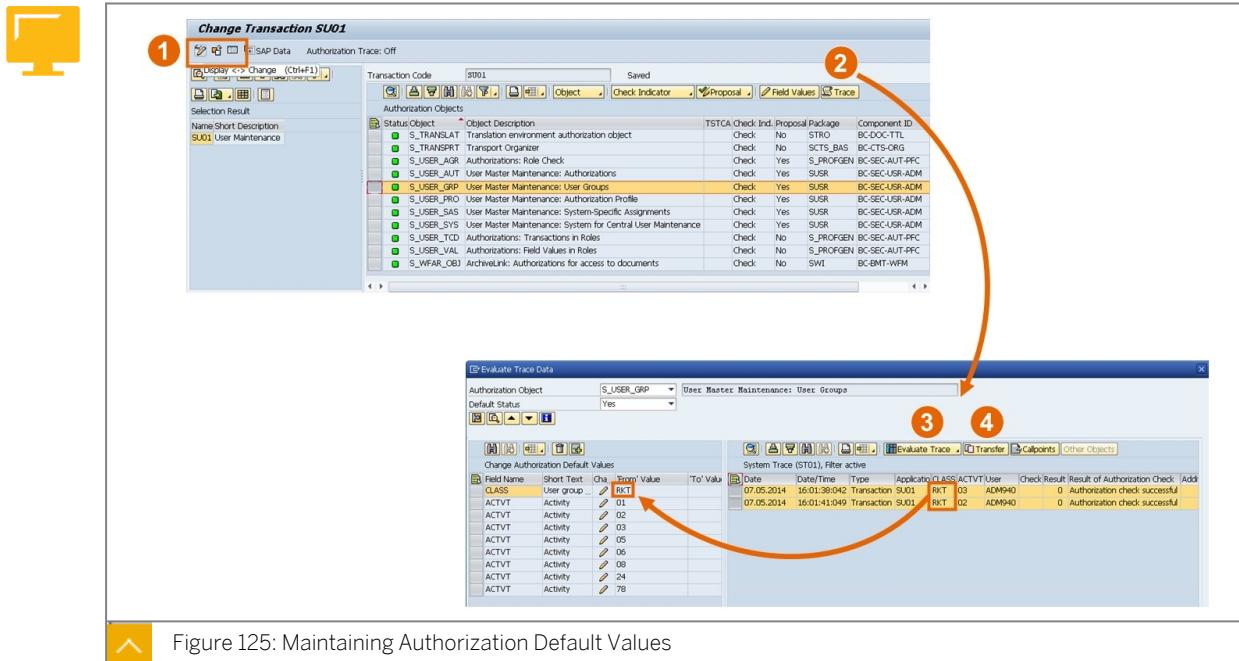


Figure 125: Maintaining Authorization Default Values

Unit 6

Exercise 11

Practice System Exercise: Use Authorization Trace

Business Example

During your daily work as an administrator, you use the system trace for authorization checks for evaluation of successful and unsuccessful authorization checks and for maintenance of role menus and authorization values.

As a prerequisite, the instructor must start the System Trace for Authorization Checks, transaction STAUTHTRACE. This is done as the first task. The participants complete the exercise as the second task.

Task 1: Enable the System Trace for Authorization Checks. (Done by Your Instructor)

As a prerequisite, the instructor must start the System Trace for Authorization Checks (transaction STAUTHTRACE) for the GR* users.

1. Start the system trace for authorization checks and activate the trace for GR* users.

Task 2: Use the System Trace for Authorization Checks to Analyze Unsuccessful Authorization Checks

Log on to the system as user GR##-MM1. Start transactions MM03 and MM19 and display the accounting view of material P605-100 in plant 1010 and 1030.

1. Log on to the system as user GR##-MM1.
2. Start transactions MM03 and MM19 and display the accounting view of material P605-100 in plant 1010 and 1030.
3. Log on to the system as user ADM940-## and evaluate the system trace for authorization checks.

Which authorization objects are checked?

Which field values are checked for authorization object M_MATE_WRK?

Are the authorization checks of M_MATE_WRK successful?

Task 3: Create a Role Based on the Result of the System Trace for Authorization Checks

Create a role GR##_TRACE. Maintain the role menu and the authorization values using the system trace for authorization checks generated in task 1.

1. Start the role maintenance transaction and create the role GR##_TRACE. Enter a short description, and save.

2. Create the role menu using the system trace for authorization checks generated in the previous task.

Result

The transactions MM03 and MM19 are added to the role menu.

3. Maintain the authorization values for the organizational levels.

Define the organizational levels:

- Company code: 1010,
- Warehouse number/complex: *
- Sales organization: 0001
- Distribution Channel: *
- Plant: 1010, 1030

4. Maintain the authorization values for authorization object M_MATE_STA using the system trace for authorization checks generated in task 1.

5. Generate the authorization profile for your role. Accept the proposed profile name.

Task 4: Deactivate the System Trace for Authorization Checks (Done by Your Instructor)

At the end of this exercise, the instructor must deactivate the System Trace for Authorization Checks (transaction STAUTHTRACE) for GR* users.

1. Start the system trace for authorization checks and activate the trace for GR* users.

Unit 6 Solution 11

Practice System Exercise: Use Authorization Trace

Business Example

During your daily work as an administrator, you use the system trace for authorization checks for evaluation of successful and unsuccessful authorization checks and for maintenance of role menus and authorization values.

As a prerequisite, the instructor must start the System Trace for Authorization Checks, transaction STAUTHTRACE. This is done as the first task. The participants complete the exercise as the second task.

Task 1: Enable the System Trace for Authorization Checks. (Done by Your Instructor)
As a prerequisite, the instructor must start the System Trace for Authorization Checks (transaction STAUTHTRACE) for the GR* users.

1. Start the system trace for authorization checks and activate the trace for GR* users.
 - a) Start transaction STAUTHTRACE.
 - b) Enter **GR*** in the *Trace for user only* field of the *Trace Options* screen area.
 - c) Choose *Activate Trace (F6)*.

Task 2: Use the System Trace for Authorization Checks to Analyze Unsuccessful Authorization Checks

Log on to the system as user **GR##-MM1**. Start transactions **MM03** and **MM19** and display the accounting view of material **P605-100** in plant **1010** and **1030**.

1. Log on to the system as user **GR##-MM1**.
 - a) Start *SAP Logon*.
 - b) Select system **T41** and choose *Log On*.
 - c) Enter the user name **GR##-MM1** in the *User* field.
 - d) Enter the password given in exercise 6 in the *Password* field.
 - e) Choose *Continue (Enter)*.
2. Start transactions **MM03** and **MM19** and display the accounting view of material **P605-100** in plant **1010** and **1030**.
 - a) Start transaction **MM03** from the *User menu*.
 - b) In the *Material* field, enter the material ID **P605-100**.
 - c) Choose *Select view(s)*.

d) Choose the *Accounting 1* view.

e) Choose *Continue*.

f) In the *Plant* field, enter **1010**.

g) Choose *Continue (Enter)*.

The accounting view of material **P605-100** for plant 1010 is shown.

h) Choose *Back (F3)*.

i) In the *Material* field, enter the material ID **P605-100**.

j) Choose *Select view(s)*.

k) Choose the *Accounting 1* view.

l) Choose *Continue*.

m) In the *Plant* field, enter now **1030**.

n) Choose *Continue (Enter)*.

An error message appears: No authorization to display data for plant 1030.

o) Choose *Confirm (Enter)*.

p) Choose *Cancel (F12)*.

q) Start transaction **MM19** from the *User menu*.

r) In the *Material* field, enter the material ID **P605-100**.

s) Choose *Select view(s)*.

t) Choose the *Accounting 1* view.

u) Choose *Continue*.

v) In the *Plant* field, enter **1010**.

w) Choose *Continue (Enter)*.

The material at key date **P605-100** for plant 1010 is shown.

x) Choose *Confirm (Enter)*.

y) Choose *Cancel (F12)*.

3. Log on to the system as user **ADM940-##** and evaluate the system trace for authorization checks.

Which authorization objects are checked?

Which field values are checked for authorization object **M_MATE_WRK**?

Are the authorization checks of **M_MATE_WRK** successful?

- a) Log on to the system as user ADM940-##.
- b) Start transaction STAUTHTRACE.
- c) In the *Restrictions for the Evaluation* screen area, in the *User* field, enter **GR##-MM1**.
- d) Choose *Evaluate Trace (F8)* to evaluate the trace.
If no result is displayed, please adjust the time interval so that it fits your time zone.
- e) The authorization objects that are checked are shown in the *Objects* column.
- f) The field values that are checked are shown in the columns *Field#* and *Value#*.
The following field values are checked for authorization object M_MATE_WRK:
Field1: ACTVT _____ Value1: 03
Field2: WERKS _____ Value1: 1010, 1030

Result

The authorization check of M_MATE_WRK (ACTVT = 03; WERKS = 1010) was successful.

The authorization check of M_MATE_WRK (ACTVT = 03; WERKS = 1030) was not successful.

An unsuccessful authorization check is shown in the columns *Result* and *Result of Authorization Check*.

Task 3: Create a Role Based on the Result of the System Trace for Authorization Checks

Create a role GR##_TRACE. Maintain the role menu and the authorization values using the system trace for authorization checks generated in task 1.

1. Start the role maintenance transaction and create the role GR##_TRACE. Enter a short description, and save.
 - a) SAP Menu:
Tools → Administration → User Maintenance → Role Administration → Roles (transaction code PFCG).
 - b) Enter the name for the role **GR##_TRACE** in the *Role* field.
 - c) Choose *Create Single Role*.
 - d) Enter description **Trace** in the *Description* field.
 - e) Then choose *Save (Ctrl+S)* to save your role.
2. Create the role menu using the system trace for authorization checks generated in the previous task.
 - a) Go to the *Menu* tab.
 - b) Choose *From Menus → Import from Trace*.
 - c) Choose *Evaluate Trace → System Trace (STAUTHTRACE) → Local* in the *Evaluate Trace Data* window.
 - d) Enter **GR##-MM1** in the *Trace for user only* field.
 - e) Choose *Evaluate* on the *System Trace* window.
If no result is displayed, please adjust the time interval so that it fits your time zone.

- f) In the *Value1* field, select transactions MM03 and MM19 of the *System Trace* and choose *Transfer*.
- g) Choose *Insert as List*.
- h) Choose *Save*.

Result

The transactions MM03 and MM19 are added to the role menu.

3. Maintain the authorization values for the organizational levels.

Define the organizational levels:

- Company code: 1010,
- Warehouse number/complex: *
- Sales organization: 0001
- Distribution Channel: *
- Plant: 1010, 1030

- a) Go to the *Authorizations* tab page.

- b) Choose *Change Authorization Data*.

- c) Enter the following values in the *Define Organizational Levels* window:

When you maintain organizational levels, you usually only see those lines where values have been assigned. If an organizational level field has not yet been maintained, only one line is displayed. You can display multiple lines by choosing the *More Values* button.

- Company code: **1010**
- Warehouse number/complex: *
- Sales organization: **0001**
- Distribution Channel: *
- Plant: **1010, 1030**

- d) Choose *Save (Ctrl+S)* to save the authorization values for the organizational levels.

4. Maintain the authorization values for authorization object M_MATE_STA using the system trace for authorization checks generated in task 1.

- a) Choose the *Evaluate Trace Data (Ctrl+F5)* icon on the *Change Role: Authorizations* screen.
- b) On the *Evaluate Trace Data* window, choose authorization object **M_MATE_STA**.
- c) On the *Evaluate Trace Data* window, choose *Evaluate Trace → System Trace (STAUTHTRACE) → Local*.
- d) Enter **GR##-MM1** in the Trace for *user only* field.
- e) Choose *Evaluate* on the *System Trace* window.
- f) Select all values in the *STADM* field of the *System Trace*.
- g) Choose *Transfer*.

- h) Choose *Continue (Enter)*.
 - i) Check the field values of the authorization object M_MATE_STA.
5. Generate the authorization profile for your role. Accept the proposed profile name.
- a) Choose the *Generate* icon.
 - b) Press *Generate* again or in the *Assign Profile Name for Generated Authorization Profile* window, accept the proposed profile name and choose *Execute (Enter)*.
 - c) Choose *Back (F3)* to return to the *Change Roles* screen.

Task 4: Deactivate the System Trace for Authorization Checks (Done by Your Instructor)

At the end of this exercise, the instructor must deactivate the System Trace for Authorization Checks (transaction STAUTHTRACE) for GR* users.

1. Start the system trace for authorization checks and activate the trace for GR* users.
 - a) Start transaction STAUTHTRACE.
 - b) Choose *Deactivate Trace (F7)*.



LESSON SUMMARY

You should now be able to:

- Utilize authorization trace data.

Learning Assessment

1. For which of the following checks is the Auditing Information Systems (AIS) used?

Choose the correct answers.

- A Authorization checks
- B Audit (business audit)
- C Tax audits
- D Internal auditing

2. System trace can be used to maintain the menu and authorization data for roles and authorization default values.

Determine whether this statement is true or false.

- True
- False

Learning Assessment - Answers

1. For which of the following checks is the Auditing Information Systems (AIS) used?

Choose the correct answers.

- A Authorization checks
- B Audit (business audit)
- C Tax audits
- D Internal auditing

The AIS provides a framework for conducting both business and system audits.

2. System trace can be used to maintain the menu and authorization data for roles and authorization default values.

Determine whether this statement is true or false.

- True
- False

System trace can be used to maintain the menu and authorization data for roles and authorization default values.

Lesson 1

Transporting Authorization Components	284
Exercise 12: Practice System Exercise: Transport Authorization Components	291

UNIT OBJECTIVES

- Transport the SAP business roles and data.

Transporting Authorization Components

LESSON OVERVIEW

This lesson will provide an overview about how to transport user master records, roles, and check indicators.

Business Example

Authorization components such as roles should be created and tested in development systems, and not in production systems. At the end of the test phase they are transported from the development systems to the production system. The transport behavior varies depending on various profile parameters. It is also important whether or not CUA is implemented in the system landscape.



LESSON OBJECTIVES

After completing this lesson, you will be able to:

- Transport the SAP business roles and data.

Options for Transporting Authorization Components

User data and authorization data must be exchanged in system landscapes with multiple SAP systems. The data is either exchanged between different clients of an SAP system or between clients of different SAP systems.

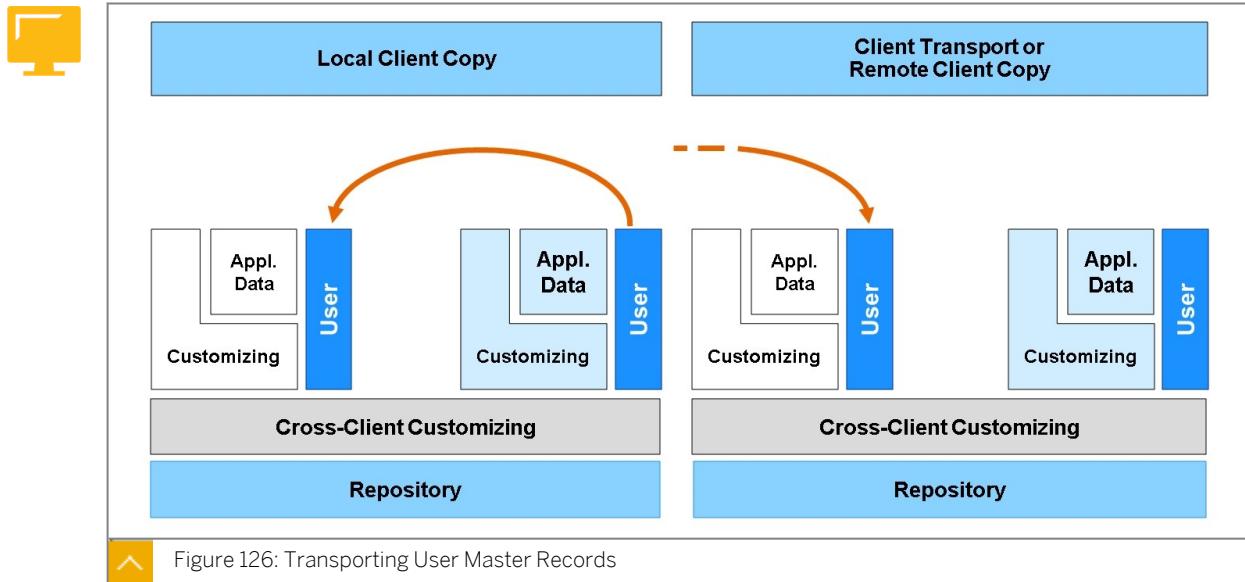
In principle, the SAP authorization concept differentiates between the transport components described here.

Which Authorization Components Can Be Transported?



- User master records
- Roles
- Authorization profiles
- Authorization default values

Authorization profiles can be transported together with their roles. Working with authorization profiles without an assigned role should remain the exception. The transport connection of transaction SU02 for maintaining authorization profiles is only mentioned here for completeness and is not discussed further.



User master records can be maintained centrally in one client of a system. If a new client is built, it can initially be filled with the user master records of the maintenance client. Client management transactions can be found under the menu path:
Tools → Administration → Administration → Client Management →

Local Client Copy

If a new client is filled with data from another client of the same SAP system, this copy process is called a local client copy. Since the data of both clients is stored in the same database, it is not necessary to transport the data using the network or the operating system. The local client copy is started with transaction SCC1 or in the client management with ... → *Client Copy → Local Copy*.



Hint:

Schedule the transport as a background job during the night. This helps to avoid data inconsistencies.

Client Copy Between Systems

If a new client is filled with data from another SAP system, it can be copied with a client transport (1) or as a remote client copy (2).

1. The client transport exchanges its data with a data export at the operating system level. Transaction SCC8 can be started in the client management by choosing ... → *Client Transport → Client Export*.
2. In a remote client copy, the data is copied over the network and not as a file. Transaction SCC9 can be found in the client management under ... → *Client Copy → Remote Copy*.



Caution:

Prior to each client copy, the data areas to be copied are deleted in the target client.

Only the **complete** user master, and not individual users, can be copied. Roles are also copied when you copy Customizing data.

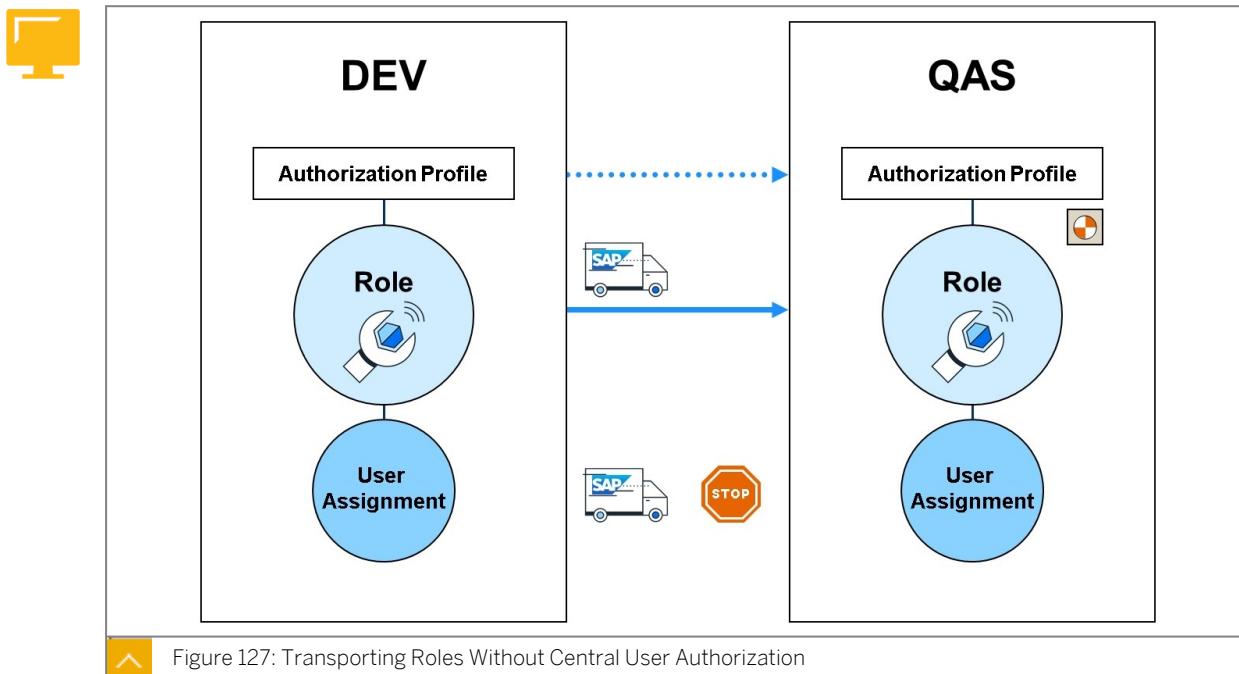
**Hint:**

User master records can also be distributed using Central User Administration. In this case, it is possible to distribute individual users.

Transport roles: With and without profile information, with and without user assignments, in a CUA landscape or without CUA

Roles Without Central User Administration

SAP roles are available in all systems and are not transported. If roles that you developed yourself are to be transported between clients or SAP systems, you must differentiate between situations where Central User Administration is implemented, and those in which it is not.



If you are **not** using Central User Administration, roles can be transported with user assignments. The transport is started with a Customizing request, which you can create in Role Maintenance by choosing *Utilities* → *Mass Transport*. The transport request is either imported into another SAP system with the Transport Management System or into another client of the same SAP system using transaction *scc1*. The user master records of the target client must be compared after the import. You can do this manually from Role Maintenance by choosing *Utilities* → *Mass Comparison* or periodically in the background (*PFCG_TIME_DEPENDENCY*). You can also create the background job there.

By default, authorization profiles are transported with roles. If this is not desired, you must prevent the data export in the source system with the control entry (*PROFILE_TRANSPORT:=NO*) in table *PRGN_CUST*. The table entry can be made using maintenance transaction *SM30*.

**Caution:**

If the Customizing entry “NO” is set, you must generate the profiles in the target system using a mass generation before performing a user master comparison. Transaction code SUPC.

You can start the mass generation in Role Maintenance by choosing *Utilities → Mass Generation*.

Transporting Roles with User Assignment

If you do not want to transport the user assignments to roles, you can protect the target system with an import lock. To do this, the control table *PRGN_CUST* must contain the entry (*USER_REL_IMPORT:=NO*).

**Caution:**

If you transport user assignments, the entire user assignment for the role in the target system is replaced. Existing connections to this role are removed.

You must also perform a user master comparison for all affected roles in the target system after the import.

Roles with Central User Administration

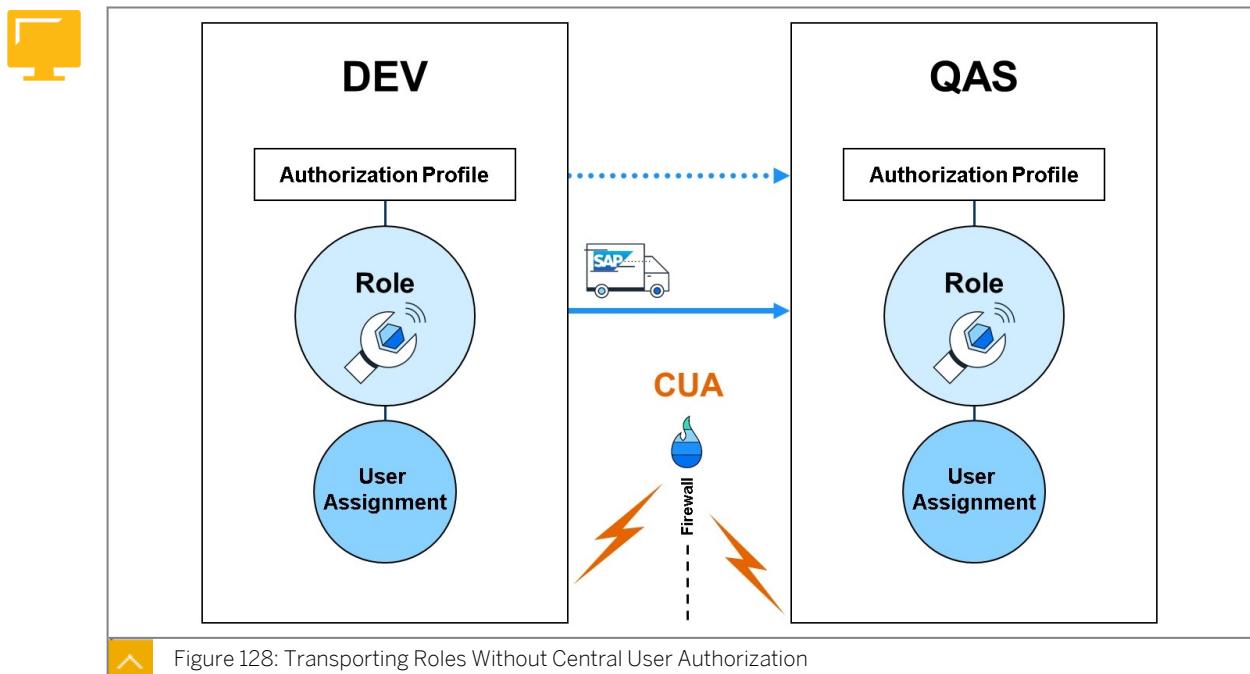


Figure 128: Transporting Roles Without Central User Authorization

Roles must also exist in the systems in which they are assigned to users within the Central User Administration. If systems are assigned to a Central User Administration, roles must be transported without user assignment since these assignments are made in and distributed from the central system. If user assignments were transported, there would be a temporary inconsistency between the actual state of the system and its subsystems. The imported assignments are deleted without being copied to the central system the next time there is a distribution. For security reasons, the import lock for user assignments therefore should be

set for systems within the Central User Administration ("SM30", *PRGN_CUST*, *USER_REL_IMPORT := NO*).

A Customizing request for roles is created analogously to the scenario without Central User Administration. The authorization profiles are also transported in the same way.

Uploading and Downloading Roles

Normally, it is only possible to exchange data with transport requests between SAP systems with the same release status. For example, if roles have to be exchanged within the Central User Administration across releases, this can be done by downloading or uploading roles, if necessary.

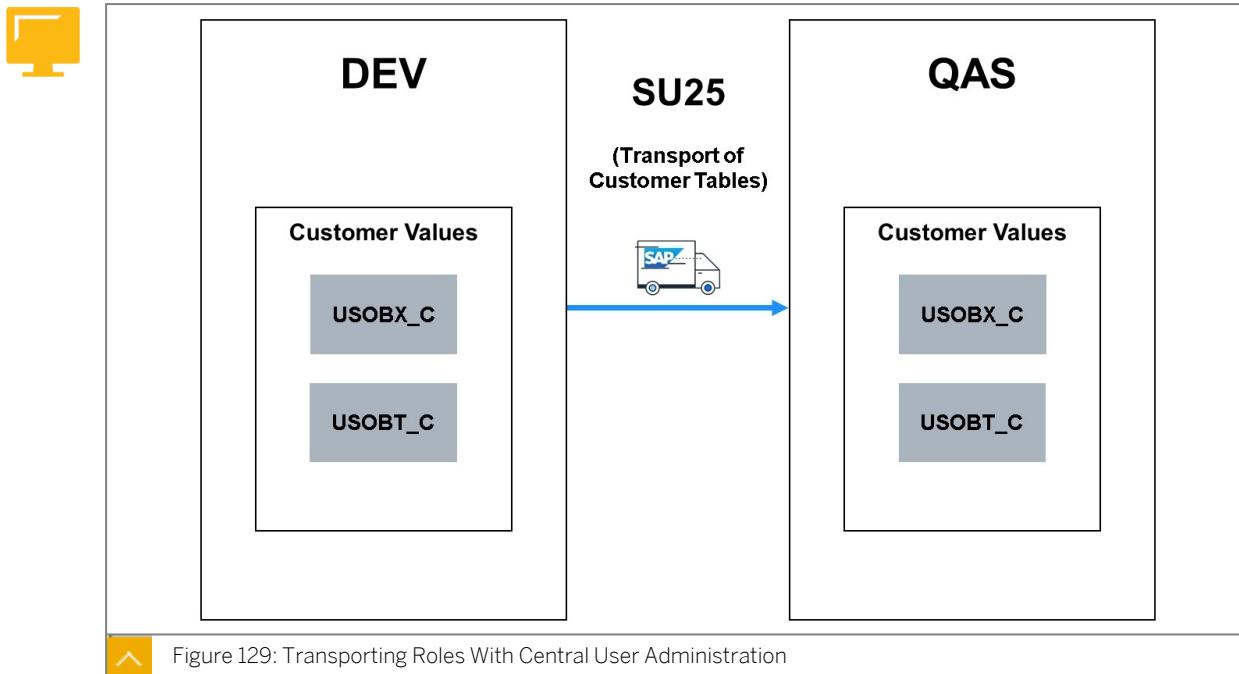


Hint:

When you download the data, it is all stored in a local file, with the exception of the generated authorization profiles and the user assignments.

After an upload, the role may have to be edited and generated. You can choose to upload or download in Role Maintenance by choosing *Role → Upload/Download*. You can save multiple roles in a local file at the same time by choosing *Utilities → Mass download*.

Transporting the Authorization Default Values



The customer tables *USOBX_C* and *USOBT_C*, which control the behavior of Role Maintenance, must be filled in each system in which Role Maintenance is used.

If these tables are adjusted to the customer's needs, they can then be transported as a whole. This means that you transport all the settings for the authorization checks, authorization default values, and the corresponding field values.

1. The transport link can be found under step 3 of transaction SU25, which must be executed when you activate Role Maintenance.

2. You can use transaction SU24 to change individual authorization default values. In this case, the system automatically and immediately creates a transport request.

In both cases, a transport request is transported and distributed to other SAP systems in the context of the Transport Management System.



Caution:

During the transport, all of the authorization default values and field values in the target system are replaced.

Unit 7

Exercise 12

Practice System Exercise: Transport Authorization Components

Business Example

On a daily basis, authorizations are created or changed or default values of the Role Maintenance are adjusted. These settings must be transported. This exercise addresses and runs through a few examples on the topic of transport.

Task 1: Transport of User Assignments with the Roles

You want to ensure that any user assignment that exists is **never** evaluated in your system by a transport request for a role.

1. Where must you set the import lock?

Result

You must use transaction SM30 to set the lock in table PRGN_CUST with the entry *user_rel_import := NO*.

2. What would happen if the transport request had user assignments and no import lock had been set up?
-
-
-
-

Result

If you transport the user assignments with the roles, the user assignments for the roles in the target system are completely replaced by those from the transport request.



Caution:

As part of this, existing connections to users that are not contained in the transport request are also deleted.

Task 2: Create a Transport Request for a Specified Role

Create a transport request for the role *ADM940_SD_SALES*.

1. Open the role maintenance transaction and select the role *ADM940_SD_SALES*. Create a transport request for the specified role (without user assignment). To do this, use the Own Requests button and choose the request from which your user is assigned.

Practice System Exercise: Transport Authorization Components

Business Example

On a daily basis, authorizations are created or changed or default values of the Role Maintenance are adjusted. These settings must be transported. This exercise addresses and runs through a few examples on the topic of transport.

Task 1: Transport of User Assignments with the Roles

You want to ensure that any user assignment that exists is **never** evaluated in your system by a transport request for a role.

1. Where must you set the import lock?

Result

You must use transaction SM30 to set the lock in table PRGN_CUST with the entry *user_rel_import := NO*.

2. What would happen if the transport request had user assignments and no import lock had been set up?
-
-
-
-
-

Result

If you transport the user assignments with the roles, the user assignments for the roles in the target system are completely replaced by those from the transport request.



Caution:

As part of this, existing connections to users that are not contained in the transport request are also deleted.

Task 2: Create a Transport Request for a Specified Role

Create a transport request for the role *ADM940_SD_SALES*.

1. Open the role maintenance transaction and select the role *ADM940_SD_SALES*. Create a transport request for the specified role (without user assignment). To do this, use the *Own Requests* button and choose the request from which your user is assigned.

a) SAP Menu:

Tools → Administration → User Maintenance → Role Administration → Roles
(transaction code PFCG).

- b) Enter the name for the role **ADM940_SD_SALES** in the *Role* field.
- c) Choose *Transport Role* (*Ctrl+Shift+F9*).
- d) Which objects can be transported with the role during the transport?

- e) Select *Generated Profiles of Single Roles*.
- f) Choose *Execute* (*F8*).
- g) Choose the *Own Requests* (*F7*) icon.
- h) Choose the *Create Request* (*F6*) icon.
- i) Enter **GR## Role Transport Test** in the *Short Description* icon.
- j) Choose *Save (Enter)*.
- k) Select the transport request in the list.
- l) Choose *Choose* (*F2*).
- m) Choose *Continue (Enter)*.
- n) Choose *Back* (*F3*) twice to return to the *Role Maintenance* screen.



LESSON SUMMARY

You should now be able to:

- Transport the SAP business roles and data.

Learning Assessment

1. Which of the following authorization components can be transported?

Choose the correct answers.

- A User master records
- B Roles
- C Authorization profiles
- D Authorization default values

Learning Assessment - Answers

1. Which of the following authorization components can be transported?

Choose the correct answers.

- A User master records
- B Roles
- C Authorization profiles
- D Authorization default values

All the options are correct.

Lesson 1

Working with the Central User Administration

299

UNIT OBJECTIVES

- Manage SAP central user administration.

Unit 8

Lesson 1

Working with the Central User Administration

LESSON OVERVIEW

This lesson provides you with information about the principles of Central User Administration to help you decide whether to implement Central User Administration.

Business Example

In complex system landscapes, users in multiple systems must be managed locally. These users work in different systems with different authorizations. In the Central User Administration, the required management functions can be carried out **centrally** on one system.



LESSON OBJECTIVES

After completing this lesson, you will be able to:

- Manage SAP central user administration.

Introduction to Central User Administration

In complex system landscapes with multiple systems and clients, the administration effort required to compare and update user master records is very high. Employees join the company, leave, or change jobs within the company. Individual users usually need to access various systems and clients to perform their work, and therefore require multiple users.



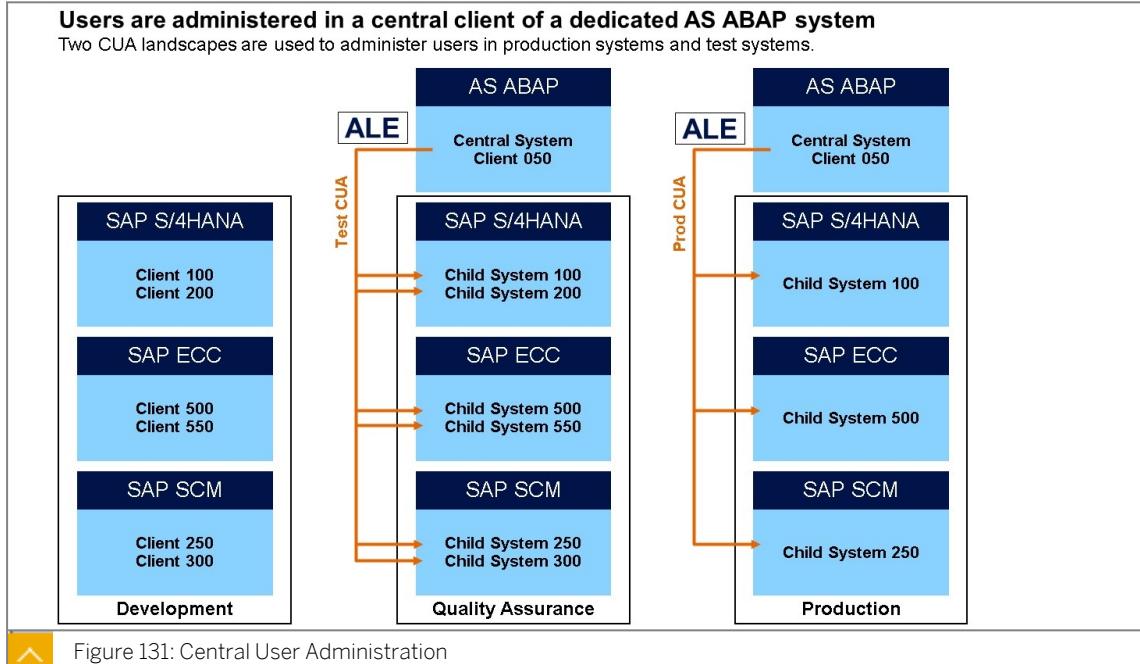
The users are administered individually in each client



Figure 130: Decentralized User Administration

Since user master records are client-specific, they must be administered in each client of each and every system. For example, if you want to create a new user, you must create it manually in all the clients of all the SAP systems in which it should be valid.

User master records can be managed centrally in one client of a system. If a new client is built as a copy of another client, the new client can initially be filled with the user master records of that client. During this copy, the roles of the original client are copied together with the user master records. However, you cannot copy individual users selectively. Also, the user master records cannot be automatically synchronized sequentially.



The essential feature of the Central User Administration is the definition of a **central client** in a selected system. It can be used to manage the user master records for all the clients of the system landscape. For example, you can define which roles should be assigned to which users in which systems. This greatly reduces the administrative cost for authorization administration.



Hint:

You can decide individually for each user which systems that user should be able to log on to.



Caution:

Central User Administration does not mean that every user must exist in each system of the system landscape. In particular, users of child systems do not necessarily need to exist in the central system.

Which user master record data is administered centrally or only locally can be individually set. Local administration by a user or by an administrator could be useful for certain data of the user master record.

The authorization data is exchanged based on the ALE concept. ALE means Application Link Enabling and permits you to build and operate distributed SAP links. It includes a business-

controlled message exchange between loosely linked SAP systems. The application is integrated with asynchronous communication.



Hint:

In the rest of this lesson, the central client will be referred to as the “central system”. A “child system” is a client of an SAP system included in Central User Administration.

The following data can be distributed with Central User Administration.

Data Distributable Using Central User Administration



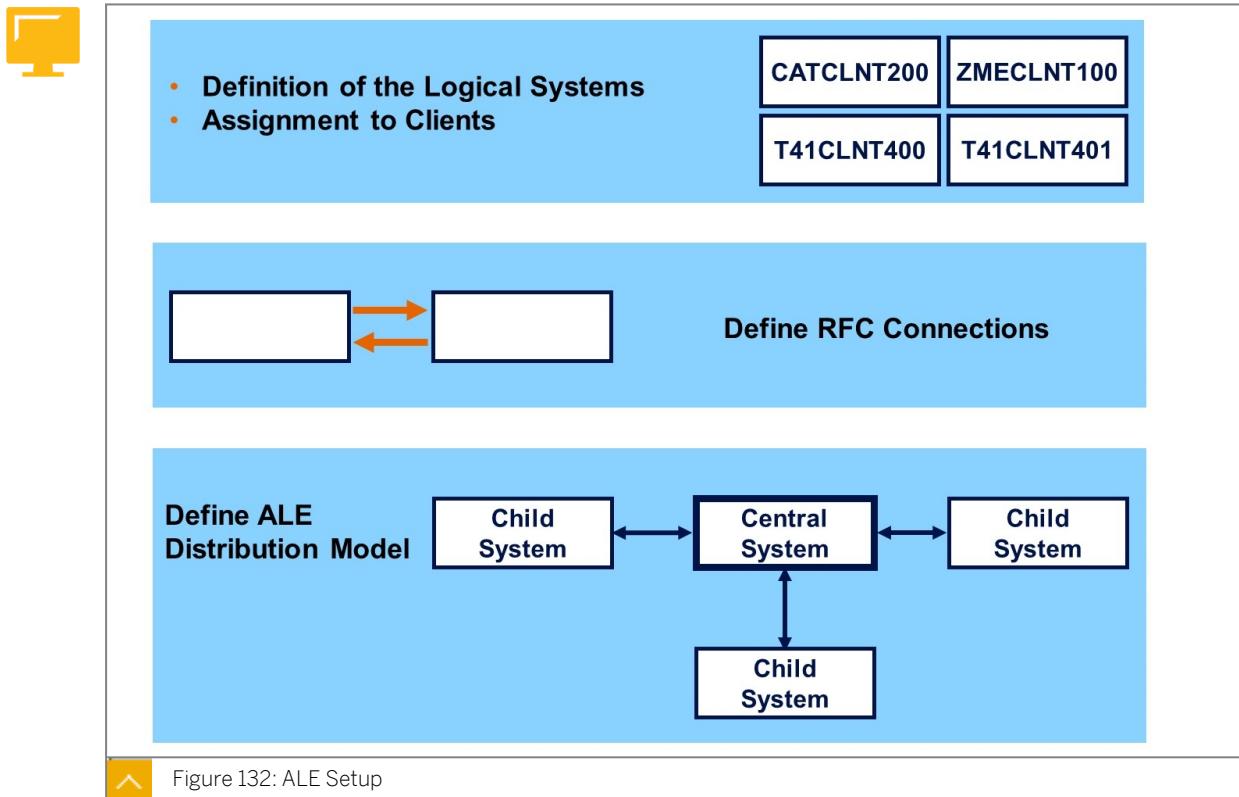
- User master record data, such as the address, logon data, user defaults, and user parameters.
- The **assignment** of the user to roles or profiles for each child system. The advantage of administering assignments centrally is that you no longer need to log on to each system to make system-specific assignments of roles and profiles; it is all managed at one location in the central system.
- The initial password. When you create a new user, the initial password is distributed to the child systems as a default value. The passwords are distributed in coded form.
- The lock status of a user. In addition to the locks caused by incorrect logon that already existed in previous releases or those set manually by the local administrator, there is now also a new “global lock”. This applies to all of the child systems in which the user is defined and can be canceled in the central system or locally if required.



Hint:

Although roles and authorization profiles can be transported, they are normally managed in the child systems and not centrally. Different Customizing settings and releases in the child systems normally make it necessary to adjust the roles individually. Therefore, Central User Administration transfers only an assignment of the users to roles and profiles, but not the authorization values that are contained in the authorization profiles.

Setting Up CUA



Communication partners are addressed in the ALE scenario with aliases, which are called *logical systems*.

The central system itself and every sub-system is defined by name in the central system in the IMG activity → *Name Logical System*.

You can call this in two ways:

- In the transaction **SALE** by choosing the menu path *IDoc Interface / Application Link Enabling (ALE)* → *Basic Settings* → *Logical Systems* → *Define Logical System*
- By calling transaction **BD54**

In the central system, **all** child systems and the central system are specified. In the child systems, the child system itself, and the central system are defined. The logical system names are assigned to the client definitions in the corresponding systems in transaction **SCC4**. Each logical system therefore identifies a certain client of an SAP system.



Caution:

You have to name the central system in the central system itself.

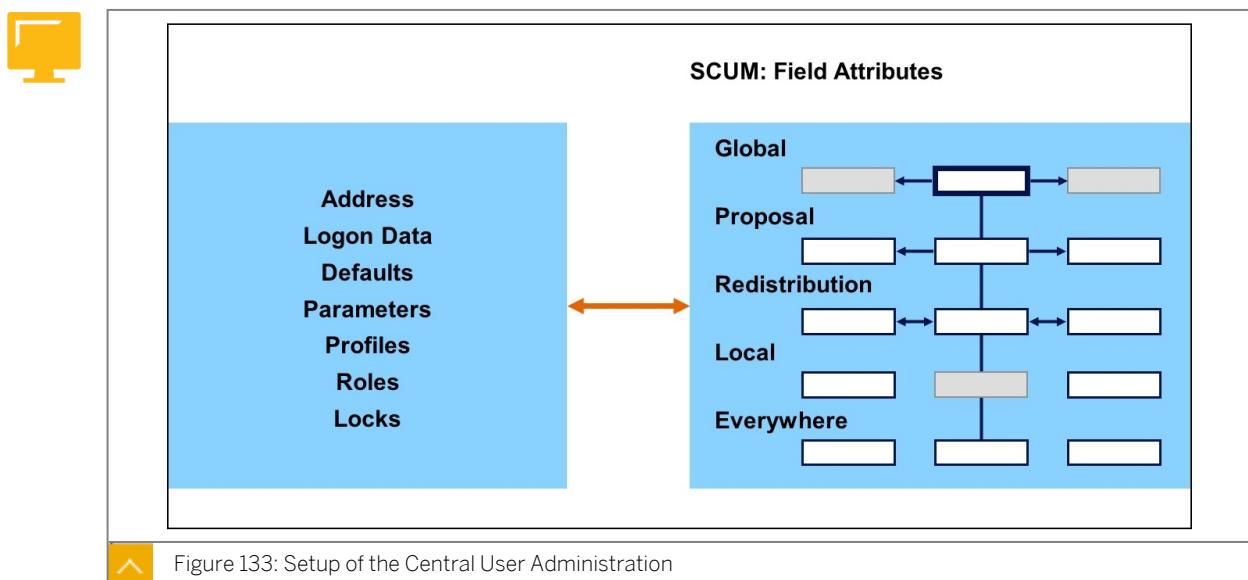
Communication between the central system and the child systems at the network level is performed using Remote Function Calls (RFCs). The technical definition of the connection is maintained in transaction **SM59**. All the connections to all child systems must be created in the central system, and the connection to the central system must be maintained in the child systems. The RFC connection names must be the same as the names of the logical systems.

The communication must be performed using communication users with certain RFC authorizations for CUA in the relevant system.

What data is sent from where to where is defined in the ALE distribution model. User and company data is exchanged within Central User Administration. The distribution model is created and generated in, and distributed from transaction BD64 in the central system. It only needs to be generated in all of the child systems.

Central User Administration is then activated centrally in transaction SCUA.

You can find a detailed description of Central User Administration in the SAP online documentation. SAP course ADM103, "System Administration II for SAP S/4HANA and SAP Business Suite", deals with the technical implementation.



You can define whether each individual component of a user master record should be administered in the central system or locally in the child systems. This is defined within transaction SCUM in the central system. A *field attribute* can be defined for each input field of the user maintenance transaction SU01.

- If a field of the user maintenance transaction has field attribute **global**, data for this field can only be maintained in the central system. The data is automatically distributed to child systems when it is saved. Such fields are in display mode in the user maintenance transaction of the child systems, that is, you cannot change these fields.
- If you use field attribute **default**, a default value, which is automatically distributed to the child systems when it is saved, can be maintained when you create a user in the central system. After distribution, the data is only maintained locally in the child systems and cannot be returned.
- If you use field attribute **Redistribution**, the data can be maintained in both the central system and the child systems. If a change is made to the child system, the data is returned to the central system and passed on to other existing child systems from there.
- The field attribute **local** means that the data for the corresponding field can only be administered locally in the child systems. When fields of this type are changed in the central system, this data is not distributed to the child systems.

- The field attributed **everywhere** is used if you can want to be able to change data locally and globally. In the case of local maintenance, however, no redistribution takes place.

**Caution:**

The attribute **everywhere** is only used for user locks, not for other settings in transaction SU01.

Integration of Existing Systems

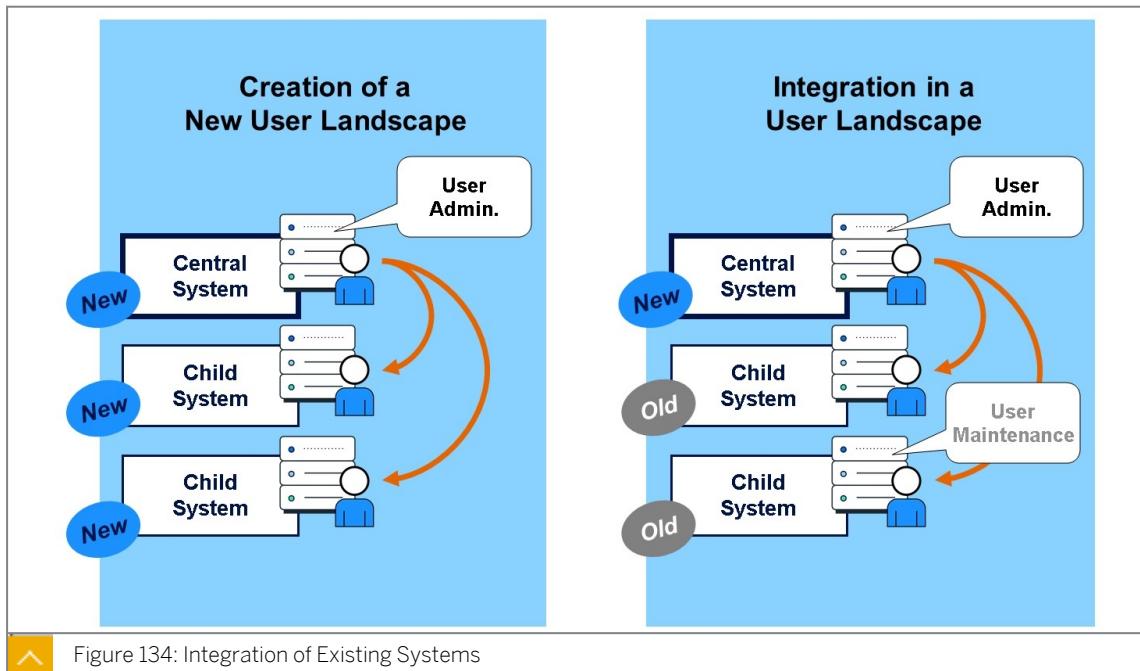


Figure 134: Integration of Existing Systems

The integration of existing systems in the central user administration depends on whether there is a complete new installation of the system infrastructure, or the user master records are built completely anew in all existing systems, or whether the central user administration is set up at a time at which there are already users in the relevant systems that must be migrated to the central user administration.

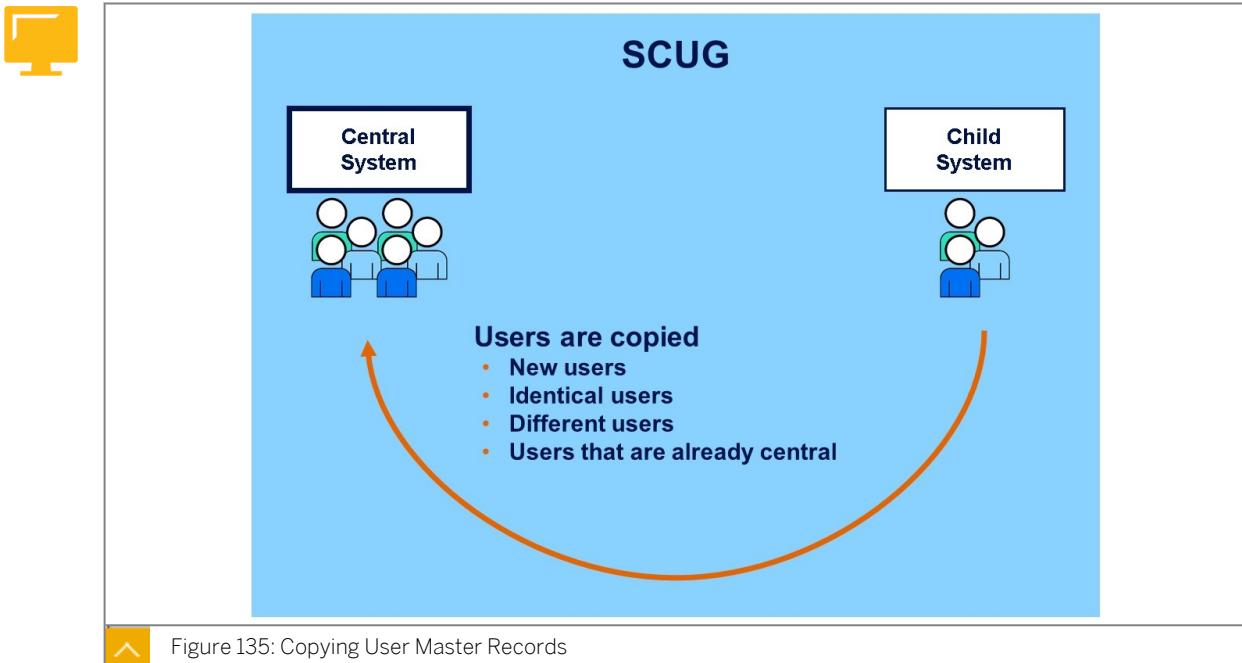
For a new installation, all the users are newly created in the central system and distributed by Central User Administration. Distribution ensures that the user data is consistent in all systems.

If Central User Administration is installed at a later time, the existing users of the system infrastructure must be copied to the central system. This procedure is called migration. The user identifications copied from the child systems must be compared and adjusted in the central system.

Roles that were already developed and assigned to users in the old systems must be identified by name in the central system. Only then can the users be assigned centrally to roles. The old assignment between users and roles can be copied if required.

**Hint:**

The authorization-specific contents of the roles remain in the old systems and are still maintained there.



Existing user master records are migrated to the central system with transaction SCUG in the central system. This procedure can only be performed once for each child system. "User identification" is the SAP logon name to which a combination of the first and last names is assigned.

If the user identification to be copied is not yet contained in Central User Administration, it is entered as *new user*. New users including their user master records can be copied to the central system and then maintained there.

If the user identification to be copied is already in Central User Administration with the identical first and last names, it is entered as *identical user*. Identical users can be copied to the central system. The old system assignment including the valid roles and profile assignment are recorded there.

If the user identification to be copied is already in Central User Administration with a different first or last name, it is entered as a *different user*. If the name given in the central system is correct, the user can be copied.

If the name given in the child system is correct, the first or last name must be corrected in the central system using transaction SU01. If, on the other hand, there are two different people with identical user IDs, you create a new user ID for the user in the child system, delete the old user ID in the child system, and copy the user to the central system.

Transaction SCUG shows the copied users under *Already central users*.

Central User Maintenance



SU01					
Text Comparison					
...	Systems	Roles	Profiles	Groups	
	T41CLNT400 T41CLNT401	T41CLNT400 T41CLNT401	Superuser Agent	T.....	Administrator

Figure 136: Central User Maintenance

After activating Central User Administration, the appearance of user maintenance transaction SU01 changes.

An additional *Systems* tab, under which the logical systems to which the user is distributed are entered, appears in the central system. The user is only known in these child systems and in the central system. The column *Systems* also appears on the *Roles* and *Profiles* tab pages. You can therefore define the assignment of users to roles and profiles individually for each child system. The data is distributed to the appropriate child systems when you choose *Save*.

Existing roles are still maintained and new roles are still built in the child systems. To assign users in the central system the roles and profiles defined in the child system, there is the *Text comparison* button in the *Roles* and *Profiles* tab pages in the central system. The names of the roles and profiles defined in the child systems are stored in the central system together with their short texts. The names of the roles and profiles are available in the central system in the value help (F4 help). Since the information in the child systems might change, you should occasionally repeat the text comparison.

Only the fields of SU01 for which the field attributes were not defined as “global” accept input in the child systems. It is not possible to create or copy users in the child systems.

Determining Cross-System Information on Users

There are a number of evaluation options available using the *Users* node of the user information system (SUIM). Using Central User Administration (CUA) cross-system information on users can be evaluated in the central system.

When evaluating the users on a child system, you have the option to determine the CUA systems in which a certain user exists or to determine all or some of the users in one or more CUA systems. It is also possible to search for users with no system assignment.

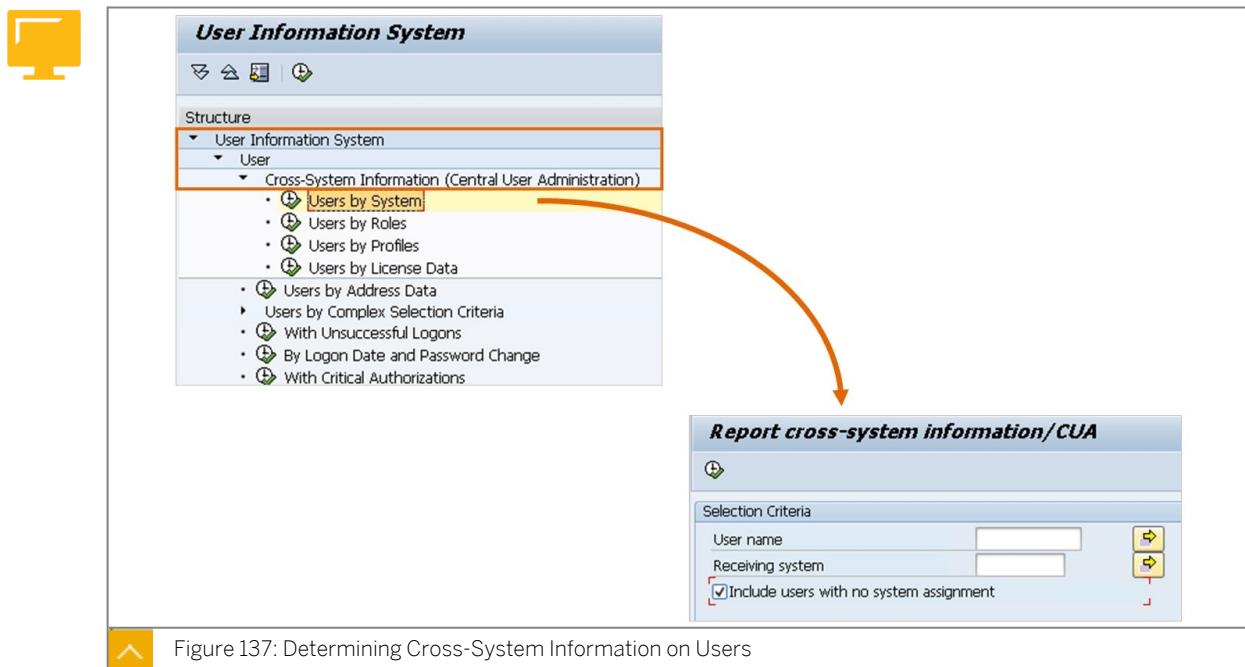


Figure 137: Determining Cross-System Information on Users

**Hint:**

These evaluation options can only be used if you are using CUA.

Analysis of Existing CUA Landscape

You use Central User Administration (CUA) and notice problems in the distribution of user changes to specific child systems or simply in the status confirmation from child systems.

Among others, it can be a problem that changes made to users in the central system are not visible in one or more child systems. This might be due to an incorrect configuration of the RFC connections or to insufficient postprocessing after client or system copies.

The report RSUSR_CUA_LANDSCAPE_CHECK provides the option of checking the CUA landscape for certain basic properties (see SAP note 2108938 – CUA: Analysis of existing CUA landscape). You can only execute the check of the CUA landscape from your CUA central system. To do this, you can use the new report RSUSR_CUA_LANDSCAPE_CHECK. This report is also integrated into transaction SCUA. Here, you can check the entire CUA landscape from the initial screen of the transaction or you can check selected child systems from the CUA landscape display. For a more detailed description of the report's result list, see the report documentation, which you can reach using the *Program Documentation* (Shift+F1) button in the result lists. Note that for each CUA child system, a check of the RFC connections from and to the CUA central system must be performed. Depending on the availability of the systems and their response time behavior, this check can take a long time.



LESSON SUMMARY

You should now be able to:

- Manage SAP central user administration.

Learning Assessment

1. Which of the following are true about the ALE concept in SAP systems?

Choose the correct answers.

- A It provides synchronous communication.
- B It involves a business-controlled message exchange between SAP systems.
- C It permits the building of distributed SAP links.
- D It is based on the integration of applications through asynchronous communication.

2. What is Central User Administration used for?

Choose the correct answer.

- A To administer password for SAP users centrally
- B To maintain the printer landscapes centrally
- C To administer user master records centrally
- D To create authorization profiles centrally

Learning Assessment - Answers

1. Which of the following are true about the ALE concept in SAP systems?

Choose the correct answers.

- A It provides synchronous communication.
- B It involves a business-controlled message exchange between SAP systems.
- C It permits the building of distributed SAP links.
- D It is based on the integration of applications through asynchronous communication.

The ALE concept facilitates a business-controlled message exchange with asynchronous communication in SAP systems, enabling the creation and management of distributed links.

2. What is Central User Administration used for?

Choose the correct answer.

- A To administer password for SAP users centrally
- B To maintain the printer landscapes centrally
- C To administer user master records centrally
- D To create authorization profiles centrally

Central User Administration used to administer user master records centrally. CUA does not cover central password administration in SAP systems. Printer landscapes are not maintained with CUA. No profiles are created centrally with CUA.

Lesson 1

Course Glossary

313

UNIT OBJECTIVES

- Review the glossary terms.

Course Glossary



LESSON OBJECTIVES

After completing this lesson, you will be able to:

- Review the glossary terms.

Glossary Terms

APO

Advanced Planning and Optimization

CRM

Customer Relationship Management. Supports all processes involving direct customer contact throughout the entire customer relationship life cycle - from market segmentation, sales lead generation and opportunities, to post-sales and customer service.

authorization object class

The organizational grouping of authorization objects.

authorization object

Allows you to define complex authorizations. An authorization object contains up to 10 authorization fields that are checked in an AND relationship. This determines whether a user is permitted to perform a certain action. To pass an authorization check, the user must satisfy the check for each field contained in the object.

authorization field

An element of an authorization object. In authorization objects, authorization fields represent values for individual system elements that must undergo authorization checking to verify a user's authorization.

authorization

References an authorization object. It defines one or more permissible values for each authorization field contained in the authorization object. Authorizations are combined in profiles, which are entered in a user's master record.

authorization profile

A group of multiple individual authorizations or other authorization profiles. Authorization profiles give users access to the system. They contain authorizations, which are identified using the name of an authorization object and the name of an authorization.

SAP Easy Access

A menu that contains all functions required by a user, and which is assigned by the system administrator in the user master record using roles. It can be extended individually using favorites.

user buffer

The buffer from which the data of a user master record is loaded when a user logs on.

CUA

Central User Administration — Management of users in a central system. A system group consists of several SAP systems with several clients. The same users are often created and the same roles assigned in each client. Central User Administration is designed to perform these tasks in a central system and distribute the data to the systems in the system group.

RFC

Remote Function Call

ALE

Application Link Enabling

TMS

Transport Management System

ITS

Internet Transaction Server

UTC

Universal Time Coordinated

Role Maintenance

Tool for generating authorization profiles in role maintenance. You use Role Maintenance to generate an authorization profile based on the activities in a role.

IMG

Implementation Guide. Tool for configuring the SAP system to meet customer requirements. The hierarchical structure of the IMG is based on the application component hierarchy. The main section is IMG activities, where the relevant system settings are made.

CCMS

Computing Center Management System: Integrated tools for monitoring and administration of SAP systems and independent SAP business components, with which operations such as resource distribution and the administration of SAP databases can be automated.

AIS

The Audit Information System is a tool used by auditors to optimize a system and examine any weak points. The old menu-based version (AUDIT area menu) was replaced by a role-based environment after SAP Release 4.6C. The role concept used now includes the same collections, structuring, and defaults for standard SAP programs, but is easier to scale.

**LESSON SUMMARY**

You should now be able to:

- Review the glossary terms.

Learning Assessment

1. Identify the descriptions that correctly match the terms from the SAP system tools.

Choose the correct answers.

- A SAP Easy Access: A menu assigned via roles in the user master record by the system administrator.
- B IMG: Tool for central user management with the hierarchical structure for configuration.
- C Role Maintenance: A tool for generating authorization profiles based on a role's activities.
- D AIS: Integrated tools for monitoring SAP system operations and resource distribution.

Learning Assessment - Answers

1. Identify the descriptions that correctly match the terms from the SAP system tools.

Choose the correct answers.

- A** SAP Easy Access: A menu assigned via roles in the user master record by the system administrator.
- B** IMG: Tool for central user management with the hierarchical structure for configuration.
- C** Role Maintenance: A tool for generating authorization profiles based on a role's activities.
- D** AIS: Integrated tools for monitoring SAP system operations and resource distribution.

SAP Easy Access is a menu assigned through roles, and Role Maintenance generates authorization profiles. The IMG configures systems, but is not for user management, and AIS is specifically for audit information.