

ADM940

ABAP AS Authorization Concept

SAP NetWeaver

Date _____
Training Center _____
Instructors _____
Education Website _____

Participant Handbook

Course Version: 72
Course Duration: 3 Day(s)
Material Number: 50099897



An SAP course - use it to learn, reference it for work

Copyright

Copyright © 2011 SAP AG. 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 AG. The information contained herein may be changed without prior notice.

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

Trademarks

- Microsoft®, WINDOWS®, NT®, EXCEL®, Word®, PowerPoint® and SQL Server® are registered trademarks of Microsoft Corporation.
- IBM®, DB2®, OS/2®, DB2/6000®, Parallel Sysplex®, MVS/ESA®, RS/6000®, AIX®, S/390®, AS/400®, OS/390®, and OS/400® are registered trademarks of IBM Corporation.
- ORACLE® is a registered trademark of ORACLE Corporation.
- INFORMIX®-OnLine for SAP and INFORMIX® Dynamic ServerTM are registered trademarks of Informix Software Incorporated.
- UNIX®, X/Open®, OSF/1®, and Motif® are registered trademarks of the Open Group.
- Citrix®, the Citrix logo, ICA®, Program Neighborhood®, MetaFrame®, WinFrame®, VideoFrame®, MultiWin® and other Citrix product names referenced herein are trademarks of Citrix Systems, Inc.
- HTML, DHTML, XML, XHTML are trademarks or registered trademarks of W3C®, World Wide Web Consortium, Massachusetts Institute of Technology.
- JAVA® is a registered trademark of Sun Microsystems, Inc.
- JAVASCRIPT® is a registered trademark of Sun Microsystems, Inc., used under license for technology invented and implemented by Netscape.
- SAP, SAP Logo, R/2, RIVA, R/3, SAP ArchiveLink, SAP Business Workflow, WebFlow, SAP EarlyWatch, BAPI, SAPPHIRE, Management Cockpit, mySAP.com Logo and mySAP.com are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world. All other products mentioned are trademarks or registered trademarks of their respective companies.

Disclaimer

THESE MATERIALS ARE PROVIDED BY SAP ON AN "AS IS" BASIS, AND SAP EXPRESSLY DISCLAIMS ANY AND ALL WARRANTIES, EXPRESS OR APPLIED, INCLUDING WITHOUT LIMITATION WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WITH RESPECT TO THESE MATERIALS AND THE SERVICE, INFORMATION, TEXT, GRAPHICS, LINKS, OR ANY OTHER MATERIALS AND PRODUCTS CONTAINED HEREIN. IN NO EVENT SHALL SAP BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES OF ANY KIND WHATSOEVER, INCLUDING WITHOUT LIMITATION LOST REVENUES OR LOST PROFITS, WHICH MAY RESULT FROM THE USE OF THESE MATERIALS OR INCLUDED SOFTWARE COMPONENTS.

About This Handbook

This handbook is intended to complement the instructor-led presentation of this course, and serve as a source of reference. It is not suitable for self-study.

Typographic Conventions

American English is the standard used in this handbook. The following typographic conventions are also used.

Type Style	Description
<i>Example text</i>	Words or characters that appear on the screen. These include field names, screen titles, pushbuttons as well as menu names, paths, and options. Also used for cross-references to other documentation both internal and external.
Example text	Emphasized words or phrases in body text, titles of graphics, and tables
EXAMPLE TEXT	Names of elements in the system. These include report names, program names, transaction codes, table names, and individual key words of a programming language, when surrounded by body text, for example SELECT and INCLUDE.
Example text	Screen output. This includes file and directory names and their paths, messages, names of variables and parameters, and passages of the source text of a program.
Example text	Exact user entry. These are words and characters that you enter in the system exactly as they appear in the documentation.
<Example text>	Variable user entry. Pointed brackets indicate that you replace these words and characters with appropriate entries.

Icons in Body Text

The following icons are used in this handbook.

Icon	Meaning
	For more information, tips, or background
	Note or further explanation of previous point
	Exception or caution
	Procedures
	Indicates that the item is displayed in the instructor's presentation.

Contents

Course Overview	vii
Course Goals	vii
Course Objectives	vii
Unit 1: Authorizations in General	1
What Are Authorizations?	2
Creating and Implementing an Authorization Concept.....	11
Unit 2: Basic Terminology of Authorizations.....	41
Elements and Terminology of the Authorization Concept (ABAP).....	42
Authorization Checks in the SAP System	63
Unit 3: User Settings	75
Maintaining and Evaluating User Data	76
Unit 4: Working with the Role Maintenance	105
Role Maintenance and Standard Roles	107
Special ABAP Roles	144
Subtleties of Authorization Maintenance.....	172
Unit 5: Basic Settings.....	189
Role Maintenance: Installation and Upgrade	191
Access Control and User Administration.....	214
Troubleshooting and Administration Aids	251
Unit 6: Transporting Authorizations.....	271
Transporting Authorization Components.....	272
Unit 7: Integration into the Company Landscape	287
Central User Administration (CUA).....	289
Integration into Organizational Management	307
SAP NetWeaver Identity Management.....	327
Appendix 1: SAP Notes About Authorizations	343
Appendix 2:	347
Glossary.....	349

Index	353
--------------------	------------

Course Overview

This course provides information about the fundamentals of the SAP authorization concept, using SAP systems based on AS ABAP. Basic knowledge about the SAP environment is vital for this training course.

Target Audience

This course is intended for the following audiences:

- Project team members
- Authorization and user administrators from system administration
- Authorization and user administrators from the user departments

Course Prerequisites

Required Knowledge

- SAPTEC (*SAP NetWeaver: Fundamentals of the Application Platform*)

Recommended Knowledge

- SAP01 (SAP Overview)
- Attendance of basic and advanced training courses in at least one application area

Course Goals



This course will prepare you to:

- Outline the elements, strategies, and tools of the SAP authorization concept
- Generate and assign authorization profiles with the Role Maintenance
- Work with the Central User Administration (CUA) tool

Course Objectives



After completing this course, you will be able to:

- List the elements and objects of the authorization concept
- Explain the use and purpose of the Role Maintenance
- Analyze authorizations
- Describe special objects for administrators

Unit 1

Authorizations in General

Unit Overview

This unit is the entry point into the topic of authorizations.

Starting with the basic concepts of the authorizations topic, it addresses SAP's role-based authorization concept, and discusses a method that describes how to create and structure authorizations, and how to implement them in a customer landscape.



Unit Objectives

After completing this unit, you will be able to:

- Describe the SAP authorization concept as part of a comprehensive security concept
- Explain the access control mechanisms
- Explain how users, roles, and authorizations are related
- Describe the technical implementation of a role-based authorization concept
- Explain the structure of an authorization concept
- List the steps required to implement a concept
- Describe the activities for the individual implementation steps
- Use the presented procedure model for implementing an authorization concept for your own projects
- Explain the strategy for user and authorization administration

Unit Contents

Lesson: What Are Authorizations?	2
Lesson: Creating and Implementing an Authorization Concept	11
Exercise 1: Creating and Implementing an Authorization Concept ...	29

Lesson: What Are 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.



Lesson Objectives

After completing this lesson, you will be able to:

- Describe the SAP authorization concept as part of a comprehensive security concept
- Explain the access control mechanisms
- Explain how users, roles, and authorizations are related
- Describe the technical implementation of a role-based authorization concept

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.

Content Overview for SAP Course ADM940 and Positioning in the SAP Customer Curriculum

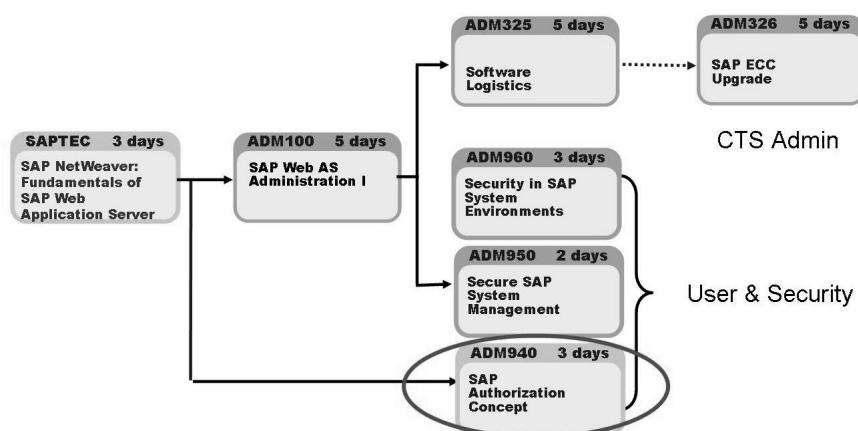


Figure 1: Curriculum - Overview

Why and for What Do We Require Authorizations?

Security Expectations



- **Protection of sensitive business data on the basis of**
 - *Laws*
 - *Agreements*
 - *Regulations*
- **Advantageous cost-benefit relation**
- **No obstruction of business processes**

Table 1: 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.

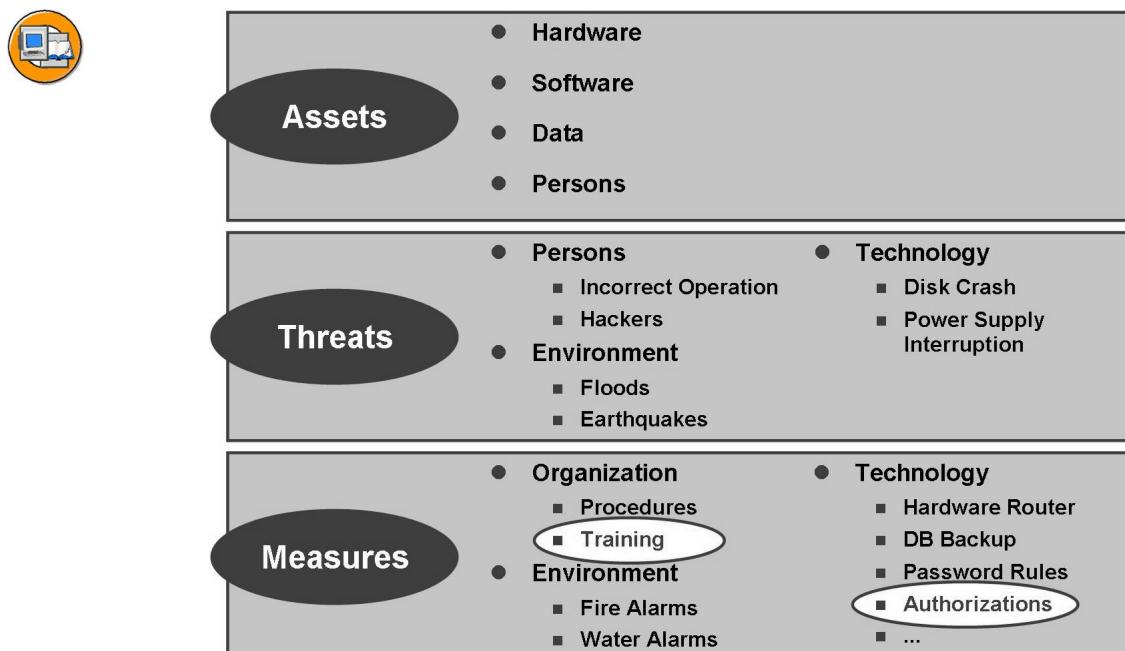


Figure 2: Security - Overview

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	ITS	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	ADM5xx
Operating System	UNIX, Windows NT, OS/400, OS 390	Access to SAP files, OS services	???

Figure 3: 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



- **System Access Control**
 - Users must identify themselves in the system
 - Configuration of system access control (such as password rules)
- **Access Control**
 - Access rights for functions and data must be granted explicitly using authorizations
 - Authorization checks for
 - ♦ transaction/report calls
 - ♦ program execution

Figure 4: SAP Access Controls

In order 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. In order 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.

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

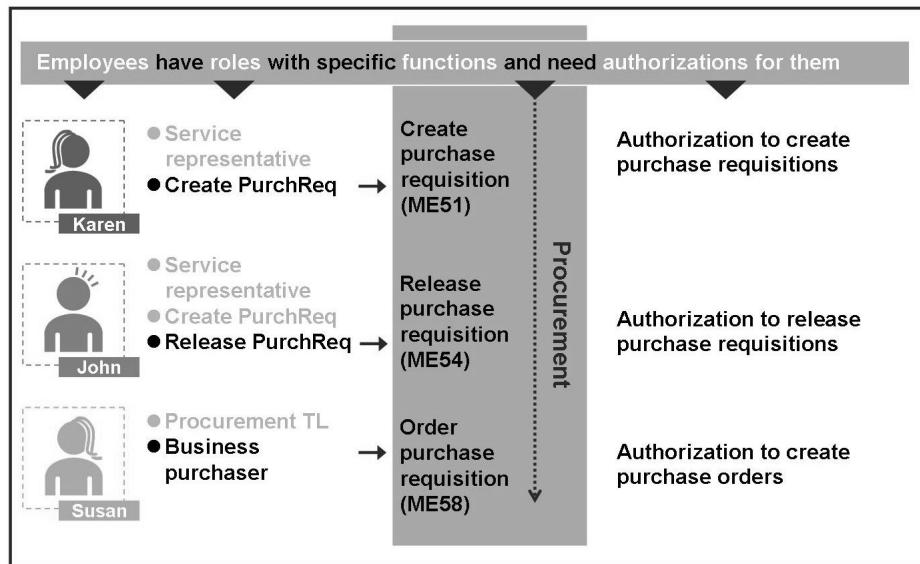


Figure 5: Users, Roles, and Authorizations

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.

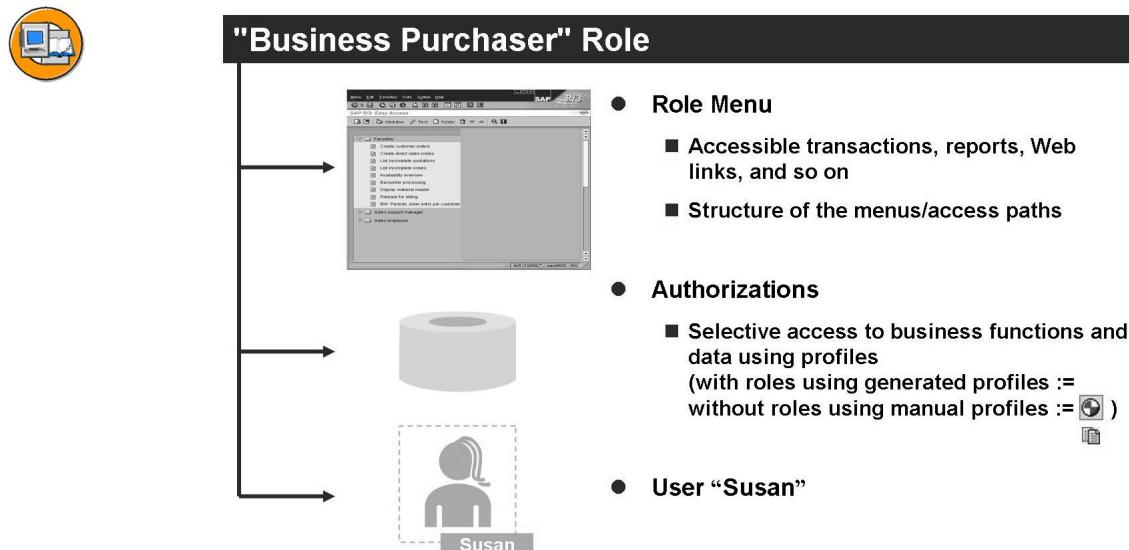


Figure 6: Technical Implementation of Roles

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.

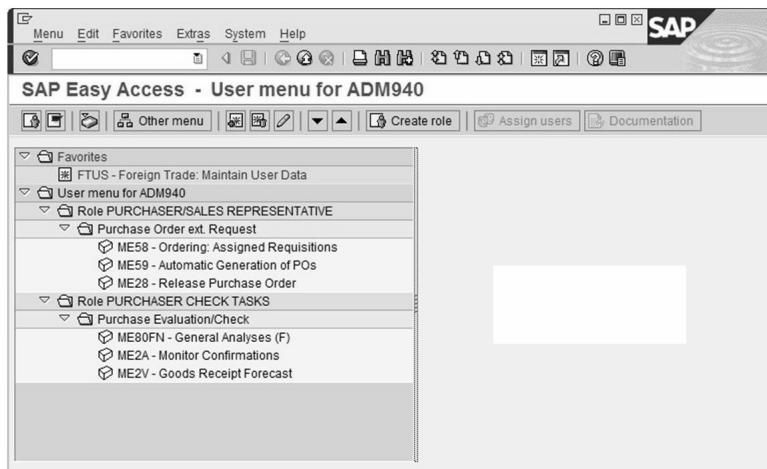


Figure 7: SAP Easy Access - User-Specific Menus

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.



Lesson Summary

You should now be able to:

- Describe the SAP authorization concept as part of a comprehensive security concept
- Explain the access control mechanisms
- Explain how users, roles, and authorizations are related
- Describe the technical implementation of a role-based authorization concept

Lesson: 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.



Lesson Objectives

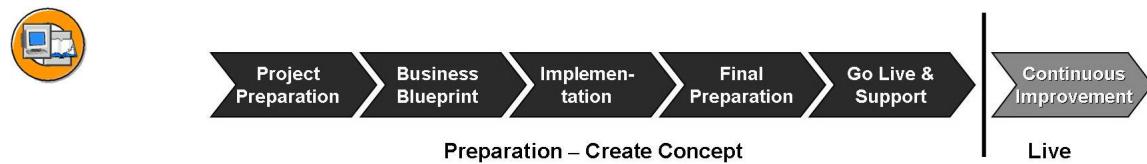
After completing this lesson, you will be able to:

- Explain the structure of an authorization concept
- List the steps required to implement a concept
- Describe the activities for the individual implementation steps
- Use the presented procedure model for implementing an authorization concept for your own projects
- Explain the strategy for user and authorization administration

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.

Development of an Authorization Concept



- Implementation guide for SAP projects
- Implementation divided into a model with 5 steps
- Creating authorization content in combination with
 - the project team
 - the user departments
- Integration of authorization assignment and user administration in the "Business Blueprint" and "Implementation" phases

Figure 8: Implementation Methods and Authorizations

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 which 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**

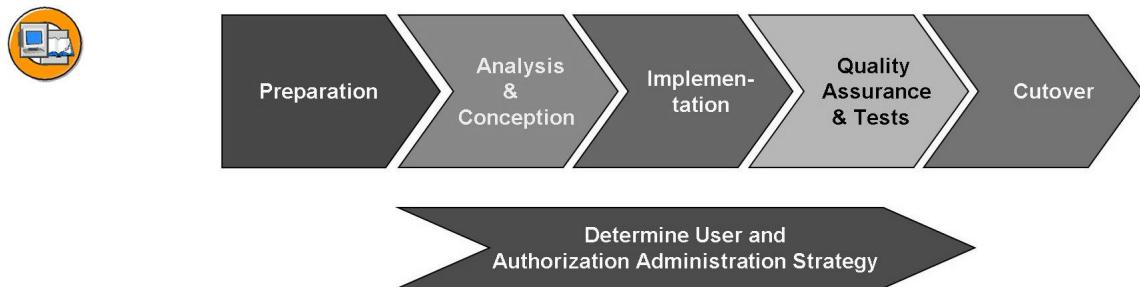
Configuration and fine tuning of the SAP system. The business processes created and described in the previous phase are the starting point for the implementation of the roles.

- **Final Preparation**

Testing of all interfaces, training of users, 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.



- **A role and authorization concept is implemented in five steps**
 - Each step comprises different activities
 - Each activity is associated with a responsible person
- **User administration and authorization management organization is done in parallel with the user and authorization concept implementation**

Figure 9: Role and Authorization Concept: Steps

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 which 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 are necessary to perform the role-specific tasks.

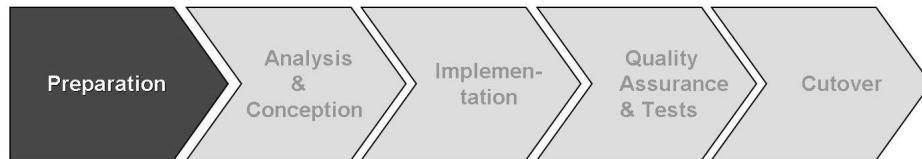
Besides authorizations, a role comprises the user menu specifications. When a user logs on to an SAP system, the system displays a user-specific menu, with selected transactions, reports, and Internet links in the form of a tree structure. This menu is based on the assigned role. Users can only access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

**Measures:**

- **Set up a team for user roles and authorizations**
- **Clarify prerequisites for authorization assignment**
- **Define and communicate processes and guidelines**
- **Train the team for user roles and authorizations**
- **Trigger role and authorization project**

Figure 10: 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.

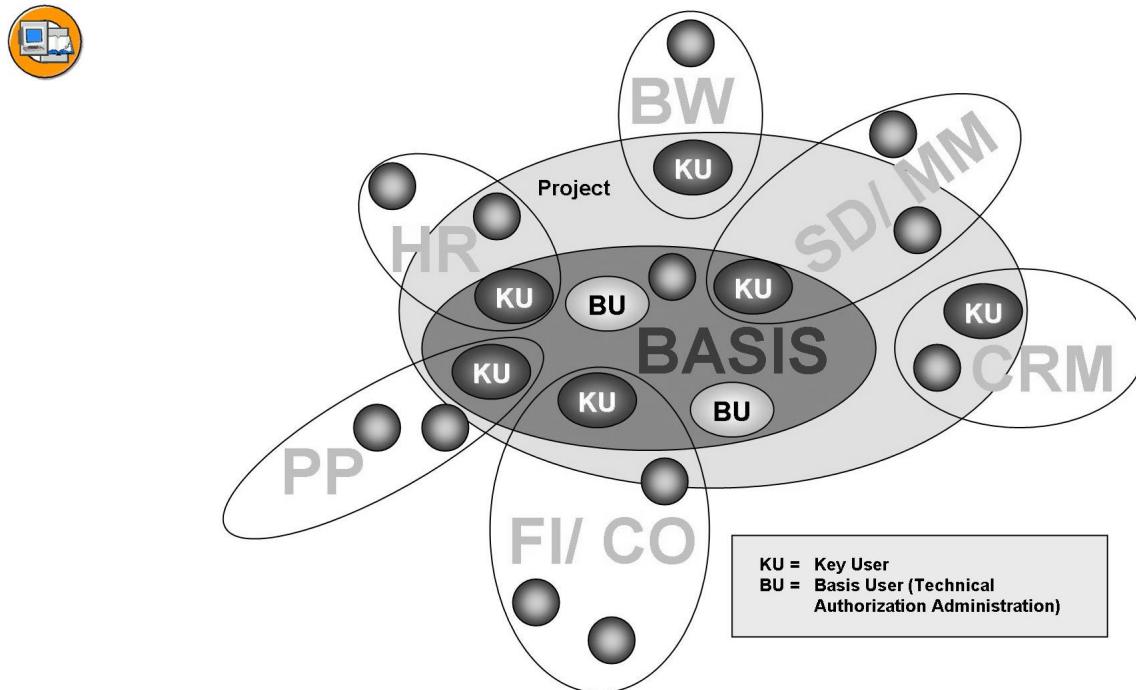


Figure 11: Working Party for Roles and Authorizations

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

**Measures:**

- **Analyze business processes in company (project team)**
- **Realize job roles through role concept**
- **Determine user roles**
- **Complete roles**
- **Determine framework for implementing the roles**
- **Check and accept framework for role implementation**

Figure 12: 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.

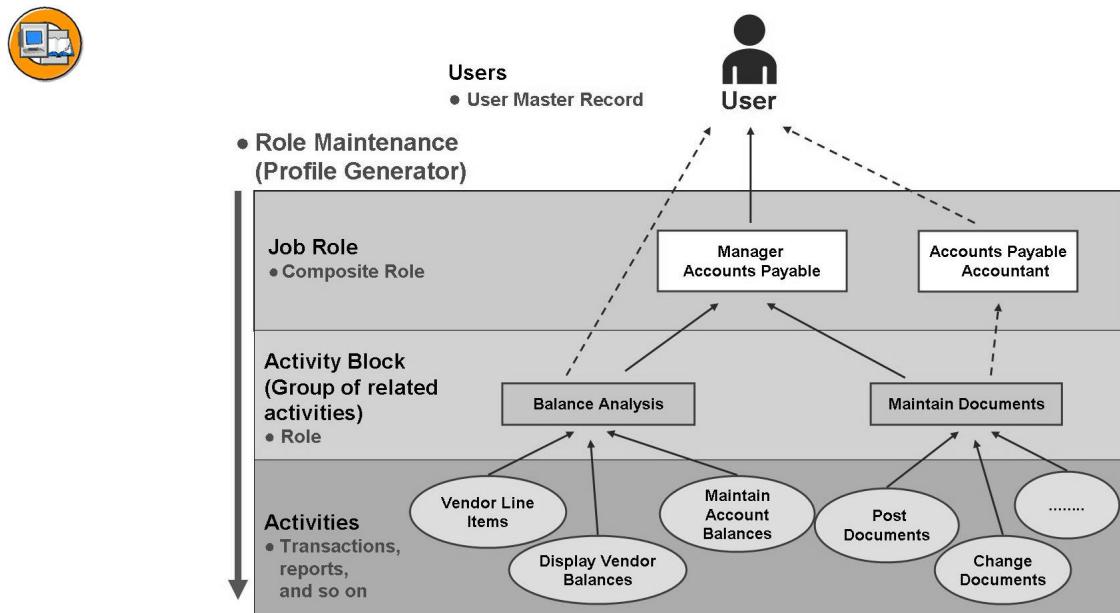


Figure 13: Technical Conception: Role Implementation (1)

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 >>>		
E1	E2	E3	E4	E5	E6	Job Role >>>		
						R/3-Links: T-Code	Scope	Scope
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.	F 5D		
					General Ledger: Post Balance Sheet Readj.	F 5E		
					General Ledger: Balance Sheet Readj., Log	F 5F		
					General Ledger: Upd. Balance Sheet Spec.	F 5G		
	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	FBLIN		
	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 14: 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
E1	E2	E3	E4	E5	E6	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										
F0 50										
General Ledger: Upd. Balance Sheet Adj.										
F 5D										
General Ledger: Post Balance Sheet Readj.										
F 5E										
General Ledger: Balance Sheet Readj., Log.										
F 5F										
General Ledger: Upd. Balance Sheet Spec.										
F 5G										
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 15: 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
E1	E2	E3	E4	E5	E6	Job Role	>>>	FI_Manag	AP_Manag	AP_Acc
						R/3-Links:	Scope	Scope	Scope	Scope
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						FBLIN		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 16: 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.

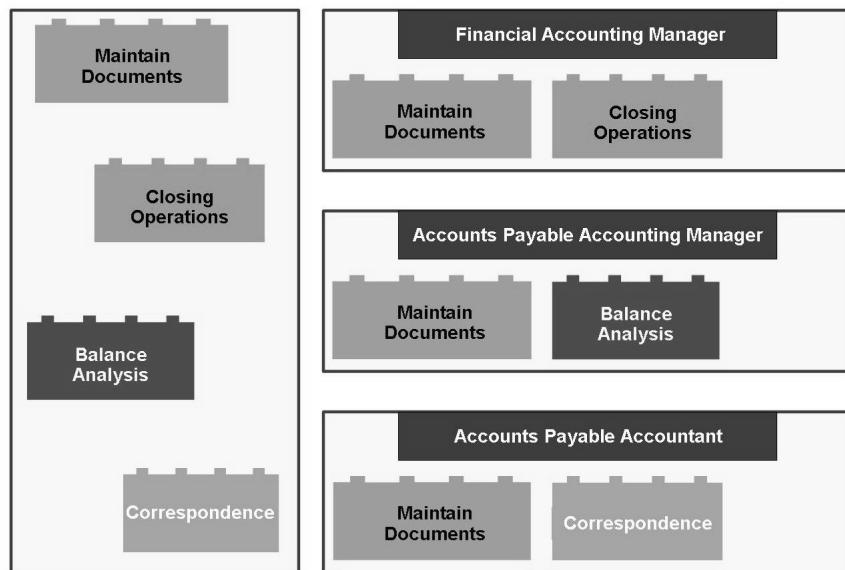


Figure 17: Technical Conception: Role Implementation (2)

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 have been properly defined before implementation.

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

Step 3: Implementation

**Measures:**

- **Implement role concept**
- **Create roles**
 - Single role
 - Imparting role (reference role)
 - Derived role
 - Composite role
 - Customizing role
- **Function check of role contents**

Figure 18: Step 3: Implementation

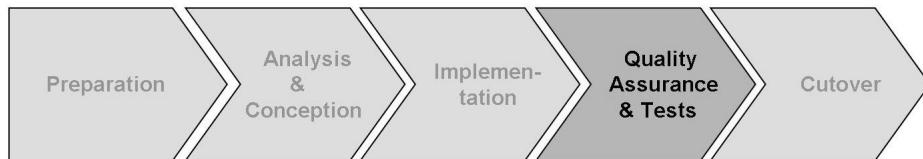
From a technical point of view, user roles (job roles) can be implemented as composite roles using the Role Maintenance. Composite roles consist of individual and composite roles that each contain the relevant authorizations and menu data. Authorizations specify the scope of access to data and functions. 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.



Measures:

- **Test user roles and authorization concept**
- **Realize job roles through role concept**
- **Check quality for combination of roles**
- **Train end users with new role concept**
- **Release roles and authorization concept**

Figure 19: Step 4: Quality Assurance & Tests

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** and **negative checks** of the authorizations of the individual roles. The positive test checks whether the functions are executed as desired, while the negative test 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.

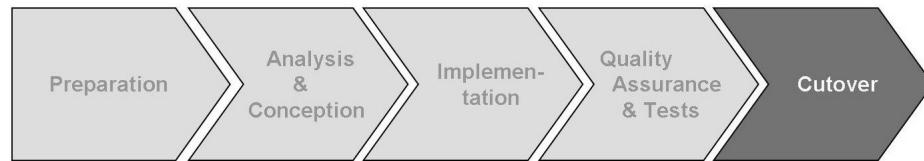
If a function cannot be called during the test, you must correct the user roles and the authorization concept. Note that changes may affect several (derived) roles. In extreme cases, you must revise the entire role and authorization concept.

You may also be required to modify the user menus in order 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.

**Measures:**

- **Set up production environment**
- **Create user master records for production users**
- **Accept role and authorization project**
- **Implement, test and release new requirements in accordance with implementation request**

Figure 20: Step 5: Cutover

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



- **Measures:**
- **Determine technical user and authorization administration strategy**
- **Specify and implement user and authorization administration procedure**
- **Train users and authorization administrators**

Figure 21: Strategy for 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.

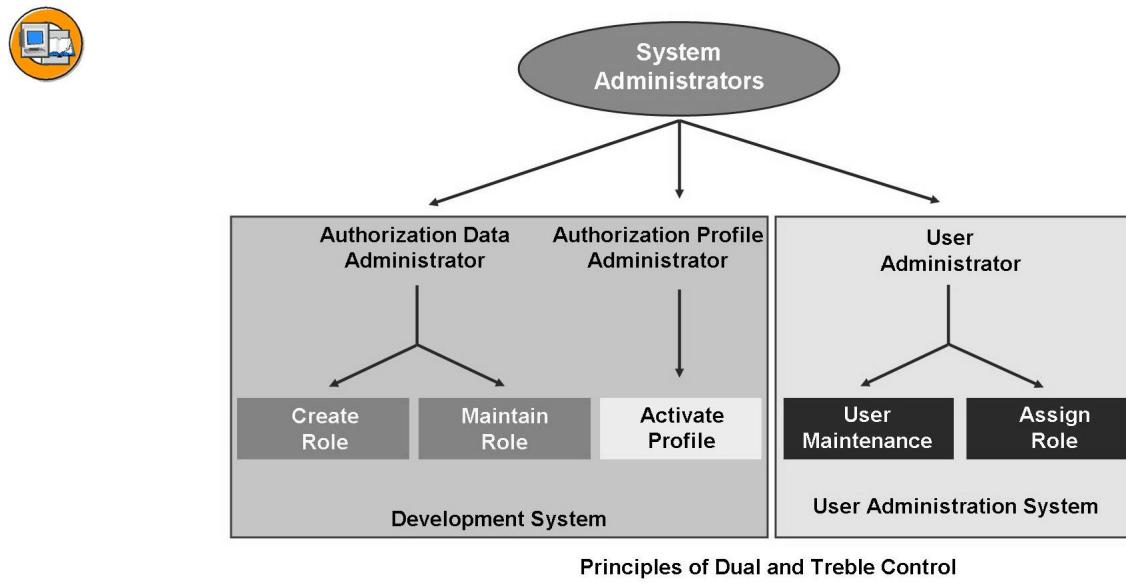


Figure 22: Organization of User and Authorization Administration

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.

Exercise 1: Creating and Implementing an Authorization Concept

Exercise Objectives

After completing this exercise, you will be able to:

- Describe the individual worksheets of the authorization list
- Define roles in the authorization list
- Assign transactions to these roles
- Group transactions
- Generate an overview of the roles with the relevant transactions

Business Example

This exercise should provide you with a brief impression of how you can create, structure, and usefully implement a new authorization concept in a company. A prepared Microsoft Excel list is provided for this purpose. It allows you to divide the user tasks into small reusable blocks (roles).

Task 1:

Open the Excel file AL-ADM940.XLS, which you can find in the Shared Folders, and answer the following questions.

The Shared Folders are in the Business Workplace.

Menu path: SAP Menu → Office → Workplace , then → Shared Folders → ADM940: Authorization Concept → AL-ADM940

Double click the Microsoft Excel file to open it. If a dialog box appears, choose *Enable Macros*. If an error message appears when opening the Excel file you can ignore it.

Then choose the menu path *Extras* → *Macro* → *Security* and select the security level *Low*.

Save the settings and the Microsoft Excel file on the hard disk (for example, in the directory C:\Temp or N:\MyDocuments) under the name *GR##_AL-ADM940.xls*. Close the file (not Microsoft Excel). If you now reopen the file (*GR##_AL-ADM940.xls*) in Microsoft Excel, all macro functions are available (this is indicated by the icons on the right-hand side).

1. Which **master data** is used by the company at *Scenario Level*, and should be used in the job roles (*Level 3, Column C*)?

Master data for

Continued on next page

_____ and _____

2. Which business processes (**Level 5, Column E**) should be taken into account for assigning authorizations and were included in the Microsoft Excel list?

3. Which *transaction codes* were copied for the business process ***sales order processing***?

Task 2:

In the following exercises (exercises 2.1 - 2.5), define the roles for the enterprise areas:

- Financial Accounting (FI)
- Sales and Distribution (SD)
- Materials Management (MM)

and assign transactions to these roles. If you are not experienced in the areas in question, and you are not sure which transactions to use, use the solution as a guideline.

1. FI Enterprise Area

Create the job role for an **Accounts Receivable Accountant (AccRec, FI)**. To do this, enter *FI* in the column header for Enterprise area and *AccRec* as a job role name on the *Roles Design* worksheet (field I2).

Assign all transactions of the *Manual Incoming Payments* business process to the accounts receivable accountant by placing an “x” for these transactions in the *AccRec* column. The accounts receivable accountant should also be able to maintain the accounting views of the accounts receivable master.

What does ***maintain*** mean? Discuss this term with your neighbor and consider opinions and points of view.

2. SD Enterprise Area

Continued on next page

Define a job role for a **Sales and Distribution clerk (SDClerk, SD)**, and assign all transactions of the *Sales Order Processing (Standard)* business process as well as transactions for overall maintenance of the SD views of the accounts receivable master records to this role.

3. **SD** Enterprise Area

Define a job role for the **Sales and Distribution manager (SDMan, SD)**, and assign all transactions of the *Sales Order Processing (Standard)* business process as well as transactions for overall maintenance of all (accounting and sales and distribution) views of the accounts receivable master to this role.

4. **MM** Enterprise Area

Define a job role for a **Warehouse Supervisor (Whouse)** for the MM enterprise area. Assign the transactions of the *Goods Receipt Processing* business process to this role.

5. Add transactions “MM03”, “MM04”, and “MM19”for displaying material master data for all job roles.

Task 3:

1. Switch to the Microsoft Excel list on the second worksheet *T Codes for each Role*. Generate an overview of the transactions and roles by pressing the appropriate button. Do you remember them?

How many transactions were chosen for the individual roles:

AccRec:	_____	Transactions
SDClerk	_____	Transactions
SDMan	_____	Transactions
Whouse	_____	Transactions

Continued on next page

Task 4:

Now combine these transactions into meaningful roles to ensure that these single roles can be reused in several composite roles.



Hint: There are several ways to do this.

Do not worry if your solution is not the same as your neighbor's. The solutions will vary from group to group.

Go back to the first worksheet “*Roles Design - scope*”.

1. Combine several transactions into roles in such a way that these single roles can be reused in several composite roles. To do this, you can color code the roles or draw a border around them.
2. Give the roles meaningful names and enter the associated transactions in the following table. Compare the names that you have given the roles with the suggestions in the solution. Which naming convention do you use in your company?

Name of the Role	Transactions for this Role

Solution 1: Creating and Implementing an Authorization Concept

Task 1:

Open the Excel file AL-ADM940.XLS, which you can find in the Shared Folders, and answer the following questions.

The Shared Folders are in the Business Workplace.

Menu path: SAP Menu → Office → Workplace , then → Shared Folders → ADM940: Authorization Concept → AL-ADM940

Double click the Microsoft Excel file to open it. If a dialog box appears, choose *Enable Macros*. If an error message appears when opening the Excel file you can ignore it.

Then choose the menu path *Extras* → *Macro* → *Security* and select the security level *Low*.

Save the settings and the Microsoft Excel file on the hard disk (for example, in the directory C:\Temp or N:\MyDocuments) under the name *GR##_AL-ADM940.xls*. Close the file (not Microsoft Excel). If you now reopen the file (*GR##_AL-ADM940.xls*) in Microsoft Excel, all macro functions are available (this is indicated by the icons on the right-hand side).

1. Which **master data** is used by the company at *Scenario Level*, and should be used in the job roles (*Level 3, Column C*)?

Master data for

_____ and _____

- a) *Master Data/General Master Data* for

Material master and **customer master records**

2. Which business processes (*Level 5, Column E*) should be taken into account for assigning authorizations and were included in the Microsoft Excel list?

Continued on next page

-
- a) Customer quotation processing
Sales order processing
Goods receipt processing
Manual incoming payments
3. Which *transaction codes* were copied for the business process *sales order processing*?

- a) “VA01”,
“VA02”,
“VA03”,
“V.01”.

Task 2:

In the following exercises (exercises 2.1 - 2.5), define the roles for the enterprise areas:

- Financial Accounting (FI)
- Sales and Distribution (SD)
- Materials Management (MM)

and assign transactions to these roles. If you are not experienced in the areas in question, and you are not sure which transactions to use, use the solution as a guideline.

1. FI Enterprise Area

Create the job role for an **Accounts Receivable Accountant (AccRec, FI)**. To do this, enter *FI* in the column header for Enterprise area and *AccRec* as a job role name on the *Roles Design* worksheet (field I2).

Assign all transactions of the *Manual Incoming Payments* business process to the accounts receivable accountant by placing an “x” for these transactions in the *AccRec* column. The accounts receivable accountant should also be able to maintain the accounting views of the accounts receivable master.

Continued on next page

What does ***maintain*** mean? Discuss this term with your neighbor and consider opinions and points of view.

- a) Excel authorization list on the Roles Design worksheet

The following table contains the solutions to exercises 2.1 to 2.5:

Business area>>>	FI	SD	SD	MM
Work Place Description>>>	AccRec	SD-Clerk	SD-Man	Whouse
SAP R/3 Links: T Code	Scope	Scope	Scope	Scope
MM01				
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	

Continued on next page

Business area>>>	FI	SD	SD	MM
Work Place Description>>>	AccRec	SD-Clerk	SD-Man	Whouse
SAP R/3 Links: T Code	Scope	Scope	Scope	Scope
MB1C				x
MB90				x
VL21				x
F-18	x			
F-26	x			
F-28	x			

Sample Authorization Concept (job role)

2. **SD** Enterprise Area

Define a job role for a **Sales and Distribution clerk (SDClerk, SD)**, and assign all transactions of the *Sales Order Processing (Standard)* business process as well as transactions for overall maintenance of the SD views of the accounts receivable master records to this role.

- a) See solution 2.1

3. **SD** Enterprise Area

Define a job role for the **Sales and Distribution manager (SDMan, SD)**, and assign all transactions of the *Sales Order Processing (Standard)* business process as well as transactions for overall maintenance of all (accounting and sales and distribution) views of the accounts receivable master to this role.

- a) See solution 2.1

4. **MM** Enterprise Area

Define a job role for a **Warehouse Supervisor (Whouse)** for the MM enterprise area. Assign the transactions of the *Goods Receipt Processing* business process to this role.

- a) See solution 2.1

5. Add transactions “MM03”, “MM04”, and “MM19”for displaying material master data for all job roles.

- a) See solution 2.1

Continued on next page

Task 3:

- Switch to the Microsoft Excel list on the second worksheet *T Codes for each Role*. Generate an overview of the transactions and roles by pressing the appropriate button. Do you remember them?

How many transactions were chosen for the individual roles:

AccRec:	_____	Transactions
SDClerk	_____	Transactions
SDMan	_____	Transactions
Whouse	_____	Transactions

- The button for generating an overview of transactions and roles is in cell **A4** on the second worksheet *T Codes for each Role*.

AccRec:	9	Transactions
SDClerk	14	Transactions
SDMan	17	Transactions
Whouse	6	Transactions

Task 4:

Now combine these transactions into meaningful roles to ensure that these single roles can be reused in several composite roles.



Hint: There are several ways to do this.

Do not worry if your solution is not the same as your neighbor's. The solutions will vary from group to group.

Go back to the first worksheet “*Roles Design - scope*”.

- Combine several transactions into roles in such a way that these single roles can be reused in several composite roles. To do this, you can color code the roles or draw a border around them.
 - There are several solutions to this task.

Model solution as a sample authorization concept

See the next page or exercise 1 for the unit *Working with the Role Maintenance 1*.

Continued on next page

2. Give the roles meaningful names and enter the associated transactions in the following table. Compare the names that you have given the roles with the suggestions in the solution. Which naming convention do you use in your company?

Name of the Role	Transactions for this Role

- a) The following table shows the role names in accordance with the example authorization concept, which you will use in later exercises. The example authorization concept is then shown graphically.

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

Sample Authorization Concept (role distribution)



Lesson Summary

You should now be able to:

- Explain the structure of an authorization concept
- List the steps required to implement a concept
- Describe the activities for the individual implementation steps
- Use the presented procedure model for implementing an authorization concept for your own projects
- Explain the strategy for user and authorization administration



Unit Summary

You should now be able to:

- Describe the SAP authorization concept as part of a comprehensive security concept
- Explain the access control mechanisms
- Explain how users, roles, and authorizations are related
- Describe the technical implementation of a role-based authorization concept
- Explain the structure of an authorization concept
- List the steps required to implement a concept
- Describe the activities for the individual implementation steps
- Use the presented procedure model for implementing an authorization concept for your own projects
- Explain the strategy for user and authorization administration

Unit 2

Basic Terminology of Authorizations

Unit Overview

This unit uses two lessons to provide an introduction to the basic terms of authorization and the main authorization check in the SAP system. The relationships between the authorization terms are explained step-by-step and form a good basis for all subsequent units.



Unit Objectives

After completing this unit, you will be able to:

- Describe and differentiate between the individual elements of the authorization concept
- Describe the relationships between the elements in the overall concept
- Explain the differences between roles and authorization profiles
- Find out the meaning of an authorization object
- Explain the relationship between roles and the Easy Access Menu
- Explain when authorization checks are performed
- Describe the difference between the authorization check when a transaction is started and the authorization check performed by a program
- Define the function of the user buffer and evaluate the buffered user authorizations
- Control some additional checks without “modifying” the system

Unit Contents

Lesson: Elements and Terminology of the Authorization Concept (ABAP)	42
Exercise 2: Elements and Terminology of the Authorization Concept (ABAP)	51
Lesson: Authorization Checks in the SAP System	63
Exercise 3: Authorization Checks in the SAP System.....	67

Lesson: Elements and Terminology of the Authorization Concept (ABAP)

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 (since SAP R/3 4.6C).



Lesson Objectives

After completing this lesson, you will be able to:

- Describe and differentiate between the individual elements of the authorization concept
- Describe the relationships between the elements in the overall concept
- Explain the differences between roles and authorization profiles
- Find out the meaning of an authorization object
- Explain the relationship between roles and the Easy Access Menu

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.

Overview of the Terms and Elements in the Authorization Concept

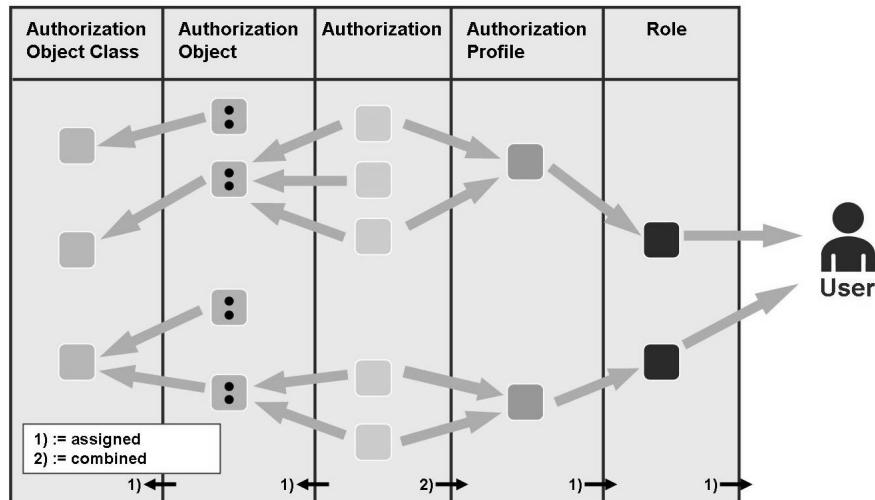


Figure 23: Overview of the Elements of the SAP Authorization Concept

Authorization object class: Logical grouping of authorization objects (for example, all authorization objects for object class FI beginning with “F_”).

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

Authorization field: 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: Is generated using the 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 contain an underscore in the second position.
- Authorization classes, objects, and fields are development objects and must begin with Y or Z (customer namespace).

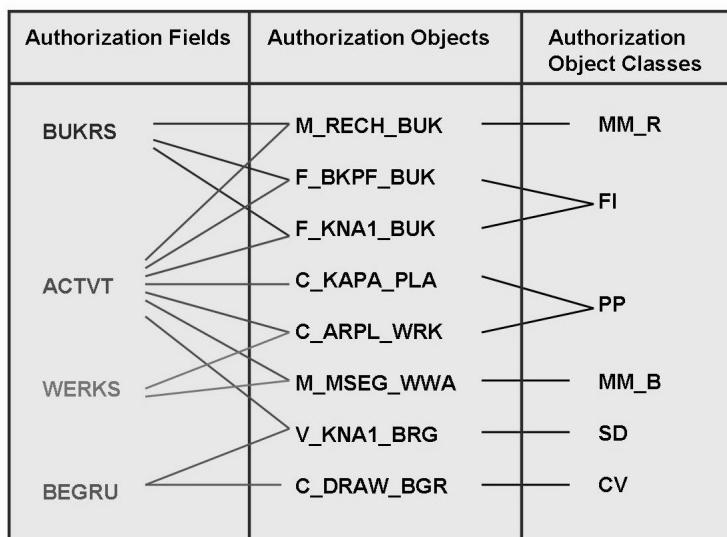


Figure 24: Authorization Fields, Objects, Object Classes

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.

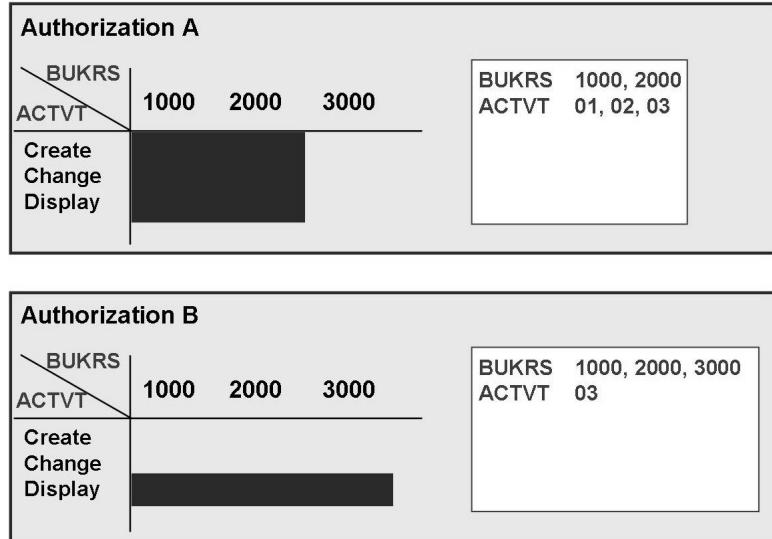


Figure 25: Authorization

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.



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 26: 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.

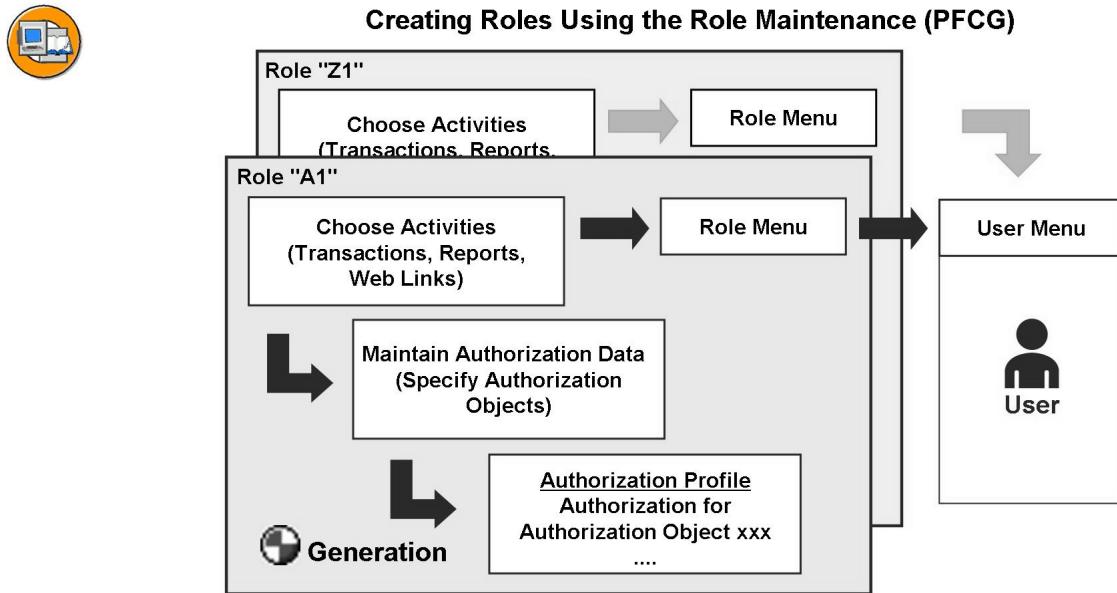


Figure 27: Roles and Authorization Profiles

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

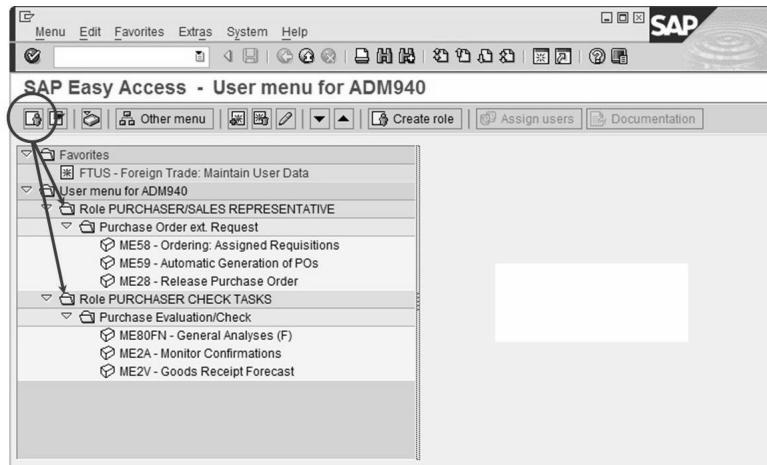


Figure 28: Roles and the Easy Access Menu

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 the 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

In order to be able 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	*

Exercise 2: Elements and Terminology of the Authorization Concept (ABAP)

Exercise Objectives

After completing this exercise, you will be able to:

- Distinguish between the elements of the authorization concept
- Display a user master record and find out the authorizations of a specific user
- Find out the meaning of an authorization object

Business Example

Task 1:

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?

3. Display the details for the authorization profile ADM94_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?

Continued on next page

- F_BKPF_BUK? _____

- PLOG? _____

- S_TCODE? _____

- S_USER_GRP? _____

What is the name of your authorization(s) for the object S_USER_GRP?

Which authorization fields does the object S_USER_GRP consist of?

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) _____

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

Exit the transaction.

Task 2:

Display various authorization information in the Information System.

1. Navigate to the Information System in the SAP Menu.

(*SAP Menu → Tools → Administration → User Maintenance → Information System*)

Expand the structure for the *Authorization Objects* node, and select the report *Authorization Objects By Object Name, Text* by double-clicking it.

Select the authorization object S_USER_GRP.

To which authorization object class is the authorization object S_USER_GRP assigned?

Display the documentation for this authorization object.

Continued on next page

In which transactions is the authorization object checked?

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

What activities are possible?

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

Exit the report *Authorization Objects by Object Name, Text*.

2. In the Information System, under the *Authorization Objects* node, double-click the report *Authorization Objects By Object Class*. Choose the *All Selections* icon (Shift+F7).

Select the authorization object class from task 2-1 (field: *Object Class*).

How many authorization objects are there, whose names begin with *S_USER*?

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

Which authorization fields does the object consist of?

Are any other authorization objects assigned to the selected authorization object class that do not start with *S_USER**?

Exit the report and return to the initial Information System screen.

3. Expand the structure for the Roles node, and choose the report *By Role Name*.

Select the role *ADM940_SD_SALES*.

Display the transaction assignment for the role.

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

Continued on next page

Does this role provide authorization to call transaction “VA03”?

Does this role provide authorization to call transaction “MM03”?

Solution 2: Elements and Terminology of the Authorization Concept (ABAP)

Task 1:

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?

_____ ,
_____ ,
_____ ,
_____ ,
_____ ,
_____ .

Continued on next page

-
- a) Choose the Profiles tab page.

Yes:

ADM94_DISP
ADM94_DISP1
ADM94_DISP2
ADM94_DISP3
ADM94_DISP4
ADM94_PLUS
ADM94_TRAI

3. Display the details for the authorization profile ADM94_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? _____

What is the name of your authorization(s) for the object S_USER_GRP?

Which authorization fields does the object S_USER_GRP consist of?

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

Authorization combination 1:

Field 1) _____ Field 2) _____

Authorization combination 2:

Continued on next page

Field 1) _____ Field 2) _____

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.

- b) Names of the authorizations for object S_USER_GRP:

ADM94_PLUS00

ADM94_PLUS01

- c) Authorization fields for the authorization object S_USER_GRP:

ACTVT Activity

CLASS User group in user master maintenance

- d) Authorization values for the authorization object S_USER_GRP:

Authorization combination 1) ADM94_PLUS00:

Field 1: ACTVT: **05**, Field 2: CLASS: **Z***.

Authorization combination 2) ADM94_PLUS01:

Field 1: ACTVT: **03, 08**, Field 2: CLASS: *.

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

Exit the transaction.

Task 2:

Display various authorization information in the Information System.

1. Navigate to the Information System in the SAP Menu.

(*SAP Menu → Tools → Administration → User Maintenance → Information System*)

Continued on next page

Expand the structure for the *Authorization Objects* node, and select the report *Authorization Objects By Object Name, Text* by double-clicking it.

Select the authorization object S_USER_GRP.

To which authorization object class is the authorization object S_USER_GRP assigned?

Display the documentation for this authorization object.

In which transactions is the authorization object checked?

_____ ; _____
_____ ; _____
_____ ; _____

What activities are possible?

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

Exit the report *Authorization Objects by Object Name, Text*.

- a) Authorization object class for authorization object S_USER_GRP:
BC_A, Basis Administration.
Select the authorization object and choose the *Documentation* button.
 - b) Transactions with integrated check of S_USER_GRP:
“SU01”, “SU10”, “SU12”, “PFCG”, “SUUM”, “SUUMD”.
 - c) Possible activities:
 - 01: 01: Create
 - 02: 02: Change
 - 03: 03: Display
 - 05: 05: Lock, Unlock
 - 06: 06: Delete
 - 08: 08: Display Change Documents
 - 22: 22: Include Users in Roles
 - 24: 24: Archive
 - 78: 78: Assign
 - 68: 68: Model

Exit the report *Authorization Objects by Object Name, Text*.

Continued on next page

2. In the Information System, under the *Authorization Objects* node, double-click the report *Authorization Objects By Object Class*. Choose the *All Selections* icon (Shift+F7).

Select the authorization object class from task 2-1 (field: *Object Class*).

How many authorization objects are there, whose names begin with *S_USER*?

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

Which authorization fields does the object consist of?

Are any other authorization objects assigned to the selected authorization object class that do not start with *S_USER**?

Continued on next page

Exit the report and return to the initial Information System screen.

- a) Select the authorization object class BC_A and the authorization object S_USER*.

Number of authorization objects that begin with S_USER:

11 Authorization objects

- b) Select the authorization object and choose the *Documentation* button.
Documentation 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 Role Maintenance, 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.

- c) Which authorization fields does the object consist of?

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

- d) YES

Examples of other authorization objects in object class BC_A:

BV_SR_TCOD, C_APO_LCAD, C_DML, E_WDPLJRNL,
F_GMGT_RLT, I_VV_IC, K_PRPS_SET, MAN_PM_KPI,
PPF_ADMIN, P_EFI, and a greater number of S_* objects.

Exit the report and return to the initial Information System screen.

3. Expand the structure for the Roles node, and choose the report *By Role Name*.

Select the role ADM940_SD_SALES.

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”?

Continued on next page

-
- a) Display the transaction assignment of the role (by choosing the corresponding button; Ctrl+Shift+F11).

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

YES

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

- b) Does this role provide authorization to call transaction “VA03”?

Yes.

- c) Does this role provide authorization to call transaction “MM03”?

No.



Lesson Summary

You should now be able to:

- Describe and differentiate between the individual elements of the authorization concept
- Describe the relationships between the elements in the overall concept
- Explain the differences between roles and authorization profiles
- Find out the meaning of an authorization object
- Explain the relationship between roles and the Easy Access Menu

Lesson: 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.



Lesson Objectives

After completing this lesson, you will be able to:

- Explain when authorization checks are performed
- Describe the difference between the authorization check when a transaction is started and the authorization check performed by a program
- Define the function of the user buffer and evaluate the buffered user authorizations
- Control some additional checks without “modifying” the system

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.

Authorization Checks When Transactions Are Started and in Programs

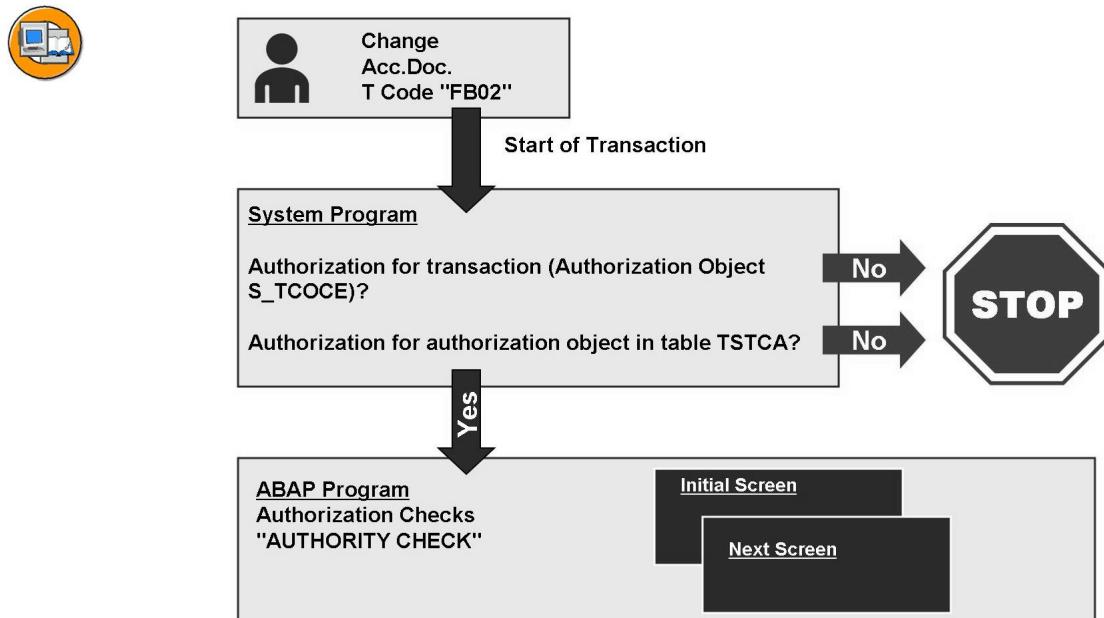


Figure 29: Authorization Checks at Transaction Start

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

Step 1: Check if the user is authorized to start the transaction. Authorization object *S_TCOC* (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 will not begin, and the user will receive 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.

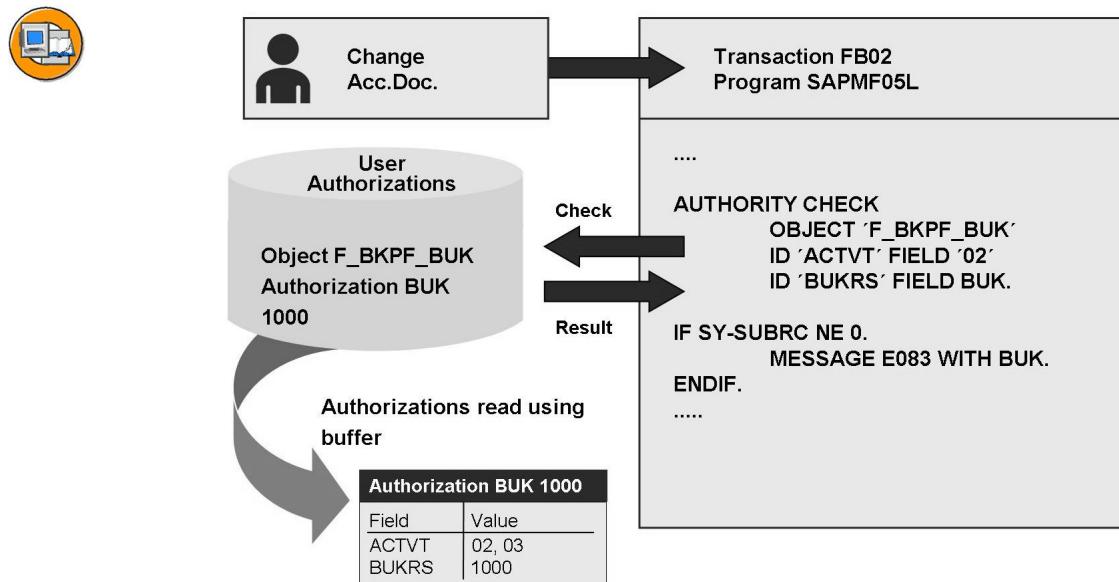


Figure 30: Authorization Check in the Program

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 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.

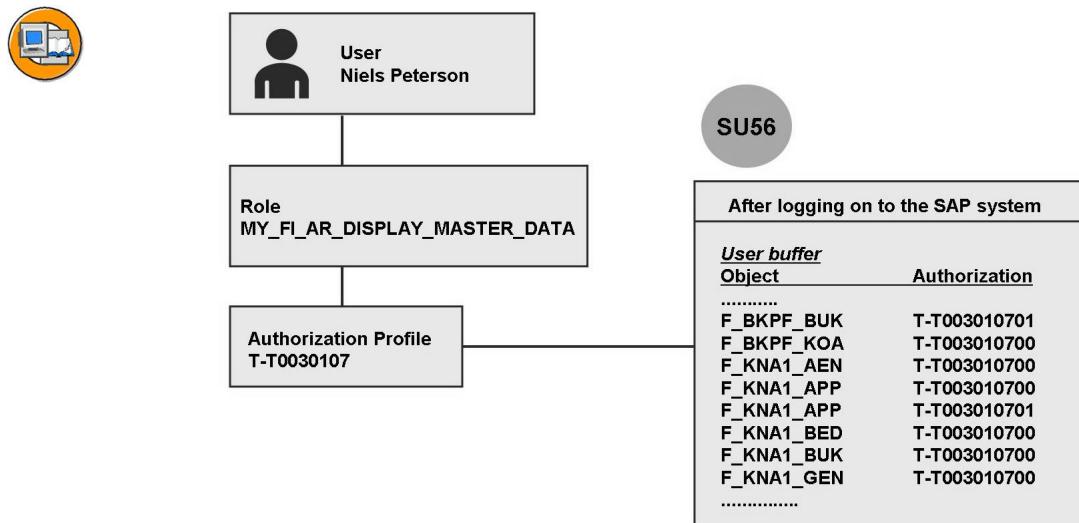


Figure 31: User Buffer

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_FI_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

Exercise 3: Authorization Checks in the SAP System

Exercise Objectives

After completing this exercise, you will be able to:

- Explain when authorization checks are performed
- Describe the relationships between the elements in the overall concept
- Explain the differences between roles and authorization profiles
- Find out the meaning of an authorization object
- Explain the relationship between roles and the Easy Access Menu

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 transaction “FB03”.



Hint: Menu path: *SAP Menu → Tools → ABAP Workbench → Development → Other Tools → Transactions.*

1. Which authorization object is checked when the transaction is called?

2. Which authorization values must exist for the authorization check to be positive and the transaction to be started?

Task 2:

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. Can you call the transaction?

Continued on next page

2. What message is returned by the system?

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

4. Can you call a failed authorization check for another participant?

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

Task 3:

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?

Solution 3: Authorization Checks in the SAP System

Task 1:

Display the definition of transaction “FB03”.



Hint: Menu path: SAP Menu → Tools → ABAP Workbench → Development → Other Tools → Transactions.

1. Which authorization object is checked when the transaction is called?

a) F_BKPF_BUK

2. Which authorization values must exist for the authorization check to be positive and the transaction to be started?

a) 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:

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. Can you call the transaction?

a) No.

2. What message is returned by the system?

a) “You are not authorized to use transaction VA07”

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

Continued on next page

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

The object “S_TCODE” was checked, and your user had authorizations only for the following transactions: “SESS”, “SESSION_MANAGER”, “SMEN”, “SSC1”, “SU3”, “SU53”, “SU56” and “YIDES”.

- 4. Can you call a failed authorization check for another participant?
-

- a) Yes.

- 5. 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:

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?

Continued on next page

-
- a) The number of entries is 3.
- S_TCODE/ADM94_PLUS00/Transaction Code Check at Transaction Start
 - S_USER_GRP/ADM94_PLUS00/User Master Maintenance: User Groups
 - S_USER_GRP/ADM94_PLUS01/User Master Maintenance: User Groups



Lesson Summary

You should now be able to:

- Explain when authorization checks are performed
- Describe the difference between the authorization check when a transaction is started and the authorization check performed by a program
- Define the function of the user buffer and evaluate the buffered user authorizations
- Control some additional checks without “modifying” the system



Unit Summary

You should now be able to:

- Describe and differentiate between the individual elements of the authorization concept
- Describe the relationships between the elements in the overall concept
- Explain the differences between roles and authorization profiles
- Find out the meaning of an authorization object
- Explain the relationship between roles and the Easy Access Menu
- Explain when authorization checks are performed
- Describe the difference between the authorization check when a transaction is started and the authorization check performed by a program
- Define the function of the user buffer and evaluate the buffered user authorizations
- Control some additional checks without “modifying” the system

Unit 3

User Settings

Unit Overview

What is the user master record? This question is answered in this unit.

SAP systems differentiate between system access control and role-based access control. Both are assigned and controlled using the user master record of a user.



Unit Objectives

After completing this unit, you will be able to:

- Create and change user master records
- Set the values on the tab pages of the user master record
- Define the differences between the user types
- Operate and implement mass maintenance
- Display and archive change documents for authorization assignment

Unit Contents

Lesson: Maintaining and Evaluating User Data.....	76
Exercise 4: Maintaining and Evaluating User Data	93

Lesson: Maintaining and Evaluating User Data

Lesson Overview

This lesson will provide you with an overview of identifying a user using the user master record. 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.



Lesson Objectives

After completing this lesson, you will be able to:

- Create and change user master records
- Set the values on the tab pages of the user master record
- Define the differences between the user types
- Operate and implement mass maintenance
- Display and archive change documents for authorization assignment

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.

The User Master Record and its Tab Pages

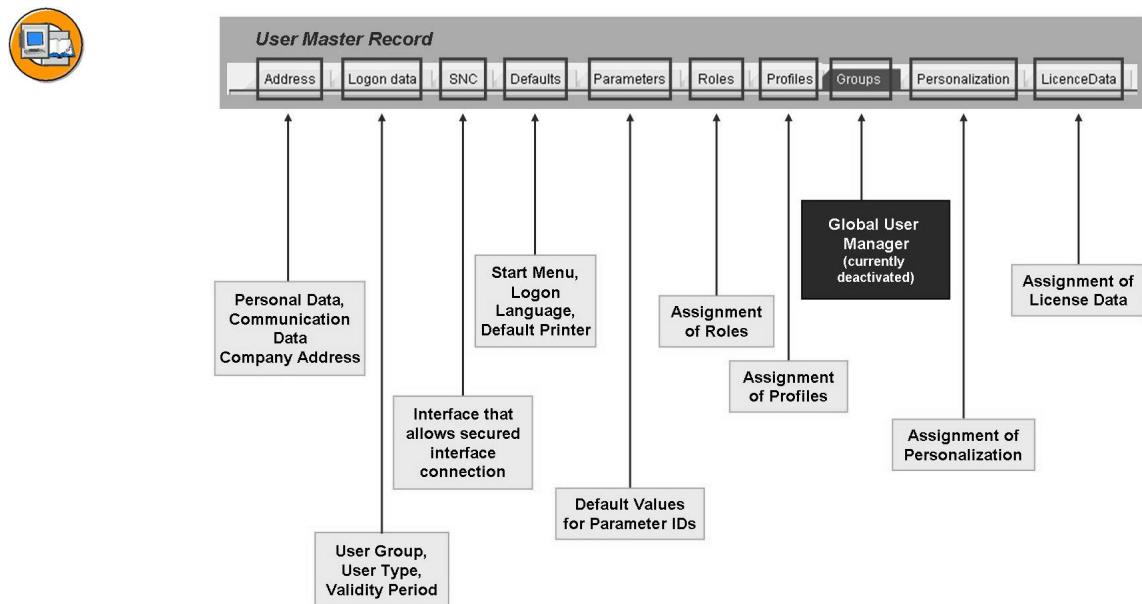


Figure 32: Components of the User Master Record

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 the 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: Address



The screenshot shows the SAP GUI interface for maintaining user data. The title bar reads 'Maintain User'. The main area is titled 'Address' and displays the following fields:

Person	Value
Title	[empty]
Last name	TEST
First name	User
Academic Title	[empty]
Format	User TEST
Function	[empty]
Department	[empty]
Room Number	[empty] Floor [empty] Building [empty]
Communication	
Language	[empty]
Telephone	[empty] Extension [empty]
Mobile Phone	[empty]
Fax	[empty] Extension [empty]
E-Mail	[empty]
Comm. Meth	[empty]

At the bottom of the screen, there are status messages: SU01, zteldc00, INS, and a save icon.

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 User

User	TEST
Last Changed On	SWIEBOCKI 17.09.2010 16:25:48
Status	Revised
<input checked="" 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	
Alias	<input type="text"/>
User Type	Dialog
Password New Password Rules (Uppercase/Lowercase Must Be Correct)	
Initial password	<input type="password" value="*****"/>
Repeat password	<input type="password" value="*****"/>
Password Status	Initial password (set by administrator)
User Group for Authorization Check	
User group	TECHNICAL Technical User
Validity Period	
Valid from	<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 using 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.

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.

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 next 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.

The User Types in Detail

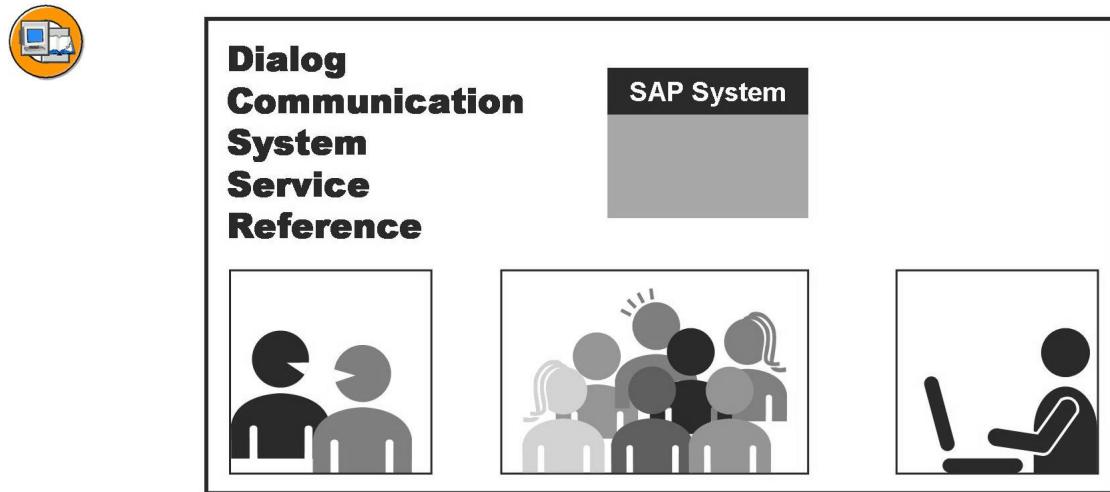


Figure 35: SAP User Types

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 his or her password himself or herself.
- 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 CUA (central user administration).

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 begun 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

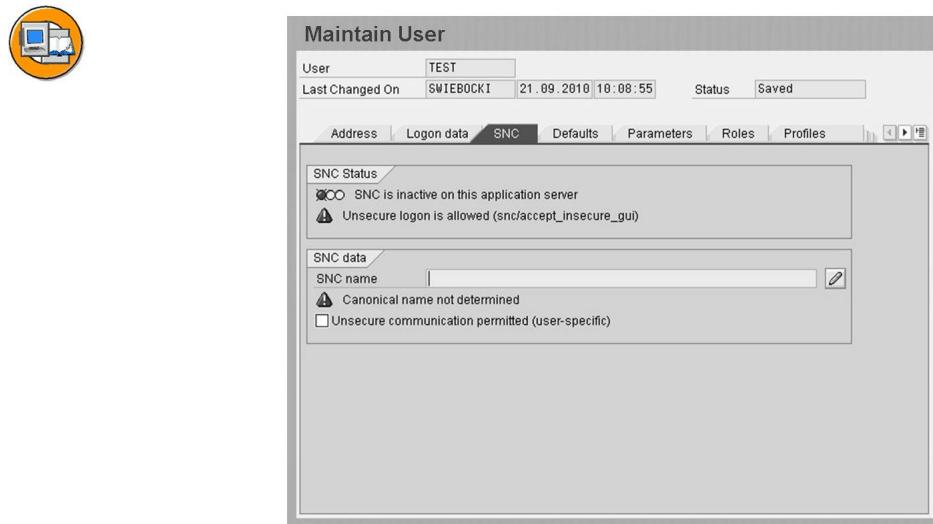


Figure 36: User Master Record: SNC

SNC

The SNC (Secure Network Communications) functions allow you to use an external security product to secure the communications between SAP System components (for example, between application servers and frontend 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

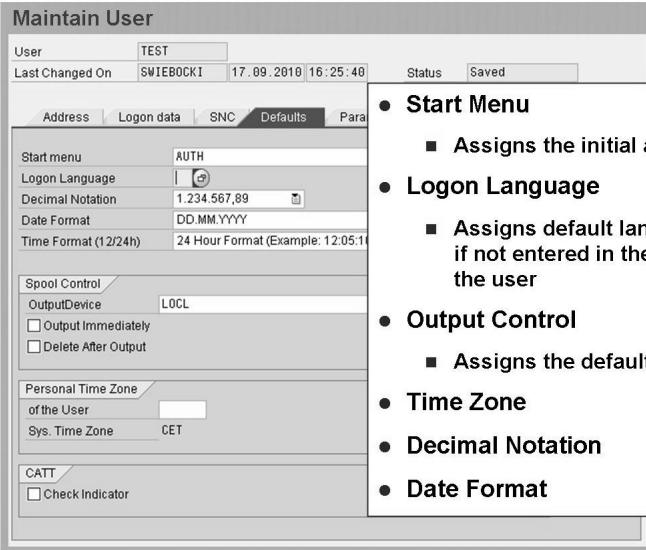


Hint: It is the customer's responsibility to make sure that the purchased network security products from any manufacturer does not conflict with local legislation for cryptography.

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

○



- **Start Menu**
 - Assigns the initial area menu
- **Logon Language**
 - Assigns default language to be used if not entered in the logon screen by the user
- **Output Control**
 - Assigns the default printer
- **Time Zone**
- **Decimal Notation**
- **Date Format**

Figure 37: User Master Record: Defaults

2011

© 2011 SAP AG. All rights reserved.

83 

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 the 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

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

Output Device

- (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 usual for your country.

Tab Page: Parameters

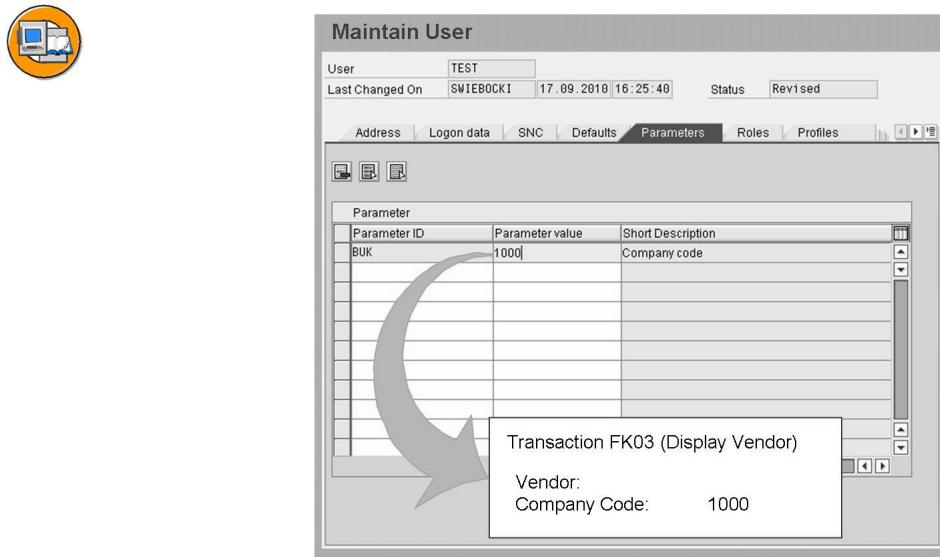


Figure 38: User Master Record: Parameters

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



Maintain User

User	TEST	Last Changed On	SWIEBOCKI	17.09.2010	16:25:48	Status	Revised
Logon data SNC Defaults Parameters Roles Profiles Groups Help							
New Delete Copy Cancel Role Role							
Reference user for additional rights							
Role Assignments							
St.	Role	Type	Valid From	Valid to	Name	Edit	
<input checked="" type="checkbox"/>	ADM940_R6B		17.09.2010	31.12.9999	Rolle für den ADM940	Up	
<input checked="" type="checkbox"/>	SAP_J2EE_ADMIN		28.09.2004	31.12.9999	Administration User for th	Down	
Singlerole							

Figure 39: User Master Record: Roles

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.

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.

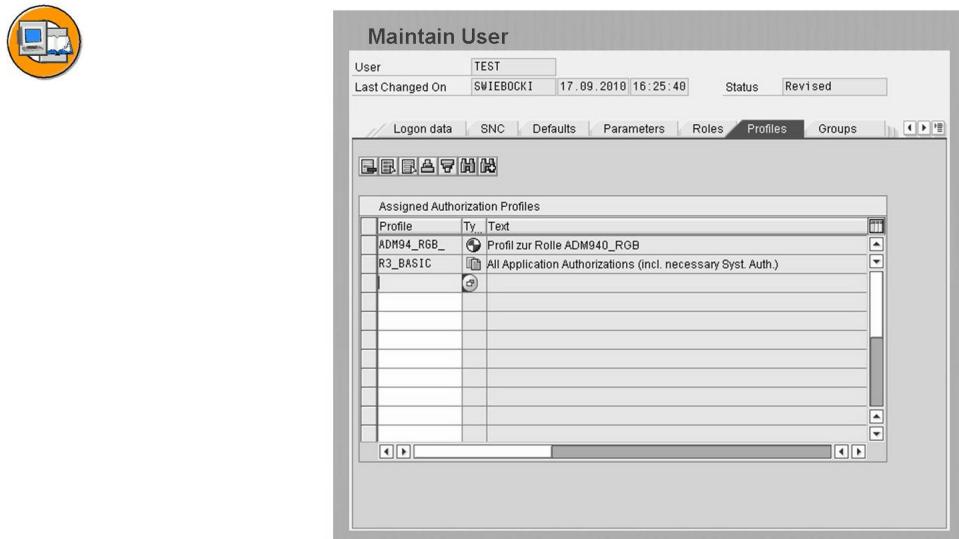


Figure 40: User Master Record: Profiles

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, since 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 and 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*: 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



Maintain User

User	TEST	Last Changed On	SWIEBOCKI	17.09.2010 16:25:48	Status	Revised																			
Defaults Parameters Roles Profiles Groups Personalization Lic...																									
<table border="1"><tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>Description</td><td>Personalization object key</td></tr><tr><td>Favorites in Web Dynpro Monitor of SEM</td><td>R_BCS_RELATED_LINKS</td></tr><tr><td>Workbench: Personalize Navigation</td><td>R_BCS_WORKBENCH</td></tr><tr><td>Balanced Scorecard: My Objects</td><td>R_CPM_BSC_MY_OBJECTS</td></tr><tr><td>MIC: Change Analysis Parameters</td><td>R_FOPC_ANA</td></tr><tr><td>MIC: Reporting Parameters</td><td>R_FOPC_REPORT</td></tr></table>														Description	Personalization object key	Favorites in Web Dynpro Monitor of SEM	R_BCS_RELATED_LINKS	Workbench: Personalize Navigation	R_BCS_WORKBENCH	Balanced Scorecard: My Objects	R_CPM_BSC_MY_OBJECTS	MIC: Change Analysis Parameters	R_FOPC_ANA	MIC: Reporting Parameters	R_FOPC_REPORT
Description	Personalization object key																								
Favorites in Web Dynpro Monitor of SEM	R_BCS_RELATED_LINKS																								
Workbench: Personalize Navigation	R_BCS_WORKBENCH																								
Balanced Scorecard: My Objects	R_CPM_BSC_MY_OBJECTS																								
MIC: Change Analysis Parameters	R_FOPC_ANA																								
MIC: Reporting Parameters	R_FOPC_REPORT																								

Figure 41: 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:

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



Maintain User

User	TEST
Last Changed On	SWIEBOCKI 17.09.2010 16:25:40
Status	Revised

Parameters Roles Profiles Groups Personalization LicenceData

Contractual User Type ID

Operational User
Requisitions/Confirmations
Only Basis Users
Development Workbench User
Enterprise HR User
SAP APO: Global Available-to-Promise
SAP APO: Production Planner
SAP APO: Supply Chain Planner
SAP APO: Collaborative Planner
SAP APO: Transportation Planner

Figure 42: 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).

Other Possibilities for User Maintenance and Change Documents

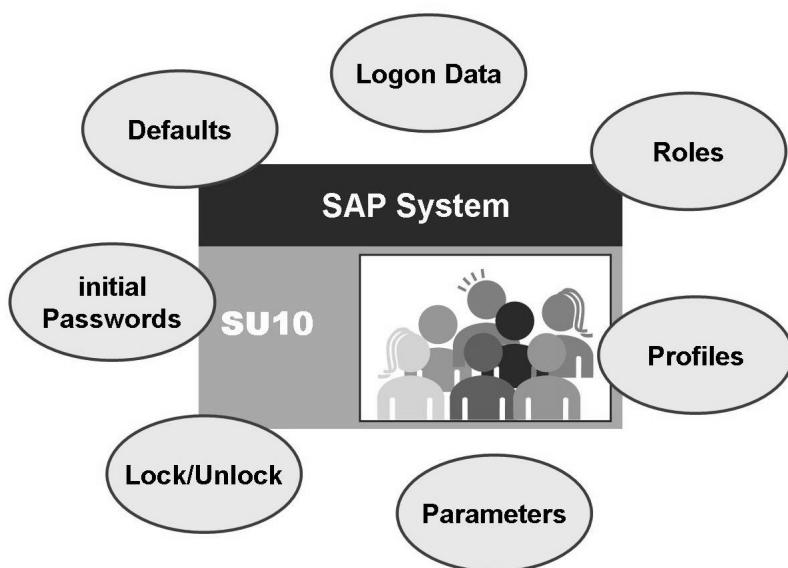


Figure 43: Mass Changes

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.

Logon 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 which changes in which system at which time.

The log contains several message levels, which 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.

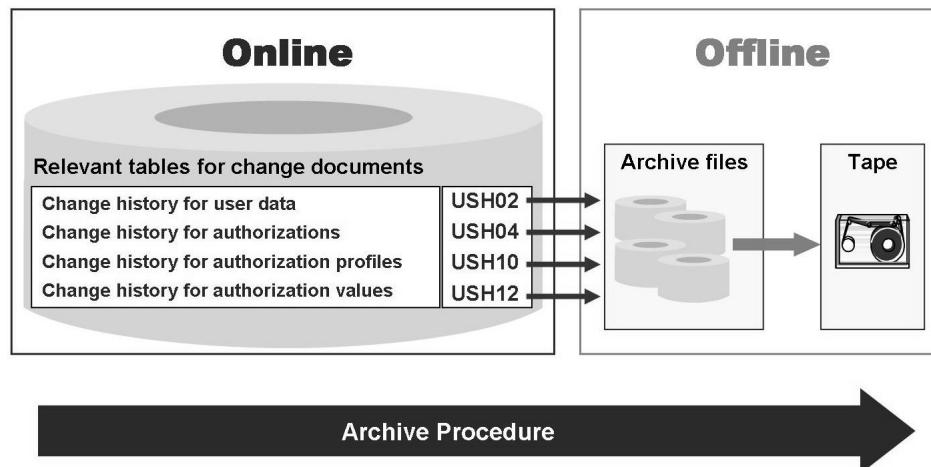


Figure 44: Change Documentation and Archiving

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*)

Exercise 4: Maintaining and Evaluating User Data

Exercise Objectives

After completing this exercise, you will be able to:

- Create and change user master records as well as evaluate changes
- Know the components of the user master record
- Use predefined work center examples
- Create multiple users in one step
- Understand the principle of the user buffer and evaluate the buffered user authorizations

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:

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

Task 2:

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

1. Enter address data of your choice.
2. Enter an initial password of your choice and assign the user to user group ZSUPER.

Initial password: _____

3. Assign the logon language that you have used yourself for logging on.
4. Save your user master record.

Continued on next page

Task 3:

Assign a predefined work center example to your new user master record by choosing the *Other Menu* button on the “*SAP Easy Access*” initial screen (on the application toolbar; [Shift+F5]).

1. Choose the role ADM940_BC_ADMIN.
2. Assign your new user GR##-ADM to the role.

Choose the *Assign users* button and enter your user ID. Accept your settings and have the user master record comparison performed automatically.

Task 4:

Switch from the *Other menu* display back to the SAP menu display.

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

1. Check whether a role is assigned to your user.

Which role?

-
2. If you are in “display mode” than change to “change mode” [Shift+F7] Link your user with another role. Choose the role ADM940_PLUS.

3. Are authorization profiles assigned to your user?

Which authorization profile(s)?

_____;
_____.

Task 5:

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.

Display the complete content for *Selection Criteria for User Attributes and Roles/Profiles*.

Does the list tell you that creating the user master record and assigning the user to roles were separate steps?

Continued on next page

Task 6:

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

1. Do you need to enter a logon language?

2. Specify your own **new** user password:

3. Check the user menu [Ctrl+F10]:

Which functions does it contain? List some examples.

4. Check the user buffer by calling the *User Buffer* function in your user menu (SAP menu).

How many authorizations exist?

For which authorization objects? List some examples.

Task 7:

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

Task 8:

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

1. In the *User* column, enter the following “6” user names and choose *Create*.

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

Continued on next page

2. Enter the user group ZGR## and the logon language that you use into the corresponding fields.
3. Save the user settings and check the result in the change log for a given user entry.



Hint: As of Web Application Server 7.0, 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” pushbutton [Shift+F8].

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

Solution 4: Maintaining and Evaluating User Data

Task 1:

1. Create a new user group ZGR## with a description of your choice.
 - a) **SAP Menu:**
→ *Tools* → *Administration* → *User Maintenance* → *User Groups*, (transaction code “SUGR”).
Enter ZGR## and choose *Create [F8]*.
Enter a description in the field *Text* and choose *Save [Ctrl+S]*.

Task 2:

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

1. Enter address data of your choice.
 - a) **SAP Menu:**
→ *Tools* → *Administration* → *User Maintenance* → *Users*, (transaction code “SU01”).
Enter GR##-ADM and choose *Create [F8]*.
Enter your choice of data under *Address*. “*Last name*” is mandatory.
2. Enter an initial password of your choice and assign the user to user group ZSUPER.
Initial password: _____
 - a) Setting possible on the *Logon Data* tab page
3. Assign the logon language that you have used yourself for logging on.
 - a) Setting possible on the *Defaults* tab page.
4. Save your user master record.
 - a) Save your user master record.

Continued on next page

Task 3:

Assign a predefined work center example to your new user master record by choosing the *Other Menu* button on the “*SAP Easy Access*” initial screen (on the application toolbar; [Shift+F5]).

1. Choose the role ADM940_BC_ADMIN.
 - a) Choose the role ADM940_BC_ADMIN.
2. Assign your new user GR##-ADM to the role.

Choose the *Assign users* button and enter your user ID. Accept your settings and have the user master record comparison performed automatically.

- a) Assign the new user *GR##-ADM* to this role. To do this, choose *Assign users* [Ctrl+Shift+F9] on the “*SAP Easy Access*” initial screen.
Enter the user ID and choose *Add users* [Ctrl+F4].

Ensure that the user master records are compared automatically by choosing *Yes* on the dialog box that appears next.

Task 4:

Switch from the *Other menu* display back to the SAP menu display.

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

1. Check whether a role is assigned to your user.

Which role?

-
- a) **Menu → SAP Menu** [Ctrl+F11]

SAP Menu:

→ **Tools → Administration → User Maintenance → Users**,
(transaction code “SU01”).

Answer: YES. A role is assigned on the "Roles" tab page.

- b) ADM940_BC_ADMIN.
2. If you are in “display mode” than change to “change mode” [Shift+F7] Link your user with another role. Choose the role ADM940_PLUS.
 - a) Enter ADM940_PLUS on the "Roles" tab page.

3. Are authorization profiles assigned to your user?

Which authorization profile(s)?

_____;

Continued on next page

-
- a) Go to the “Profiles” tab page. Assigned authorization profiles:
ADM94_BC_A;
ADM94_PLUS.
 - b) Save the new user data.

Task 5:

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.

Display the complete content for *Selection Criteria* for *User Attributes* and *Roles/Profiles*.

Does the list tell you that creating the user master record and assigning the user to roles were separate steps?

-
- a) **SAP Menu:**

→ **Tools** → **Administration** → **User Maintenance** → **Information System** → **Change Documents** → “**For Users**”.

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:

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

1. Do you need to enter a logon language?

-
- a) **No**, the logon language is set in the user master record.

2. Specify your own **new** user password:

-
- a) Specify a new user password

3. Check the user menu [Ctrl+F10]:

Which functions does it contain? List some examples.

Continued on next page

-
- a) Transaction codes for:
- Users (SU01)
Display users (SU01D)
User mass maintenance (SU10)
Maintain user groups (SUGR)
Analyze user buffers (SU56) and
an additional submenu *Information System* with other entries.
4. Check the user buffer by calling the *User Buffer* function in your user menu (SAP menu).
- How many authorizations exist?

For which authorization objects? List some examples.

-
- a) **SAP Menu:** → *Tools* → *Administration* → *Monitor* → *User Buffer*, (transaction code “SU56”).
- The number of authorization objects displayed depends on the display mode. In the new display, only nine authorization objects are shown but in sum the *Number of Authorizations* are 13.
- **Note:** In the some older releases you can see direct the 13 authorization objects. The number of instances, however, is the same.
- b) S_TCODE (twice)
S_USER_AGR (twice)
S_USER_AUT
S_USER_GRP (three times)
S_USER_PRO
S_USER_SYS
P_TCODE
PLOG
S_ADRESS1

Continued on next page

Task 7:

1. 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.

Task 8:

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

1. In the *User* column, enter the following “6” user names and choose *Create*.

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

- a) **SAP Menu:**

→ *Tools → Administration → User Maintenance → User Mass Maintenance*, (transaction code “SU10”).

In the “User” column, enter the following user names and choose the *Create [F8]* icon.

2. Enter the user group ZGR## and the logon language that you use into the corresponding fields.

- a) *Logon data* tab page:

Enter the *user group* “ZGR##”.

Defaults tab page:

Enter the *Logon Language* “EN”.

Continued on next page

3. Save the user settings and check the result in the change log for a given user entry.



Hint: As of Web Application Server 7.0, 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” pushbutton [Shift+F8].

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

- a) Expand each of the individual logs by double-clicking the appropriate line “GR##-*”. If you want to, copy the generated initial passwords into the tables in the exercise section.



Hint: Another options would be 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 (SBWP, into “Private Folders” with a free *Title*.



Lesson Summary

You should now be able to:

- Create and change user master records
- Set the values on the tab pages of the user master record
- Define the differences between the user types
- Operate and implement mass maintenance
- Display and archive change documents for authorization assignment



Unit Summary

You should now be able to:

- Create and change user master records
- Set the values on the tab pages of the user master record
- Define the differences between the user types
- Operate and implement mass maintenance
- Display and archive change documents for authorization assignment

Unit 4

Working with the Role Maintenance

Unit Overview

Role maintenance is the central place in an SAP system where you set authorizations for users, and combine them into reusable blocks (roles). This unit describes all options and buttons in role maintenance. In practice, due to historical reasons this is also referred to as the *Profile Generator* or “PFCG”, which is the transaction code.

This unit is divided into three lessons to allow a step-by-step approach.



Unit Objectives

After completing this unit, you will be able to:

- Describe and explain the basic steps for assigning authorizations with the Role Maintenance
- Create new roles, change and copy roles, and specify their activities
- Display and maintain authorizations that were generated automatically
- Compare user master records directly in role maintenance “PFCG” or in user maintenance “SU01”
- Describe how to perform a mass comparison and state which report you can schedule for an automatic comparison
- Describe the use of Customizing roles
- Explain the advantages and disadvantages of composite roles
- Define the relationship between reference roles and derived roles
- Bundle frequently used transactions and map them with different instances using derived roles
- Describe how to perform a mass comparison and state, which report you can schedule for an automatic comparison
- Interpret the red, yellow, and green traffic lights for different field contents
- Describe the meaning of the icons in the PFCG authorization maintenance
- Define the hierarchy of status terms, and explain when which term is used
- Distinguish between the expert mode and simple maintenance for authorizations

- List additional functions that are accessible through the menu

Unit Contents

Lesson: Role Maintenance and Standard Roles	107
Exercise 5: Role Maintenance and Standard Roles	125
Lesson: Special ABAP Roles	144
Exercise 6: Special ABAP Roles	153
Lesson: Subtleties of Authorization Maintenance	172
Exercise 7: Subtleties of Authorization Maintenance	179

Lesson: Role Maintenance and 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.



Lesson Objectives

After completing this lesson, you will be able to:

- Describe and explain the basic steps for assigning authorizations with the Role Maintenance
- Create new roles, change and copy roles, and specify their activities
- Display and maintain authorizations that were generated automatically
- Compare user master records directly in role maintenance “PFCG” or in user maintenance “SU01”
- Describe how to perform a mass comparison and state which report you can schedule for an automatic comparison

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.

Basic Maintenance of Roles Using the Role Maintenance

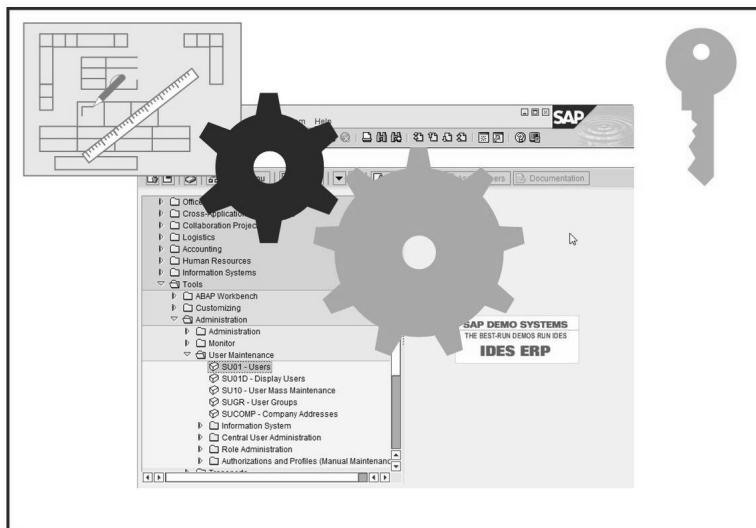


Figure 45: The Role Maintenance

What is the Role Maintenance?

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

In the 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. The 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.

The 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 need to maintain.

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

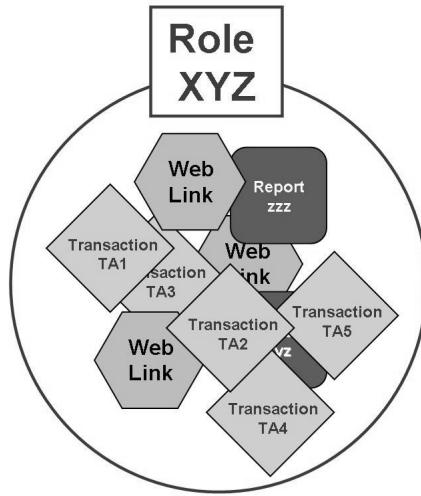


Figure 46: Roles

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.

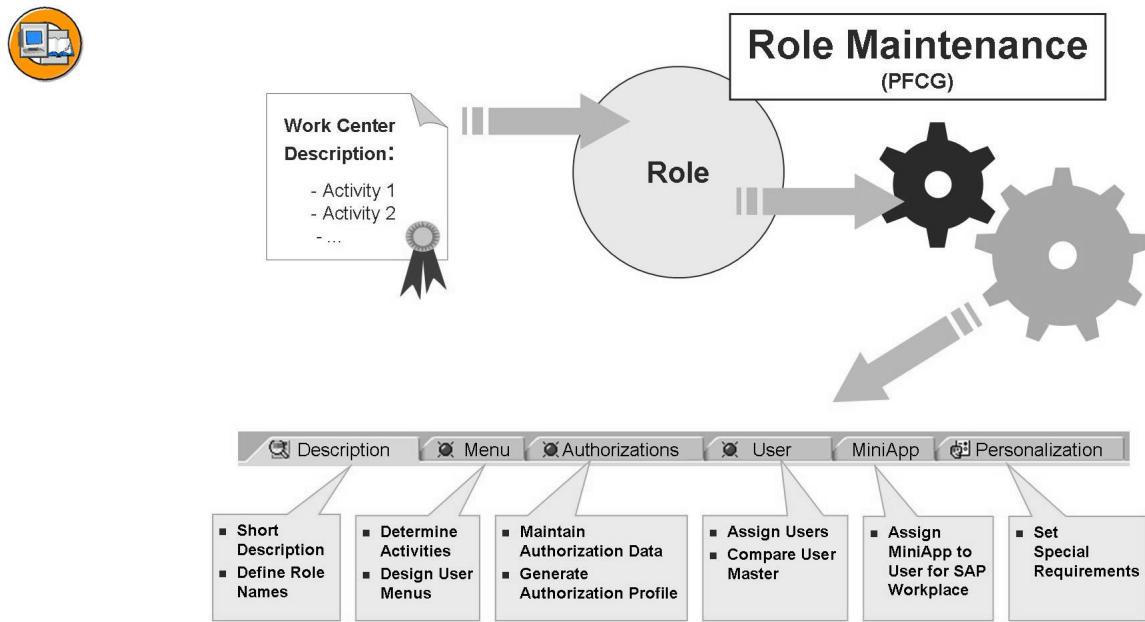


Figure 47: The Role Maintenance: Process Steps

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 the 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.
- Afterwards, 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.

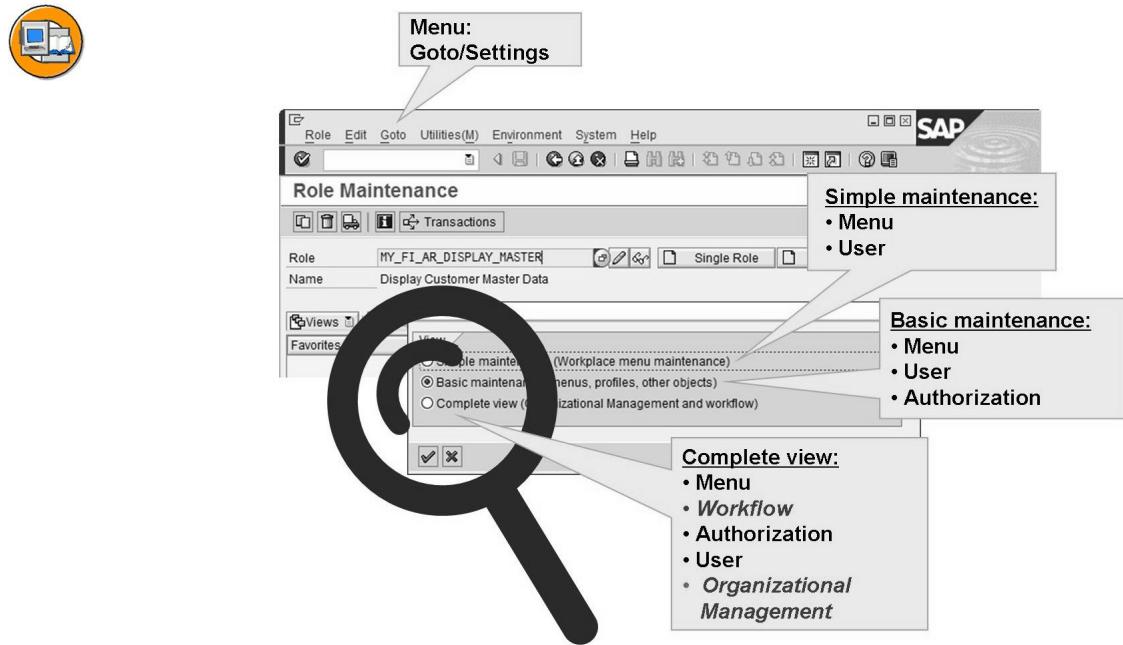


Figure 48: Role Maintenance: Views

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

So that the process of creating a role is easier to remember, all process steps are shown repeatedly in the form of a “to do” list in this lesson.

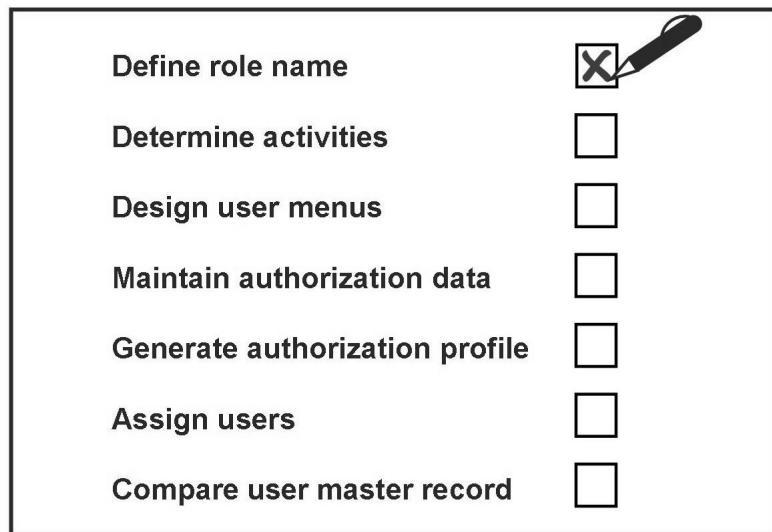


Figure 49: Process Steps: Defining Role Names

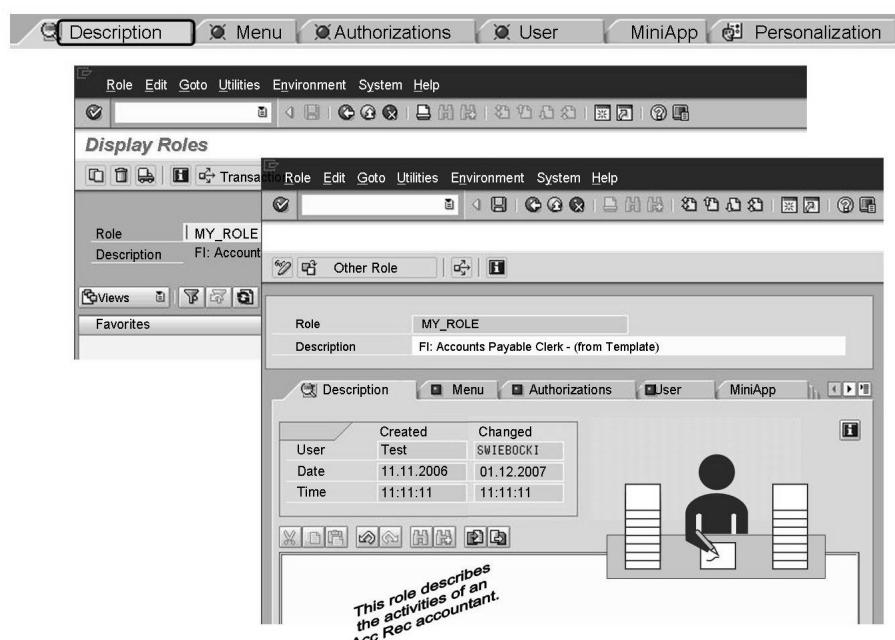


Figure 50: Defining the Role Name and Description

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 is, however, **not language-dependent**.



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 51: Process Step: Define Activities

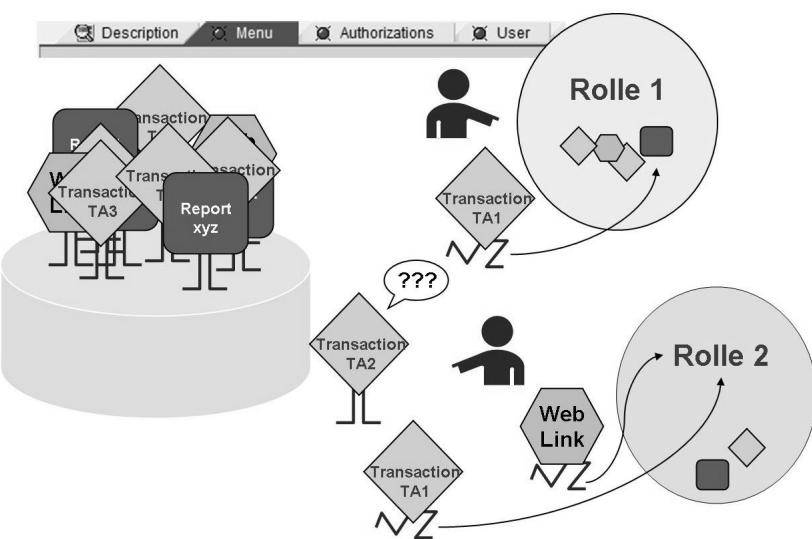


Figure 52: Defining Activities

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 the 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 “PFCCG”.

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.

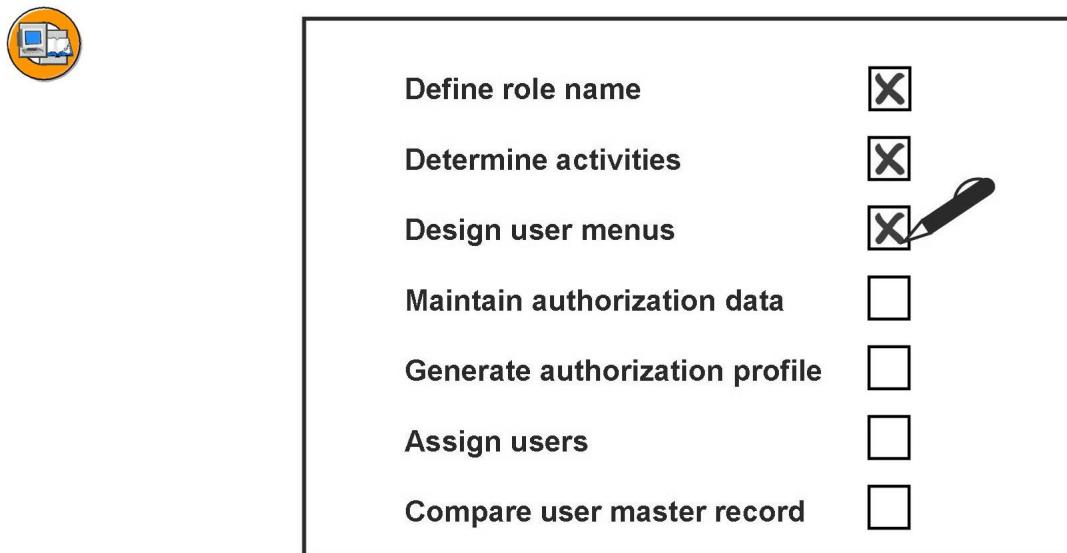


Figure 53: Process Step: Structuring Role Menus

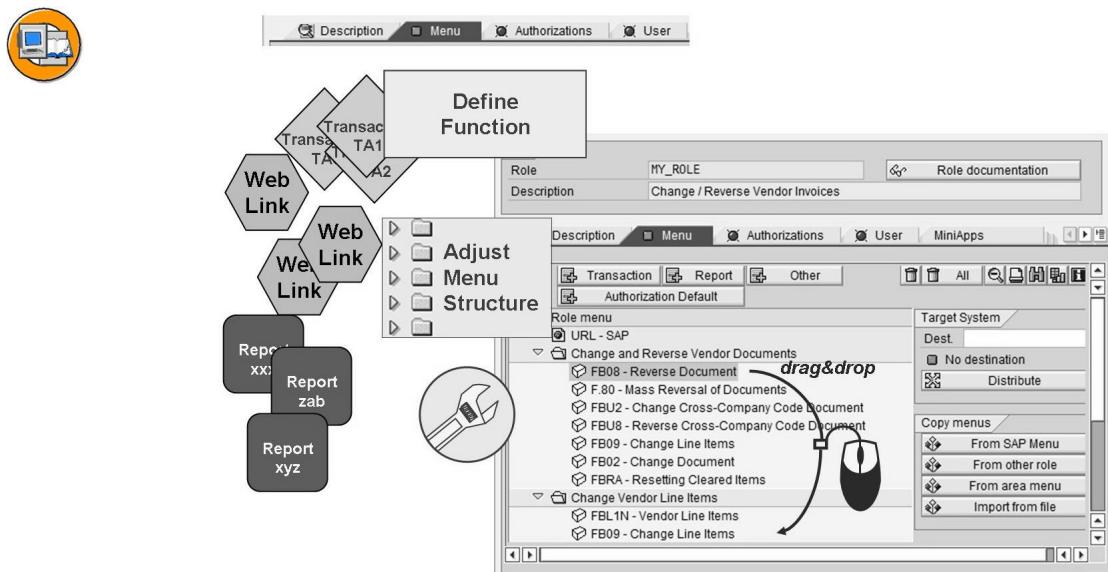


Figure 54: Creating and Structuring Menus

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). The 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.

As of Release 4.6C, you can also use transaction “ROLE_CMP” to compare and adjust role menus across systems.

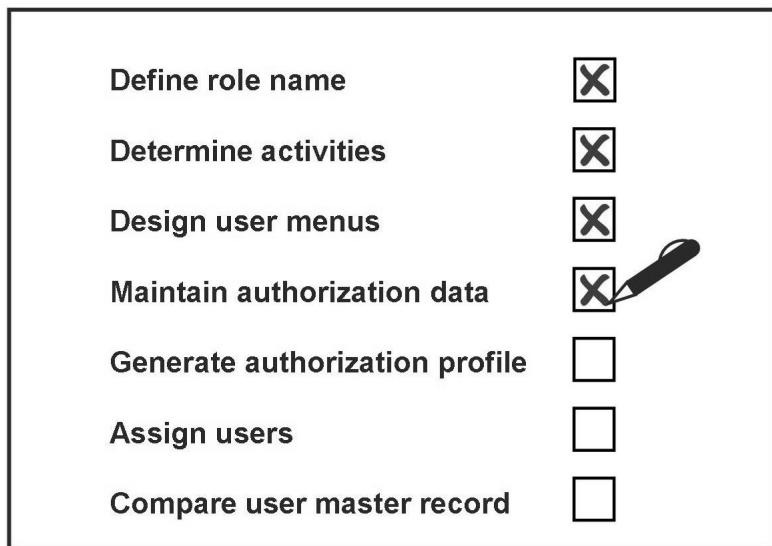


Figure 55: Process Step: Maintaining Authorization Data



The screenshot shows the SAP Role Maintenance screen. At the top, there are tabs for Description, Menu, Authorizations, and User. Below the tabs, a table displays a single role entry:

Role	MY_ROLE
Description	Change / R

Below the table, there are two panes. The left pane shows creation details: User ADM940-00, Date 30.03.2009, Time 22:36:28. It also lists 'Information About Authorization Profile' fields: Profile Name, Profile Text, and Status (Profile comparison required). The right pane lists 'MY_ROLE' authorizations:

- OAC Standard Updated Cross-application Authorization Objects Basis: Administration
- OAC Standard New Archiving Basis - Development Environment
- OAC Standard Old ABAP: Program Flow Checks Basis - Central Functions
- OAC Standard New Controlling Financial Accounting
- OAC Changed New
- OAC Changed New

At the bottom of the right pane, there is a section titled 'Maintain Authorization Data and Generate Profiles' containing buttons for 'Change Authorization Data' and 'Change authorization data Generation'. The 'Change Authorization Data' button is circled in red.

Figure 56: Maintaining Authorization Data

Creating the authorizations and authorization profiles:

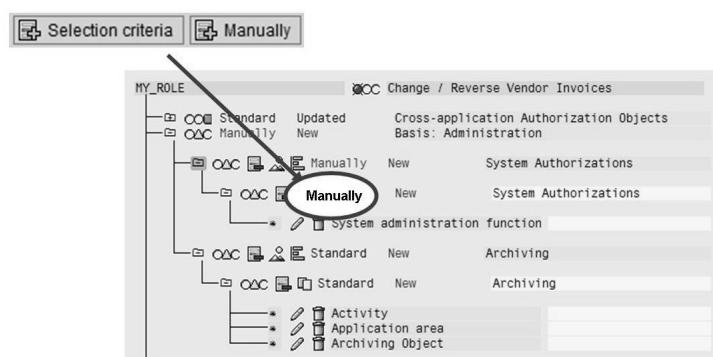
The Role Maintenance automatically generates authorizations based on the menu functions that you have chosen before. The Role Maintenance cannot, however, propose “default value” authorizations that are suitable for everyone in the company. Therefore, the authorization administrator must normally postprocess 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 postprocessing work.

In the example, the transaction “SO01” (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 postprocessing is necessary: The **Role Maintenance cannot know** if the users should have only **read access** or also **write access** to the files.



Adding Objects “Manually”



Always ask yourself the following question:

Why do I want to add this object manually?

- Isn't it better to offer the objects as Profile Generator
- Proposals in transaction SU24?
- Could the authorization proposal function in the menu support you in doing this?

Figure 57: Manual Insertion of Authorizations

Although the 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 have the 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.

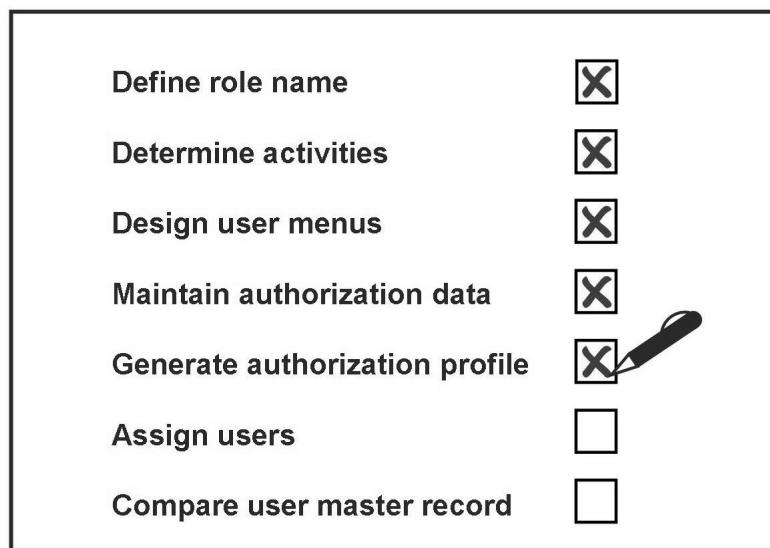


Figure 58: Process Step: Generating the Authorization Profile

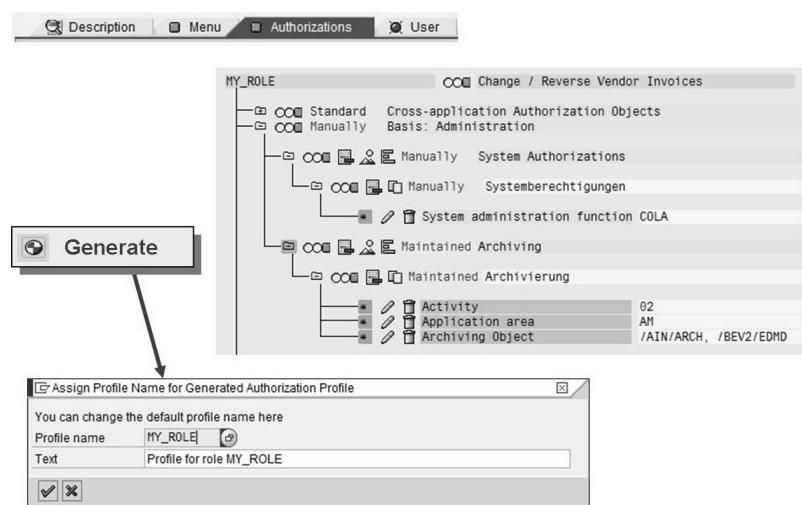


Figure 59: Generating the Authorization Profile

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, the 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 the Role Maintenance. It depends on the fields used and on the number of entries.

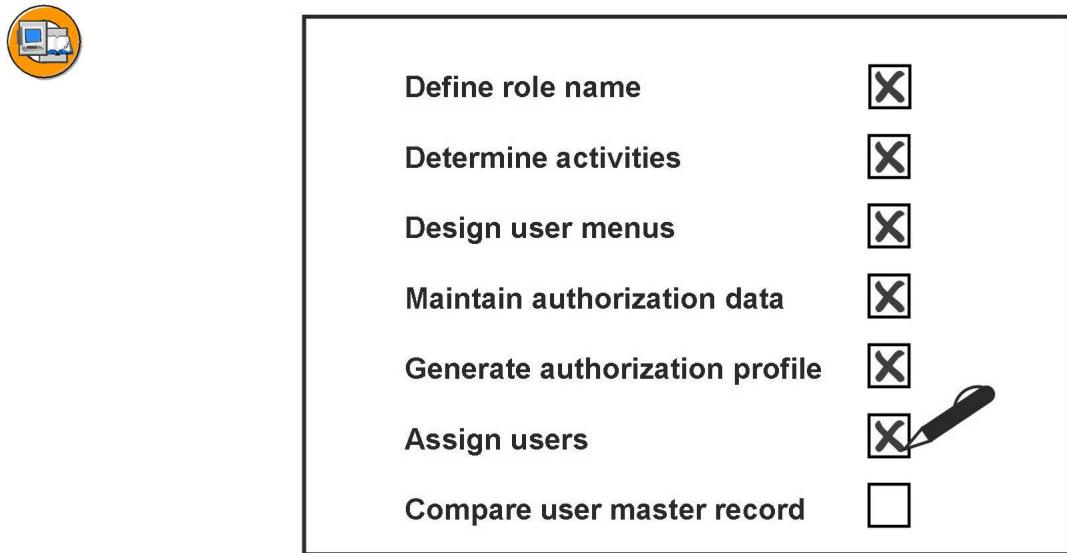


Figure 60: Process Step: Assigning Users

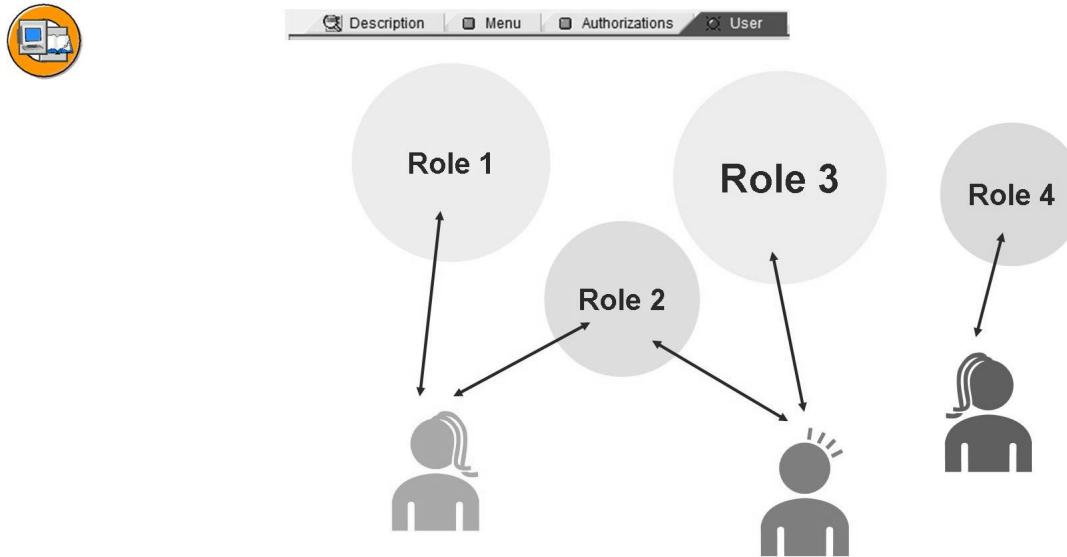


Figure 61: Assigning Users to Roles

Assigning users:

So that users are provided with the menu tree for their role when they log on to the system, you must assign roles to them.

You assign roles to users by adding the corresponding names to the list on the *User* tab page of the 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 only. 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 “**PFUD**”, (*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**”.

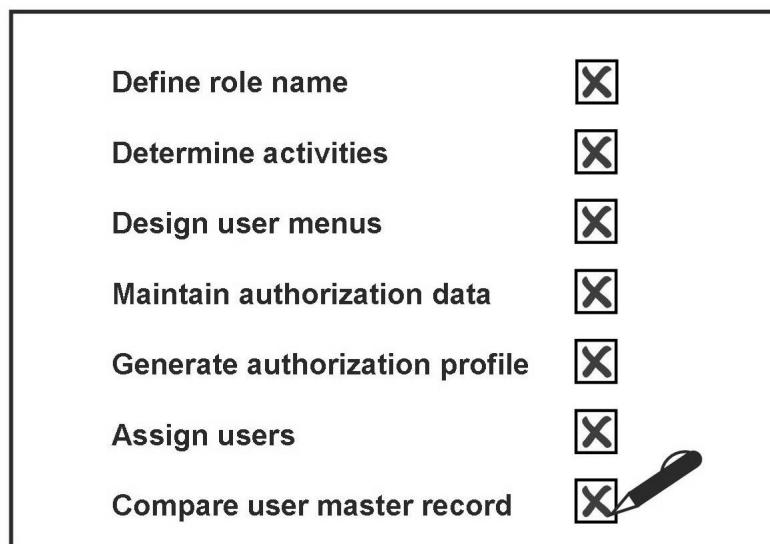


Figure 62: Process Step: Comparing the User Master Record

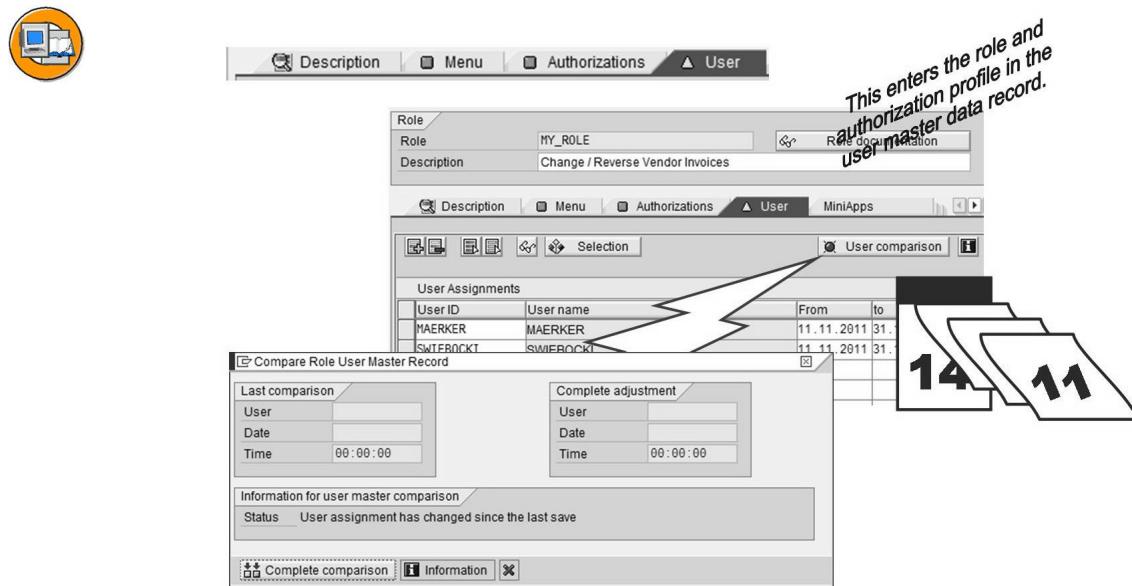


Figure 63: Comparing the User Master Record

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 the Role Maintenance (“User” tab page and “User Comparison” button). As a result of the comparison, the profile generated by the 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.

Exercise 5: Role Maintenance and Standard Roles

Exercise Objectives

After completing this exercise, you will be able to:

- Create roles with the Role Maintenance and determine their activities
- Check and maintain authorizations that were generated automatically
- Copy roles
- Assign users and perform a user comparison

Business Example

This role maintenance exercise deals with “basic maintenance” using the 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.

Task 1:

 **Note:** In task 1 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 of 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_AC-CREC_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

Continued on next page

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:	Scope	Scope	Scope	Scope
T Code				
MM01				
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

Continued on next page

Business area>>>	FI	SD	SD	MM
Work Place Description>>>	AccRec	SDClerk	SDMan	Whouse
SAP R/3 Links: T Code	Scope	Scope	Scope	Scope
F-18	x			
F-26	x			
F-28	x			

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

Task 2:

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. Go to the Menu tab and select the corresponding transaction in accordance with the sample authorization concept (**Roles for Transaction Codes** table from task 1 of this exercise).

Create a folder with the name WWW Links.

Add a Web address with the name SAP and the URL <http://www.sap.com> to this folder.

Check whether this Web address works by using a right mouse click and choosing *Execute*.

Create another Web address with a link to the homepage of your company.

Save your role.

3. Go to the Authorizations tab page. Select the normal mode, indicated by the pencil in the lower half of the screen (*Change Authorization Data*).

Define the organizational levels:

- Company code: 1000,
- Warehouse number/complex: *,
- Sales organization: 1000,
- Distribution Channel: *,
- Plant: 1000, 1100, 1200.

Display the technical names for the authorizations (*Utilities/Settings* menu).

Continued on next page

4. 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:

5. 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?

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?

6. Generate the authorization profile for your role. Assign the following profile name:

GR##_MM_01

7. Exit the authorization maintenance screen and check the status of your authorization profile in the information section of the Authorizations tab.

What is the status of your authorization profile?

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

Continued on next page

Task 3:

Create the role with authorizations for a warehouse supervisor.

Enter a short description, and save.

1. Use the role name GR##_MM_IM_POST.
2. Go to the Menu tab and select the transaction in accordance with the sample authorization concept (**Roles for Transaction Codes** table from task 1 of this exercise).

Create a folder and use Drag&Drop to move all transactions to this folder.
Save your role.

3. Go to the Authorizations tab page. Select the normal mode (*Change authorization data*).

Define the organizational levels:

- Plant: 1000, 1100, 1200.

Display the technical names for the authorizations (*Utilities/Settings* menu).

4. Make the following adjustments:

Add the authorization values 561 and 562 to the authorization values for the Movement Type field of the authorization object M_MSEG_BWA.

Then set full authorization for all open authorization values.

5. Generate the authorization profile for your role. Accept the proposed profile name. Exit the maintenance of this role.

Task 4:

The following exercise is optional.

Use the role GR##_MM_IM_POST as a template to create the role GR##_MM_IM_POST1200. To do this, choose the **Copy Role** icon and copy all settings from the template.

1. In role maintenance “PFCG”, enter the role GR##_MM_IM_POST, and choose the option *Copy Role*. Confirm the query that appears by choosing *Copy All*. After copying it, open the role in maintenance mode (F6).

Go to the Menu tab page.

Can you select other activities (menu entries, transaction codes, reports, for example) or delete existing activities?

-
2. Go to the Authorizations tab page.

Continued on next page

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

What is the status of the authorization profile?

Select the normal mode (*Change authorization data*).

Did the system copy the authorizations of the copy template?

Assign **only** the value *1200* to the organizational level *Plant*.

Generate the authorization profile for your role and accept the proposed profile name.

Exit the authorization maintenance screen and check the status of your authorization profile in the information section of the Authorizations tab.

What is the status of your authorization profile?

Task 5:

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. Create a role using the PFCG transaction. Enter a short description, and 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.
Save the menu.
3. Go to the Authorizations tab page.
Set full authorization for all open authorization field values.
Generate the profile and accept the proposed profile name.
4. Go to the User tab page.
What is the status of the 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).

Continued on next page

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

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

What happens during the user compare process?

6. 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.

7. Display the user master record of user GR##-MM1.

Is the user linked to roles? If yes, to which ones?

Are authorization profiles assigned to the user?

Solution 5: Role Maintenance and Standard Roles

Task 1:

 **Note:** In task 1 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 of 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_AC-CREC_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:	Scope	Scope	Scope	Scope
T Code				
MM01				
MM02				
MM03	x	x	x	x
MM19	x	x	x	x
MM04	x	x	x	x

Continued on next page

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

Continued on next page

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

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”).

Choose *Goto / Settings* and then the “Basic Maintenance” view. Enter a name for the role and create it (F5). Enter a short description, and save your role.

2. Go to the Menu tab and select the corresponding transaction in accordance with the sample authorization concept (**Roles for Transaction Codes** table from task 1 of this exercise).

Create a folder with the name WWW Links.

Add a Web address with the name SAP and the URL <http://www.sap.com> to this folder.

Check whether this Web address works by using a right mouse click and choosing *Execute*.

Create another Web address with a link to the homepage of your company.

Continued on next page

Save your role.

- a) A brief extract from the table in task 1 is provided here to make the task more comprehensible.

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

Use the *Transaction* button to select the following transactions:

MM03
MM04
MM19

To create a folder, choose the *Create folder* icon.

To create a Web address, choose *Web address or file* in the context menu of the *Transaction* button. Enter a description in the *Text* field and a URL into the field *Web address or file* in the format:
<http://www.sap.com>

Save your role.

3. Go to the Authorizations tab page. Select the normal mode, indicated by the pencil in the lower half of the screen (*Change Authorization Data*).

Define the organizational levels:

- Company code: 1000,
- Warehouse number/complex: *,
- Sales organization: 1000,
- Distribution Channel: *,
- Plant: 1000, 1100, 1200.

Display the technical names for the authorizations (*Utilities/Settings* menu).

- a) 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.

Display the technical names for the authorizations.

Menu: → Utilities → Technical names on

4. Check the traffic light symbol status.

Continued on next page

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) Cross-application authorization objects; AAAB
- b) 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

5. 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?

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) To do this, choose the asterisk before the open field value.
Status: *Maintained*, traffic light: *Green*.
- b) To do this, click the traffic light symbol at the top hierarchy level with the left mouse button, and confirm the assignment of full authorization for the subtree.

The indicator then switches the structure to *green*.

Continued on next page

6. Generate the authorization profile for your role. Assign the following profile name:

GR##_MM_01

- a) Choose the *Generate* icon and assign the profile name GR##_MM_01.
7. Exit the authorization maintenance screen and check the status of your authorization profile in the information section of the Authorizations tab.

What is the status of your authorization profile?

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

- a) Status: *Authorization profile is generated.*

Task 3:

Create the role with authorizations for a warehouse supervisor.

Enter a short description, and save.

1. Use the role name GR##_MM_IM_POST.

- a) **SAP Menu:**

→ *Tools* → *Administration* → *User Maintenance* → *Role Administration* → *Roles*, (transaction code “PFCG”).

Enter the role name GR##_MM_IM_POST. Use F5 to create the role GR##_MM_IM_POST and write a short description. Save your role.

2. Go to the Menu tab and select the transaction in accordance with the sample authorization concept (**Roles for Transaction Codes** table from task 1 of this exercise).

Create a folder and use Drag&Drop to move all transactions to this folder. Save your role.

- a) Select the following transactions using the *Transaction* button or using the button *from the SAP Menu* combined with *Search*:

MB1C

MB90

VL21

3. Go to the Authorizations tab page. Select the normal mode (*Change authorization data*).

Define the organizational levels:

Continued on next page

- Plant: 1000, 1100, 1200.

Display the technical names for the authorizations (*Utilities/Settings* menu).

- a) When assigning the organizational levels, you can specify multiple values for a field by choosing the *More Values* button.

Menu: → *Utilities* → *Technical names on*

4. Make the following adjustments:

Add the authorization values 561 and 562 to the authorization values for the Movement Type field of the authorization object M_MSEG_BWA.

Then set full authorization for all open authorization values.

- a) You can enter the field values for the authorization object M_MSEG_BWA by clicking the pencil. You can find this authorization object in the object class MM_B.

Assigning full authorization: To do this, click the traffic light symbol at the top hierarchy level, and confirm the assignment of full authorization.

5. Generate the authorization profile for your role. Accept the proposed profile name. Exit the maintenance of this role.
 - a) Choose the *Generate* icon.

Task 4:

The following exercise is optional.

Use the role GR##_MM_IM_POST as a template to create the role GR##_MM_IM_POST1200. To do this, choose the **Copy Role** icon and copy all settings from the template.

1. In role maintenance “PFCC”, enter the role GR##_MM_IM_POST, and choose the option *Copy Role*. Confirm the query that appears by choosing *Copy All*. After copying it, open the role in maintenance mode (F6).

Go to the Menu tab page.

Can you select other activities (menu entries, transaction codes, reports, for example) or delete existing activities?

-
- a) Copy the role GR##_MM_IM_POST to the new role GR##_MM_IM_POST1200 by choosing the *Copy Role* icon.
Choose *Change*.
 - b) Yes. The copied role behaves like a newly created role.
2. Go to the Authorizations tab page.

Continued on next page

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

What is the status of the authorization profile?

Select the normal mode (*Change authorization data*).

Did the system copy the authorizations of the copy template?

Assign **only** the value *1200* to the organizational level *Plant*.

Generate the authorization profile for your role and accept the proposed profile name.

Exit the authorization maintenance screen and check the status of your authorization profile in the information section of the Authorizations tab.

What is the status of your authorization profile?

a) Status: *Current version not generated*

b) Did the system copy the authorizations of the copy template?

Yes, they were copied too.

Choose *Organizational Levels*. Plants 1000, 1100, and 1200 have been copied. Delete the entries for plants 1000 and 1100.

c) Status: *Authorization profile is generated*

Task 5:

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. Create a role using the PFCG transaction. Enter a short description, and save your role.

a) **SAP Menu:**

→ **Tools** → **Administration** → **User Maintenance** → **Role Administration** → **Roles**, (transaction code “PFCG”).

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.

Continued on next page

Save the menu.

- a) Go to the "Menu" tab page and copy the menu of the predefined role SAP_BC_SRV_USER by choosing *From Other Role* under *Copy Menus*. Copy all listed menu nodes (transaction codes).
3. Go to the Authorizations tab page.
Set full authorization for all open authorization field values.
Generate the profile and accept the proposed profile name.
 - a) Assign full authorization? To do this, click the traffic light symbol at the top hierarchy level (next to the role name), and confirm the assignment of full authorization.
Then choose the *Generate* icon and use the proposed name.
4. Go to the User tab page.
What is the status of the 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 / Settings*). Ensure that a user master adjustment (record comparison) is automatically performed when you save.

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

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

Continued on next page

What happens during the user compare process?

- a) The status display of the tab page is green (it may be yellow if you have **not** set *Automatic User Adjustment when Saving Role* by choosing *Utilities → Settings* and checking the appropriate checkbox).
 - b) 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.
6. 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) **SAP Menu:**

→ *Tools → Administration → User Maintenance → Role Administration → Roles*, (transaction code “PFCG”).

Call the role ADM940_PLUS by choosing “Change”.

Go to the *User* tab page and assign the following users by entering their names in the *User ID* column. Remember to save your user assignment and to compare the master records.

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

7. Display the user master record of user GR##-MM1.

Is the user linked to roles? If yes, to which ones?

Continued on next page

Are authorization profiles assigned to the user?

a) **SAP Menu:**

→ **Tools** → **Administration** → **User Maintenance** → **Users**,
(transaction code “SU01”). “SU01”).

Yes, the user is linked to the roles:

ADM940_PLUS

GR##_BC_PORTALS.

b) Yes. Authorization profiles are assigned to the user.

ADM94_PLUS

T-..... (is a profile generated by you, and therefore has a name chosen by you).



Lesson Summary

You should now be able to:

- Describe and explain the basic steps for assigning authorizations with the Role Maintenance
- Create new roles, change and copy roles, and specify their activities
- Display and maintain authorizations that were generated automatically
- Compare user master records directly in role maintenance “PFCG” or in user maintenance “SU01”
- Describe how to perform a mass comparison and state which report you can schedule for an automatic comparison

Lesson: Special ABAP 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.



Lesson Objectives

After completing this lesson, you will be able to:

- Describe the use of Customizing roles
- Explain the advantages and disadvantages of composite roles
- Define the relationship between reference roles and derived roles
- Bundle frequently used transactions and map them with different instances using derived roles
- Describe how to perform a mass comparison and state, which report you can schedule for an automatic comparison

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.

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.

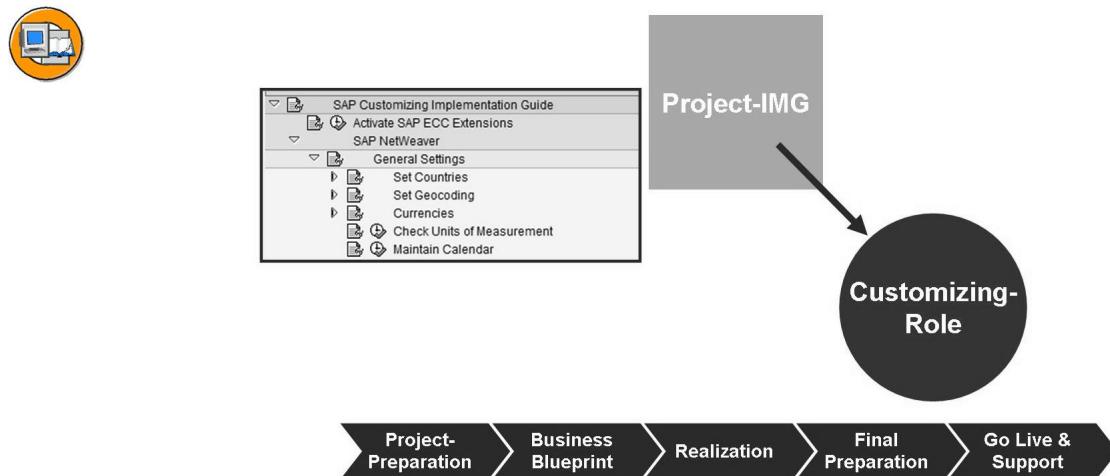


Figure 64: Customizing Roles



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.



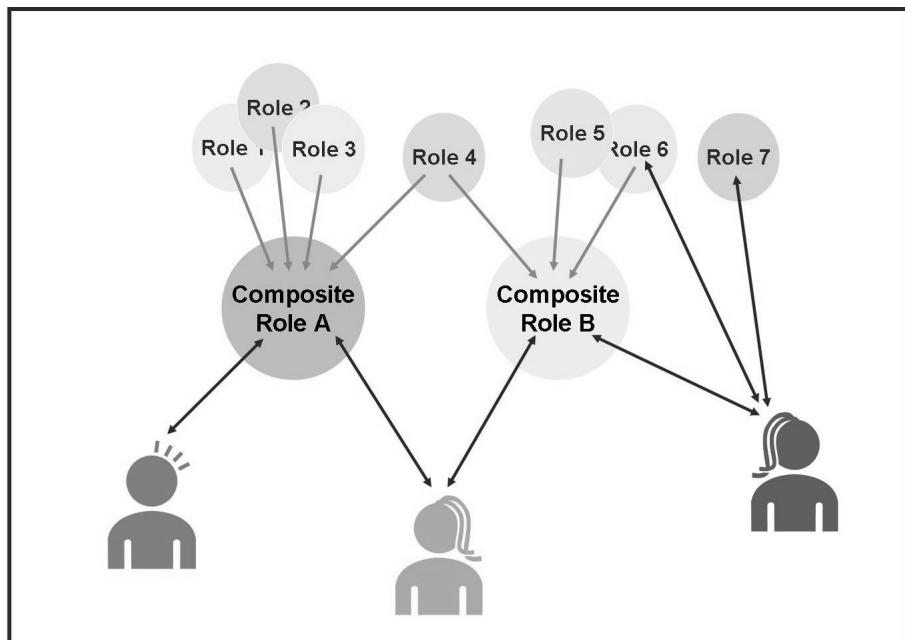
Hint: Since Customizing activities are performed on a project-related basis and for a limited period, you should maintain the end date for the assigned users. This ensures that the users assigned to the role lose the authorization for the projects/project views assigned upon completion of the project. This only applies, of course, if the user comparison is regularly performed.

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 of Support department to assign authorizations.

Advantages of composite roles:

- One work center
- One composite role
- One assignment
- One central menu

**Figure 65: 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 concept 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.

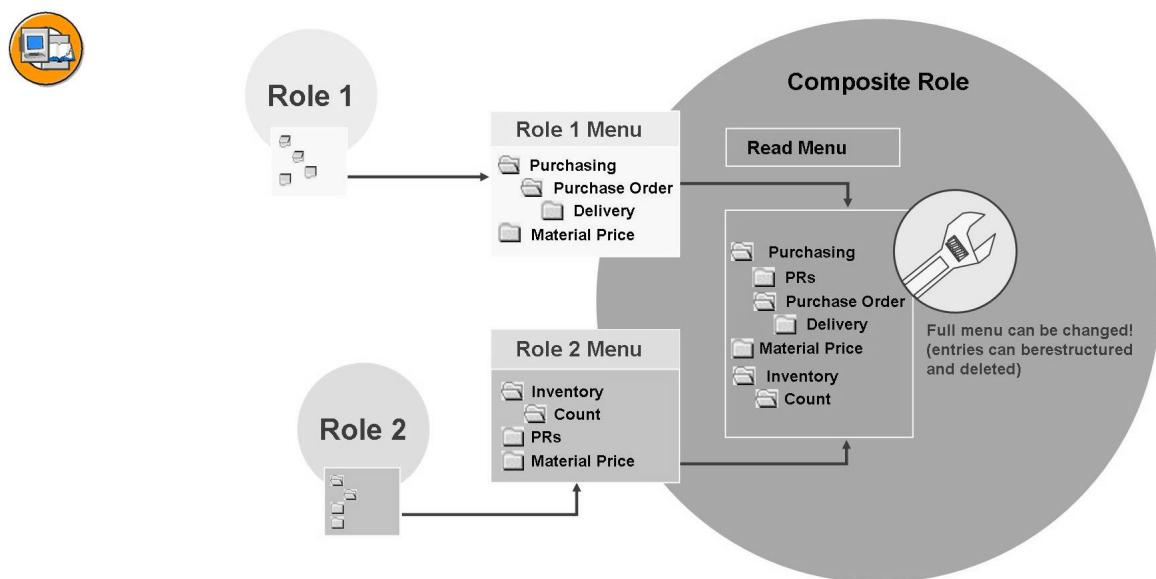


Figure 66: Menus of Composite Roles

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 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, the Role Maintenance allows you to completely rebuild the menu tree or process only the changes. If you choose the latter option, the 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 of 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).

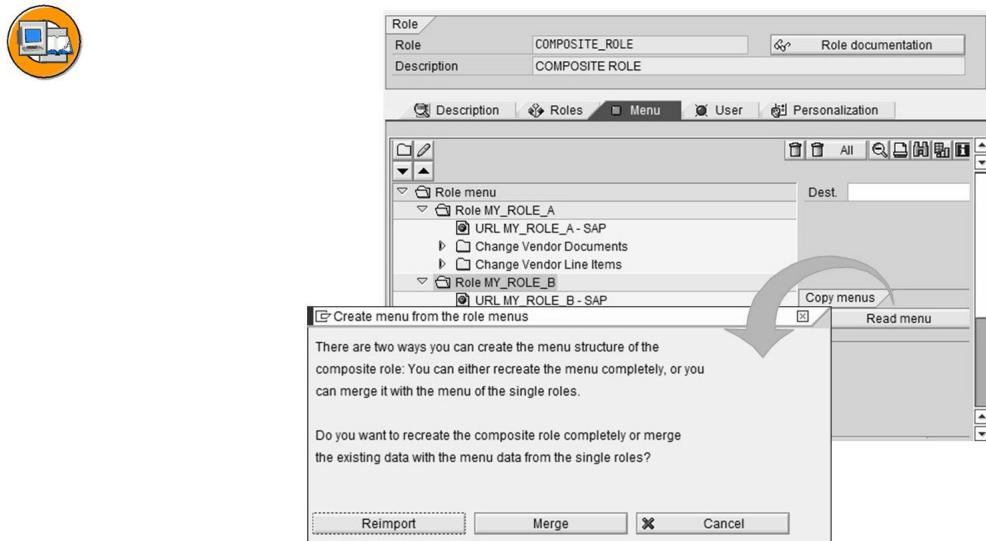


Figure 67: Building Composite Role Menus

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: Since release 4.6D, 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*.

Reference (Root) Roles and Derived Roles

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, 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.

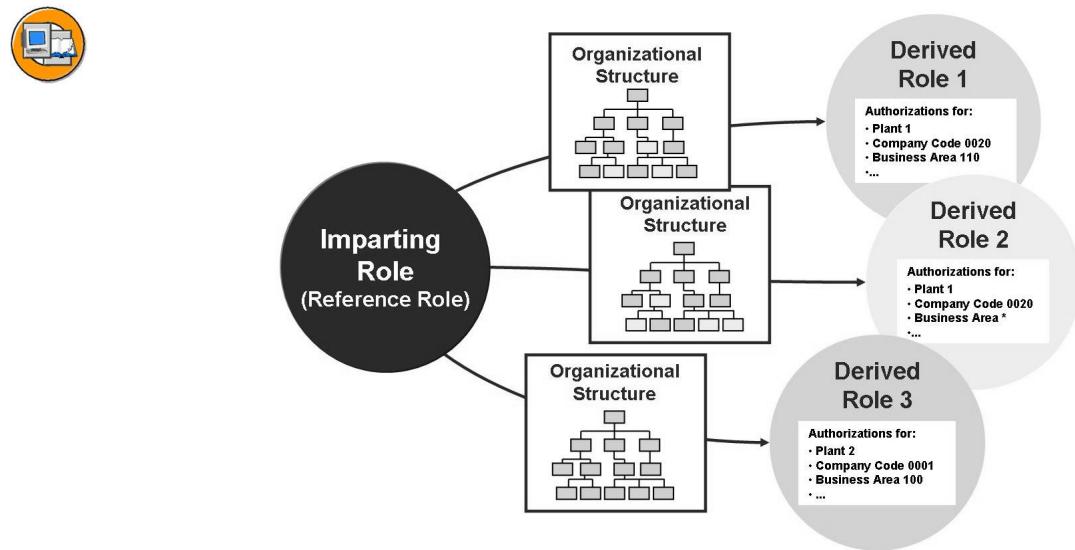


Figure 68: Derived Roles

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:

1.) 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).

2.) 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.

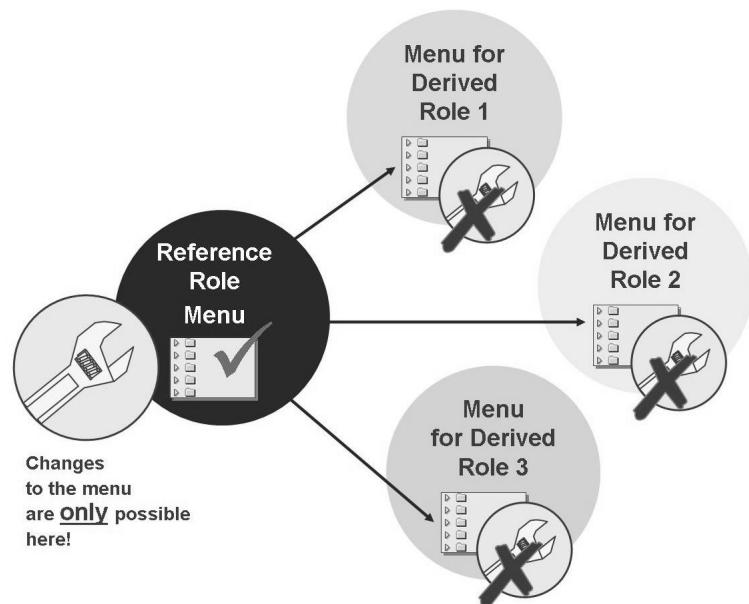


Figure 69: Menus of Derived Roles

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.

Exercise 6: Special ABAP Roles

Exercise Objectives

After completing this exercise, you will be able to:

- Work with composite roles and predefined work center examples
- Design user menus
- Create derived roles with the Role Maintenance and determine their activities
- Check and maintain authorizations that were generated automatically
- Explain the difference between derived and copied roles
- Describe differences between the master record comparison from SU01 and from PFCG

Business Example

This exercise is concerned with advanced role maintenance. The exercises should provide ideas about how you composite, reference, and derived roles can simplify your administration work.

Task 1:

Create the composite role GR##_MM_WHOUSE.



Hint: Ensure that you use the *Create Comp. Role* button on the initial screen of the Role Maintenance.

1. Enter a short description, and save your composite role.

If you look at the tab pages, what do you notice?

2. Go to the Roles tab page.

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.

Continued on next page

3. Go to the Menu tab page and 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; you can, however, move or rename them).

Save your composite role.

4. Go to the User tab page and assign user GR##-MM1. Save your user assignment.
5. Perform a user master comparison.

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.

1. Which roles is the user assigned?

If your user GR##-MM1 does not yet have the role ADM940_PLUS, assign the role and perform a user master comparison.

Display the authorization profiles. How many profiles are assigned?

_____ authorization profiles

Why are there fewer profiles than roles?

Continued on next page

Task 4:

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. Set up a user-specific favorites list by defining the transactions “MM03” and “MB1C” as favorites and adding any Web address.
2. Try to start some of the transactions, for example, “MM03”, and display the accounting view of material *P-100* in plant *1000*.

Can you also display the accounting view of material *P-100* in plant *3000*?

If not, why not?

-
3. Display the failed authorization check.



Hint: Menu path: → *System → Utilities → Display Authorization Check* (or transaction “SU53”)

Why were you not able to display material *P-100* in plant *3000*?

Log off as GR##-MM1.

Task 5:

Create a **derived** role GR##_MM_IM_POST1000 with authorizations for a warehouse supervisor in plant *1000*.

1. Write a short description. Assign the imparting role GR##_MM_IM_POST and save your role.
Display the inheritance hierarchy of the roles (Ctrl+Shift+F3 or the *Inheritance Hierarchy* icon).
2. Go to the Menu tab page.

Continued on next page

Can you select other activities (menu entries, transaction codes, reports, for example) or delete existing activities?

-
3. Go to the Authorizations tab page. Select the normal mode (*Change authorization data*).

Define the organizational levels:

- Plant: *1000*.

Did the system copy the authorizations of the imparting role?

-
4. Save the authorizations and accept the proposed profile name.

Copy the authorization data from the imparting role.

Did the system copy settings for organizational levels?

Ensure that users assigned to this derived role are only allowed to post data in plant *1000*.

5. Generate the authorization profile for your role.

Task 6:

The following exercise is optional.

Create a new single role GR##_SD_SALES by copying the predefined work center example ADM940_SD_SALES without user assignment.

1. Use the copy icon in transaction “PFCG”.

Task 7:

Change your copied role GR##_SD_SALES.

1. Change the description to a description specific to your group.

Go to the Menu tab page.

Display the technical names.

Expand all nodes of the menu and delete all transactions and nodes that are not intended for this role in the “*sample authorization concept*” (see lesson *Creating and Implementing an Authorization Concept* or look at the role distribution table **Example Authorization Concept** in the introduction to this exercise).

Save the changed user menu.

Continued on next page

2. Go to the Authorizations tab page.
Select the normal mode (*Change authorization data*).
Restrict the organizational levels as follows:
- Sales organization: *1000*.
Leave the default authorization values for all other organizational levels.
3. Assign full authorization for all other and open fields ("*").
4. Generate the authorization profile for your role. Accept the proposed profile name.

Task 8:

Create the missing three single roles of the *sample authorization concept*.

1.

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

Enter the role name and a short description. Fill the menu with the required transaction codes and import the proposed authorization values.

2. 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	1000
Business area	1000
Account type	D
Controlling area	1000
Division	*
Sales organization	1000
Distribution channel	*

Then assign the full authorization [*] for all remaining authorization fields that are still blank. Generate the respective profiles.

Continued on next page

Task 9:

Create three composite roles, which correspond to the sample authorization concept. When doing this, use the names from the following table.

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)

- When creating the roles, follow the steps from tasks 1-1 to 1-3 from this lesson.



Hint: Ensure that you use the *Create Comp. Role* button on the initial screen of the Role Maintenance.

Enter a short description, and save your composite role.

- Go to the Roles tab page.

Your composite role should consist of the roles of the role definition in the sample authorization concept.

Select the corresponding roles and copy them into your composite role.

Example: The role of the accounts receivable accountant (AccRec), that is, the composite role GR##_FI_ACCREC, must contain the following roles:

- GR##_MM_MAT_ANZ
- GR##_FI_ACCREC_MAINT
- GR##_FI_IP_POST

- Go to the *Menu* tab page and import the menus of the inserted roles into your composite role.

Optionally, you can further customize the menu of the composite role.

Save your composite role.

- Create the missing roles.

Repeat tasks 1 and 3 of this exercise, until all composite roles have been created.

Continued on next page

Composite Role	Contained Roles
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
GR##_MM_WHOUSE	GR##_MM_MAT_ANZ GR##_MM_IM_POST

Solution 6: Special ABAP Roles

Task 1:

Create the composite role GR##_MM_WHOUSE.



Hint: Ensure that you use the *Create Comp. Role* button on the initial screen of the Role Maintenance.

1. Enter a short description, and save your composite role.

If you look at the tab pages, what do you notice?

- a) **SAP Menu:**

→ **Tools** → **Administration** → **User Maintenance** → **Role Administration** → **Roles**, (transaction code “PFCG”). “PFCG”).

- b) If you look at the tab pages, what do you notice?

The tab page *Roles* has been added.

The tab page *Authorizations* has been removed.

2. Go to the Roles tab page.

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) Enter the roles listed in the exercise text and save your settings. Can you select these roles using input help, or enter them manually.
3. Go to the Menu tab page and 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; you can, however, move or rename them).

Continued on next page

Save your composite role.

- a) Goto the Menu tab page, and choose *Import Menu*.

Save your composite role.

4. Go to the User tab page and assign user GR##-MM1. Save your user assignment.
 - a) Choose the save icon (disk icon) or choose *Ctrl+S*
5. Perform a user master comparison.
 - a) Choose the *User comparison* button to enter the roles in the master record of user GR##-MM1.

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.

1. Which roles is the user assigned?

If your user GR##-MM1 does not yet have the role ADM940_PLUS, assign the role and perform a user master comparison.

Continued on next page

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”). “SU01”).

Solutions in square brackets are additional results that may have been created by other optional exercise tasks.

- GR##_MM_WHOUSE
 - GR##_MM_MAT_ANZ
- GR##_MM_IM_POST
- ADM940_PLUS
- [GR##_BC_PORTALS]

- b) 3 (4) authorization profiles, The solutions in curved brackets are the results that appear when you have performed all the tasks (standard and optional) in the previous exercises.
- c) Because the composite role does not have its own profile.

Task 4:

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. Set up a user-specific favorites list by defining the transactions “MM03” and “MB1C” as favorites and adding any Web address.
 - a) You can fill the favorites list by dragging transactions from the user menu to the favorites list or insert transactions directly using the context menu (right mouse button).

Continued on next page

2. Try to start some of the transactions, for example, “MM03”, and display the accounting view of material *P-100* in plant *1000*.

Can you also display the accounting view of material *P-100* in plant *3000*?

If not, why not?

-
- a) Call transaction *MM03*. Enter the material ID *P-100* in the *Material* field. Choose *Select view(s)* and choose the *Accounting I* view. Choose *Continue*.

Can you also display the accounting view of material *P-100* in plant *1000*?

Yes.

Can you also display the accounting view of material *P-100* in plant *3000*? Here, repeat the steps you performed for plant *1000*, but this time for plant *3000*.

No, because you **do not** have authorization for plant *3000*. Displayed in the footer or can be displayed in SU53.

3. Display the failed authorization check.



Hint: Menu path: → *System* → *Utilities* → *Display Authorization Check* (or transaction “SU53”)

Why were you not able to display material *P-100* in plant *3000*?

Log off as GR##-MM1.

- a) The program required activity *03* and plant *3000* for the authorization object *M_MATE_WRK*.

Although the user master record contains authorization for activities *03* and *08*, there is no authorization for plant *3000*.

Task 5:

Create a **derived** role *GR##_MM_IM_POST1000* with authorizations for a warehouse supervisor in plant *1000*.

1. Write a short description. Assign the imparting role *GR##_MM_IM_POST* and save your role.

Continued on next page

Display the inheritance hierarchy of the roles (Ctrl+Shift+F3 or the *Inheritance Hierarchy* icon).

- a) **SAP Menu:**

Tools → Administration → User Maintenance → Role Administration → Roles, (transaction code: “PFCG”). Choose the “Basic Maintenance” view and write a short description.

- b) Enter GR##_MM_IM_POST in the “Derive from Role” field and save your role.

Display the inheritance hierarchy of the roles.

Menu: → Role → Where-Used List

2. Go to the Menu tab page.

Can you select other activities (menu entries, transaction codes, reports, for example) or delete existing activities?

-
- a) No, since the menu of role GR##_MM_IM_POST is inherited from the role GR##_MM_IM_POST1000.

3. Go to the Authorizations tab page. Select the normal mode (*Change authorization data*).

Define the organizational levels:

- Plant: 1000.

Did the system copy the authorizations of the imparting role?

-
- a) No, they must either be maintained here directly or copied as described in the next exercise task.

4. Save the authorizations and accept the proposed profile name.

Copy the authorization data from the imparting role.

Did the system copy settings for organizational levels?

Continued on next page

Ensure that users assigned to this derived role are only allowed to post data in plant *1000*.

- a) Copy the authorization data from the imparting role by choosing *Copy data* or by choosing

Edit → *Copy data*. The authorizations are then copied from the *imparting role* (reference role).

Choose *Organizational levels*. The plants *1000*, *1100*, and *1200* were **not** copied from the reference since this is an organizational level field which was previously set in the derived role (see step 3 in this task).

→ **Note:** Additional example: Delete the entry for plant *1000* from the organizational levels. Save your entries and the profile and choose *Transfer Data* again.

What is now displayed when you display the entries of the organizational levels?

You see the entries for plants *1000*, *1100*, and *1200* again.

Reduce the entries to just that for plant *1000* and save your changes.

5. Generate the authorization profile for your role.
 - a) You do not need to enter a name since the system prompted you for one when you saved the data for the first time.

Task 6:

The following exercise is optional.

Create a new single role GR##_SD_SALES by copying the predefined work center example ADM940_SD_SALES without user assignment.

1. Use the copy icon in transaction “PFCG”.
 - a) **SAP Menu:**
→ *Tools* → *Administration* → *User Maintenance* → *Role Administration* → *Roles*, (transaction code “PFCG”).
 - b) Enter the role ADM940_SD_SALES in the initial screen of PFCG and then copy the content to the new role GR##_SD_SALES by choosing the *Copy Role* icon. Choose *Copy selectively* and do not set the user assignment checkbox. This ensures that the assigned users are not copied.

Continued on next page

Task 7:

Change your copied role GR##_SD_SALES.

1. Change the description to a description specific to your group.

Go to the Menu tab page.

Display the technical names.

Expand all nodes of the menu and delete all transactions and nodes that are not intended for this role in the “*sample authorization concept*” (see lesson *Creating and Implementing an Authorization Concept* or look at the role distribution table **Example Authorization Concept** in the introduction to this exercise).

Save the changed user menu.

- a) Open the specified role in change mode and go to the *Menu* tab page.
- b) Activate the technical names (transaction codes) by choosing the magnifying glass icon (on the right next to the delete icon (trash can)).

Delete the nodes:

- Master Data
- Outbound Delivery
- Billing Document.

by selecting the node and choosing *Delete Node*. Only the transaction codes VA21, VA22, VA23, VA25, VA01, VA02, VA03, and V.01 should remain.

2. Go to the Authorizations tab page.

Select the normal mode (*Change authorization data*).

Restrict the organizational levels as follows:

- Sales organization: *1000*.

Leave the default authorization values for all other organizational levels.

- a) Overwrite the asterisk for sales organization with the value *1000*. Keep the default values for the other organizational levels (company code, controlling area, division, distribution channel, and so on).

3. Assign full authorization for all other and open fields (“*”).

- a) To do this, click the traffic light symbol at the top hierarchy level with the left mouse button, and confirm the assignment of full authorization.

Continued on next page

4. Generate the authorization profile for your role. Accept the proposed profile name.
 - a) Choose *Authorizations* → *Generate* or the corresponding pushbutton.

Task 8:

Create the missing three single roles of the *sample authorization concept*.

1.

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

Enter the role name and a short description. Fill the menu with the required transaction codes and import the proposed authorization values.

- a) Start with the role GR##_FI_ACCREC_MAINT.

SAP Menu:

→ *Tools* → *Administration* → *User Maintenance* → *Role Administration* → *Roles*, (transaction code “PFCG”).

Perform the task up until the maintenance of authorizations.

2. 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	1000
Business area	1000
Account type	D
Controlling area	1000
Division	*
Sales organization	1000
Distribution channel	*

Continued on next page

Then assign the full authorization [*] for all remaining authorization fields that are still blank. Generate the respective profiles.

- a) Restrict the requested organizational levels with the values specified here:

Role GR##_FI_ACCREC_MAINT

- Company code: *1000*.

Role GR##_FI_IP_POST

- Company code: *1000 1000*,

- Business area: *1000, 1000*,

- Account type: *D*,

- Controlling area: *1000. 1000*.

Role GR##_SD_CUST_MAINT - Company code: *1000 1000*,

- Division: *,

- Sales organization: *1000 1000*,

- Distribution channel: *. *

Set full authorization for all remaining open authorization fields.

Generate the profiles.

Task 9:

Create three composite roles, which correspond to the sample authorization concept. When doing this, use the names from the following table.

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)

1. When creating the roles, follow the steps from tasks 1-1 to 1-3 from this lesson.



Hint: Ensure that you use the *Create Comp. Role* button on the initial screen of the Role Maintenance.

Continued on next page

Enter a short description, and save your composite role.

a) **SAP Menu:**

→ *Tools* → *Administration* → *User Maintenance* → *Role Administration* → *Roles*, (transaction code “PFCG”).

Name of the new composite role, for example, GR##_FI_ACCREC.
Create the role.

2. Go to the Roles tab page.

Your composite role should consist of the roles of the role definition in the sample authorization concept.

Select the corresponding roles and copy them into your composite role.

Example: The role of the accounts receivable accountant (AccRec), that is, the composite role GR##_FI_ACCREC, must contain the following roles:

- GR##_MM_MAT_ANZ
- GR##_FI_ACCREC_MAINT
- GR##_FI_IP_POST

a) Enter the roles intended for the work centers.

3. Go to the *Menu* tab page and import the menus of the inserted roles into your composite role.

Optionally, you can further customize the menu of the composite role.

Save your composite role.

a) 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.

4. Create the missing roles.

Repeat tasks 1 and 3 of this exercise, until all composite roles have been created.

Continued on next page

Composite Role	Contained Roles
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
GR##_MM_WHOUSE	GR##_MM_MAT_ANZ GR##_MM_IM_POST

- a) See table in the task description.



Lesson Summary

You should now be able to:

- Describe the use of Customizing roles
- Explain the advantages and disadvantages of composite roles
- Define the relationship between reference roles and derived roles
- Bundle frequently used transactions and map them with different instances using derived roles
- Describe how to perform a mass comparison and state, which report you can schedule for an automatic comparison

Lesson: 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



Lesson Objectives

After completing this lesson, you will be able to:

- Interpret the red, yellow, and green traffic lights for different field contents
- Describe the meaning of the icons in the PFCG authorization maintenance
- Define the hierarchy of status terms, and explain when which term is used
- Distinguish between the expert mode and simple maintenance for authorizations
- List additional functions that are accessible through the menu

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.

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

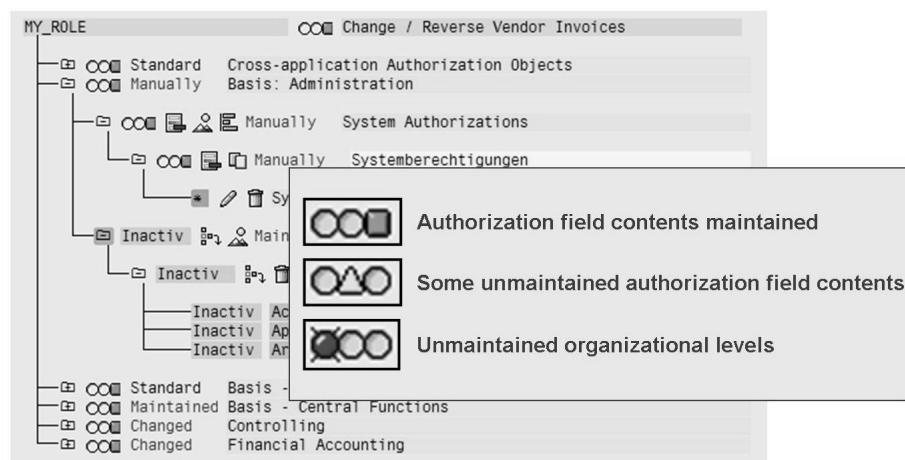


Figure 70: Authorization Maintenance: Traffic Light Legend

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 “Control + F8” to assign the values.



Important Browser Icons

-  Transactions for an authorization object
-  Allocation of full authorization
-  Maintain field contents
-  Copy authorization
-  Merge multiple authorizations
-  Deactivate/reactivate authorizations/authorization object
(the status behavior has changed here)
-  Delete field contents
or delete an inactive authorization
or delete other authorizations for an object

**or delete ALL inactive authorizations,
but only if changed or manual.
(Trash Can -> Application Toolbar)**



Figure 71: Authorization Maintenance: Icon Legend

Other icons in the object classes, authorization objects, authorizations, and authorization fields lines are:

Assignment of authorizations: Displays the transactions that use this object.

Full authorization: You can set full authorization by simply clicking the asterisk “*” next to an authorization field name or using the button in the input window.

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.

The same procedure also applies for the traffic light in the top line between the **Role Name** and the **Role Text**.

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 this icon, 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 with this icon or using the *Utilities* menu.



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 connected to 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.

Inactive/Reactivate: You can use this icon to technically hide 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: Inactive

If you click this icon:

- 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”.



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
- New: At least one new authorization added

Figure 72: 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 the 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, the 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.

Exercise 7: Subtleties of Authorization Maintenance

Exercise Objectives

After completing this exercise, you will be able to:

- Explain the traffic light colors
- Differentiate between the use and meaning of the status types
- Find out where objects are used
- Explain the term “inactive”

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 will reinforce your knowledge of the special features of role maintenance.

Task 1:

Create the role *GR##-RGB* by copying *AMD940-RGB* without user assignments and personalization.

1. Enter a short description, and save your role.
Go to the Authorizations tab page. Select the normal mode (*Change authorization data*).
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.

5. Use the *Organizational Levels* button to assign the value *10* for the *Plan Version*.

Continued on next page

Task 2:

Explain the other traffic light colors.

1. What does a Yellow traffic light mean, and which objects (role GR##-RGB have this status?

2. What does the last traffic light color mean, and what do you have to take into account here?

This must be taken into account:

3. In the authorization object *S_USER_TCD*, assign the value “*V**”, and full authorization for all other fields. What do you have to take into account here?
4. Generate the profile and accept the proposed profile name. Exit authorization maintenance and return to the Authorizations tab page.

Task 3:

Use the expert mode to merge the existing authorization data with the PG default values again.

1. Which choice must be made when starting the maintenance so that the Profile Generator reads default values again?

2. Open the authorization values and read the Profile Generator defaults again.

Continued on next page

3. Which authorization field has the status *New*?

4. Why does the field *S_USER_TCD* receive the entry *PFCG*?

5. What would you have had to do as preparation to avoid this?

Solution 7: Subtleties of Authorization Maintenance

Task 1:

Create the role *GR##-RGB* by copying *AMD940-RGB* without user assignments and personalization.

1. Enter a short description, and save your role.

Go to the Authorizations tab page. Select the normal mode (*Change authorization data*).

- a) **Menu:**

Tools → Administration → User Maintenance → Role Administration → Roles, (transaction code “PFCG”).

Choose the “Basic maintenance” view and create the required role. Enter a short description, and save your entry.

Go to the Authorizations tab page. Select the normal mode (*Change authorization data*).

2. What traffic light colors are displayed for the authorization objects used?

- a) *Red, Yellow, and 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.

Continued on next page

- a) Open the search option by choosing the menu path *Edit → Find* and enter *plan version* for the field text. If you have enabled the *Show Technical Names* setting, then 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.

If the technical names are disabled, you see the entry “*unmaintained organizational level*” in the field.

5. Use the *Organizational Levels* button to assign the value *10* for the *Plan Version*.
- a) Click the *Organizational Levels* button with the left mouse button and enter the value *10* for the *Plan Version*. Save your data by choosing save (*disk* icon).

Task 2:

Explain the other traffic light colors.

1. What does a Yellow traffic light mean, and which objects (role GR##-RGB have this status?

- a) Yellow traffic lights indicate a structure in which at least one field does not yet contain a value.

Open the structure with the node with a Yellow traffic light by clicking the plus sign next to the traffic light. The following objects have not yet been given default values by the Profile Generator: *S_GUI*, *S_USER_AUT*, *S_USER_GRP*, *S_USER_PRO*, and *S_USER_VAL*.

2. What does the last traffic light color mean, and what do you have to take into account here?

Continued on next page

This must be taken into account:

- a) The Green traffic light indicates structures in which all fields are assigned a value. However, it is not possible to identify whether this is:
 - A Profile Generator (PG) default
 - An organizational level field that received the field value through the maintenance button
 - Field for which the PG default 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 Profile Generator default values. *Green* does **not** mean that you do not have to check these default values.

3. In the authorization object *S_USER_TCD*, assign the value “*V**”, and full authorization for all other fields. What do you have to take into account here?
 - a) Use the search function (see exercise 1-4) to find the field *S_USER_TCD*. Change the field entry to *V** and use the traffic light on the top hierarchy level to assign full authorization to all remaining empty fields.
4. Generate the profile and accept the proposed profile name. Exit authorization maintenance and return to the Authorizations tab page.
 - a) Choose the "Generate" icon (red and white circle) and accept the profile name. Exit authorization maintenance by choosing *F3*.

Task 3:

Use the expert mode to merge the existing authorization data with the PG default values again.

1. Which choice must be made when starting the maintenance so that the Profile Generator reads default values again?
-

Continued on next page

- a) The mode *Read old status and merge with new data*.
2. Open the authorization values and read the Profile Generator defaults again.
- a) On the *Authorizations* tab page, choose the *Expert Mode for Profile Generation* icon. Select the radio button for the option *Read old status and merge with new data* and execute the selection.
3. Which authorization field has the status *New*?
-
- a) Search the authorizations for a line with the entry *New* or use the corresponding button. You will find the object *S_USER_TCD* with the field **TCD** and the entry *PFCG*.
4. Why does the field *S_USER_TCD* receive the entry *PFCG*?
-
-
-

- a) This is an authorization object for which the Profile Generator proposal was changed (status: *changed*).

Two conditions must be met to enable this behavior.

1. One condition is that the object continues to be proposed through the use of a transaction in the menu.
2. A Profile Generator proposal is read again if the object in question no longer exists with the status *Standard* or *Maintained* (regardless of whether it has the status *Active* or *Inactive*).

5. What would you have had to do as preparation to avoid this?
-
-
-

a)



Note: Before you process a specification in such a way that has the status *Changed* appears, you must **copy the specification**, and set the template to *Inactive*.



Lesson Summary

You should now be able to:

- Interpret the red, yellow, and green traffic lights for different field contents
- Describe the meaning of the icons in the PFCG authorization maintenance
- Define the hierarchy of status terms, and explain when which term is used
- Distinguish between the expert mode and simple maintenance for authorizations
- List additional functions that are accessible through the menu



Unit Summary

You should now be able to:

- Describe and explain the basic steps for assigning authorizations with the Role Maintenance
- Create new roles, change and copy roles, and specify their activities
- Display and maintain authorizations that were generated automatically
- Compare user master records directly in role maintenance “PFCG” or in user maintenance “SU01”
- Describe how to perform a mass comparison and state which report you can schedule for an automatic comparison
- Describe the use of Customizing roles
- Explain the advantages and disadvantages of composite roles
- Define the relationship between reference roles and derived roles
- Bundle frequently used transactions and map them with different instances using derived roles
- Describe how to perform a mass comparison and state, which report you can schedule for an automatic comparison
- Interpret the red, yellow, and green traffic lights for different field contents
- Describe the meaning of the icons in the PFCG authorization maintenance
- Define the hierarchy of status terms, and explain when which term is used
- Distinguish between the expert mode and simple maintenance for authorizations
- List additional functions that are accessible through the menu

Unit 5

Basic Settings

Unit Overview

This unit describes basic settings for the topic of authorizations. Some of these settings should be made before “PFCG” is used (lesson 1: Installation and Upgrade), while others are made during operation (lesson 2: Concept of User Administration). A number of parameters, switches, and objects are used for this purpose. These are described here. The final lesson discusses the Information System and AIS, which provide the administrator for different search options for listing the system settings and requirements for the area of authorization. This also includes the analysis of failed authorization checks, and the system trace.



Unit Objectives

After completing this unit, you will be able to:

- Perform the steps necessary to install the Role Maintenance
- Find default values and check indicators in the system
- Modify, delete, or extend the default values of the Role Maintenance
- Perform the necessary steps after an upgrade for postprocessing old and new authorization values
- Describe new functionality in transaction SU25
- Define password rules and system profile parameters
- Protect special users in the SAP system
- Protect SAP functions with authorization object S_TCODE
- Protect tables and views using authorization groups
- Protect programs with authorization groups
- Describe tasks in user and authorization administration
- List options for separating functions of user and authorization administration
- Describe options for decentralization of user administration
- Create user and authorization administrators with limited rights (using authorization objects)
- Analyze authorization checks in various ways
- Use transaction “SU53” to find missing authorizations (also for other users)

- Run the authorization trace (“ST01”)
- Apply the features of the information system and use them for different tasks
- Understand and apply the **new** functions of the Audit Information System (AIS)

Unit Contents

Lesson: Role Maintenance: Installation and Upgrade	191
Exercise 8: Role Maintenance: Installation and Upgrade.....	205
Lesson: Access Control and User Administration	214
Exercise 9: Access Control and User Administration.....	239
Lesson: Troubleshooting and Administration Aids	251
Exercise 10: Troubleshooting and Administration Aids.....	261

Lesson: Role Maintenance: Installation and Upgrade

Lesson Overview

This lesson will provide an overview of the steps required to install the Role Maintenance. The Role Maintenance has been delivered activated since SAP R/3 4.6.

The lesson will also explain which steps are to be performed after an upgrade, and how you can continue to use profiles that you have already created manually.



Lesson Objectives

After completing this lesson, you will be able to:

- Perform the steps necessary to install the Role Maintenance
- Find default values and check indicators in the system
- Modify, delete, or extend the default values of the Role Maintenance
- Perform the necessary steps after an upgrade for postprocessing old and new authorization values
- Describe new functionality in transaction SU25

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.

Basic Settings for Using Role Maintenance

Activating the Role Maintenance after a **new installation** requires that:

The Required Steps for Operating the 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 the Role Maintenance when a transaction is selected in a role.

Both steps are described in detail in this lesson.



Hint: With new settings (since SAP R/3 4.6), the parameter is already set to “Y” in the default settings. You only need to create the customer default tables.



Display Profile Parameter Properties

Documentation

Parameter Name	auth/no_check_in_some_cases
Short Description (Engl)	Special authorization checks switched off by customer
Application Area	Authentication
Parameter Type	Special Character String
Changes allowed	Changes allowed
Valid for Operating System	All Operating Systems
Dynamically Switchable	<input type="checkbox"/>
Same on All Servers	<input type="checkbox"/>
Special Character String	Y
Separator	<input type="checkbox"/>
Default Value	Y
Profile Value	Y
Current Value	Y

Figure 73: Checking Profile Parameter *auth/no_check_in_some_cases*

As described, with new installations of SAP systems (> SAP R/3 4.5), 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.

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”.

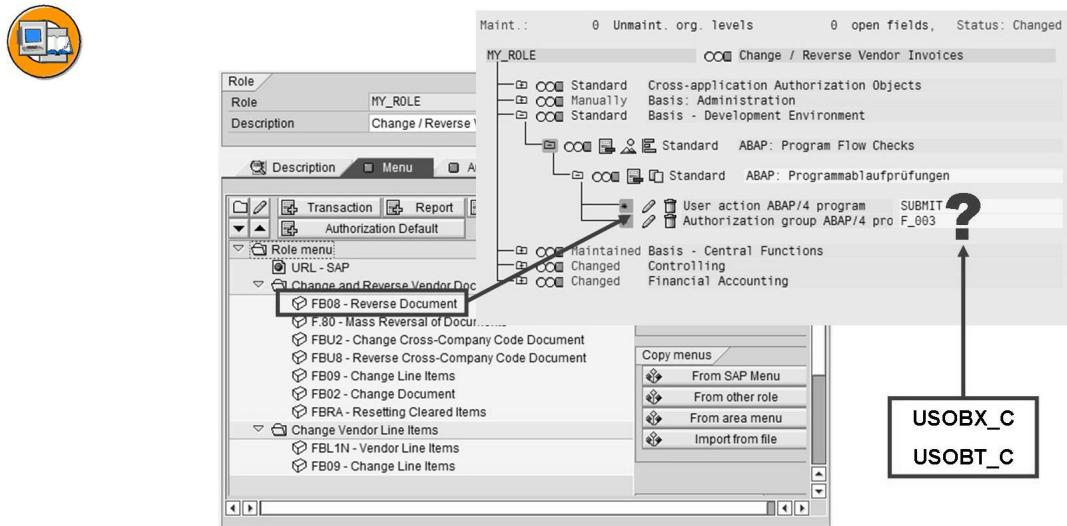


Figure 74: Where do the Default Values Come From?

If an administrator selects a transaction while creating a role, the Role Maintenance selects the authorization objects that are checked in this transaction and maintained in the Role Maintenance. Four cases can occur:

- For an authorization object against which the check is performed in the transaction selected, the 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 transaction selected, the Role Maintenance does not have default values for the authorization content. In the example on the slide, the SAP Office transaction “SO01” 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 transaction selected, the 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 the 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 the Role Maintenance after the transaction has been selected. After a new installation, these tables are empty and must be filled with values before the Role Maintenance is used for the first time. The next step, shown on the next slide is required to do this.

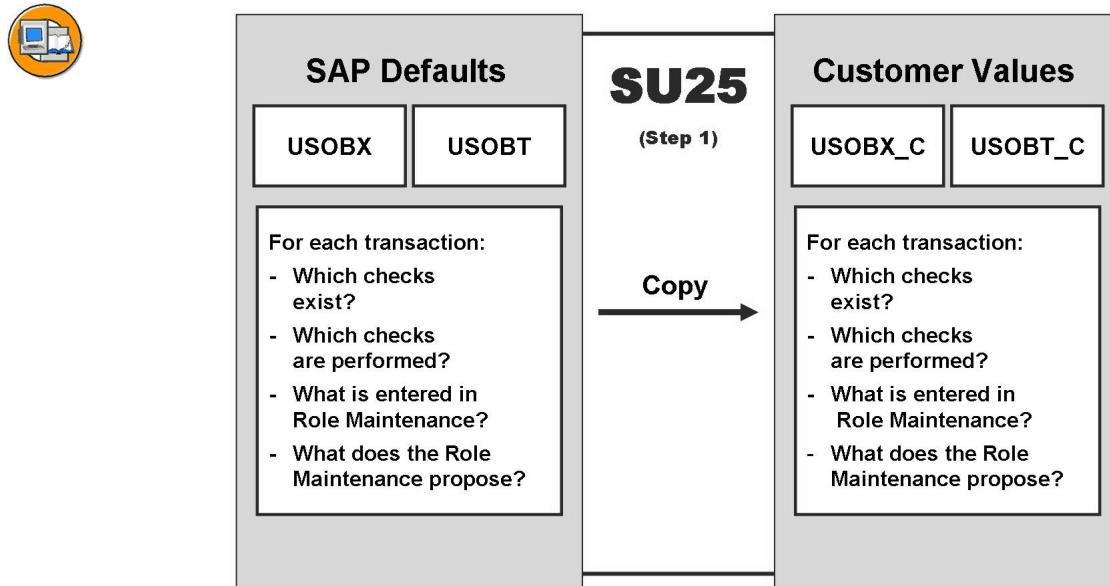


Figure 75: Initial Fill of the Default Tables

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 the 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 the 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 the 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 the 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.

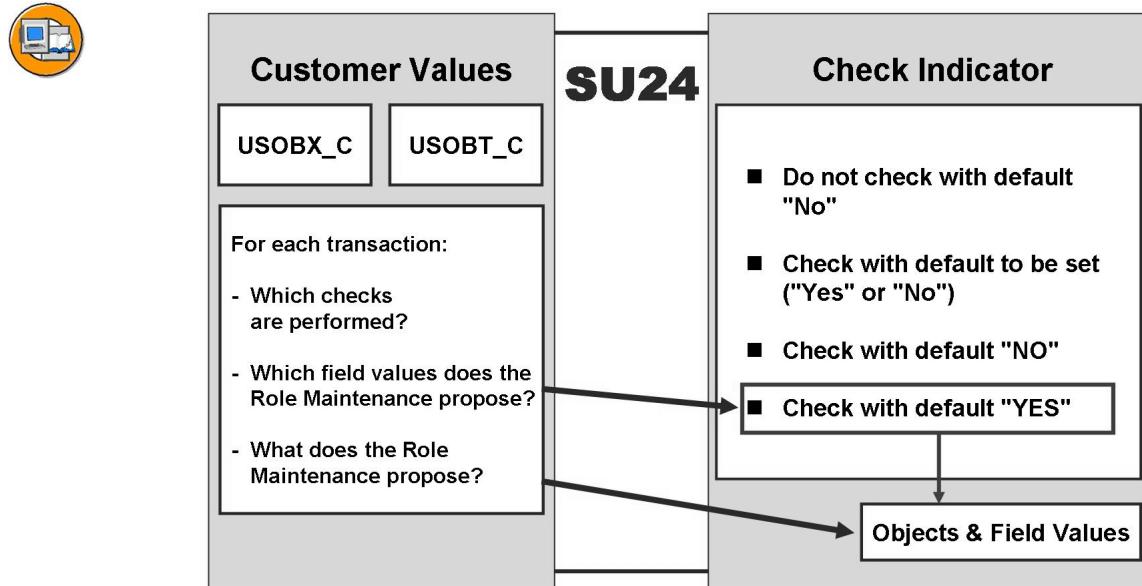


Figure 76: Optional: Adjusting Check Indicators

After the customer tables `USOBX_C` and `USOBT_C` have been filled, you can maintain them to adjust the behavior of the Role Maintenance and the authorization checks to be performed for each transaction. The tables are maintained in transaction “SU24”.

This transaction displays the check indicators of a transaction. Check indicators determine if an authorization check will run within the transaction or not.

→ **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 no longer governed solely by the check indicator (as was the situation before SAP NetWeaver 2004s); instead, the maintenance status of the authorization object is also considered.

1. Check Indicator

The following check indicators are supported:

- **Do not check with default "No"** (formerly N; do not check) check disabled. Field values are not displayed in the Role Maintenance. This indicator cannot be chosen for HR and Basis authorization objects.

- **Check with default to be set ("Yes" or "No")** (formerly U; not maintained) no indicator set. The appropriate authorization object is always checked. Field values are not displayed in the Role Maintenance.
- **Check with default "No"** (formerly P; check) check always runs. Field values are not displayed in the Role Maintenance. Example: Printer authorizations
- **Check with default "Yes"** (formerly PP; check/maintain) check always runs. Field values are displayed in the Role Maintenance and can be changed (yellow, green, and red lights are possible).



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. 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 the 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.

Upgrading the Role Maintenance

What do you need to do if you perform an upgrade?



- Migration of report trees
- Check of Role Maintenance activation
- Upgrade of the roles and default tables (“SU25”, steps 2A-2D)
- Conversion of manually created profiles to roles if necessary (“SU25”, step 6)

Different postprocessing steps are required for the authorization data in the system after an upgrade, depending on the source release and whether or not roles that are to be used in the target release were already created with the Role Maintenance in the source release.

For a full description of the changes for different releases, see the detailed online documentation.

However, the most important changes are listed here in keywords to give you a brief overview.

New Developments for SAP Web AS 6.20

- The Global User Manager was deactivated (see SAP Note 433941).
- Additional system parameter *login/password_change_for_SSO* (for logon with Single Sign-On) specifies whether the user must change his or her password.

New Developments for SAP Web AS 6.10

- Additional system parameters for logon
- Generation and deactivation of passwords
- Synchronization of the SAP database with an LDAP directory

Source release < SAP R/3 4.6B

- You have to migrate customer-defined report trees because the data structure of report trees changed internally (transaction “RTTREE_MIGRATION”). The report is automatically assigned a transaction code.
- New fields in user administration

Regardless of your release status, you will have one of the two following statuses:

1. Source release **did not use PFCG**

If the Role Maintenance was not used in the source release, it might have to be activated. If it is a new installation, the Role Maintenance is already activated.

2. Source release **used PFCG**

If roles were already used in the source release, they must be updated. 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.



Source release did not use Role Maintenance

Source release (Role Maintenance can be used as of 3.1G)

Figure 77: Upgrade Considerations (1)

You have only implemented your authorization concept with manually created profiles until now. You are now faced with the following questions:

How do I continue?

What can I transfer from the old concept?

Can I transfer anything at all?

Upgrade scenario: Source release did not use Role Maintenance



- **Option 1**

- Re-evaluate your authorization concept and rebuild authorizations using the Role Maintenance.

- **Option 2**

- Convert manually created profiles and authorizations into roles. Use transaction “SU25” (step 6) to do this.

Option 1 (create everything again):

- Advantages:
 - Authorizations are restructured based on the new authorization concept.
You can fully utilize configuration tables *USOBX_C* and *USOBT_C*.
 - Possible to use user-friendly user menus
 - Creation of clear, structured, transparent authorization concept with consistent naming convention and reorganization of the authorization administration possible
- Disadvantages:
 - Can be time-consuming (re-implementation of security features)

You can also convert manually created profiles to roles.

Option 2 (transfer parts of the existing concept):

- Advantages:
 - Allows administrator to assign all existing, well tested, profiles to corresponding roles.
 - If the profiles contain authorizations for authorization object *S_TCODE*, the corresponding user menu can be created automatically.
- Disadvantages:
 - An authorization profile in a role does not necessarily have complete relation to the menu entries. In this case, the administrator can only partially use the configuration tables *USOBX_C* and *USOBT_C*.



Hint: The menu can only be created automatically if authorizations for *S_TCODE* are included in the profile and the transactions are listed as single values. Areas cannot be resolved, such as “VA*”.

If you want the best possible conversion, you thus have to search the manual profiles for the object *S_TCODE* beforehand and change any listed areas to single values manually.

Regardless of the situation: The roles contained **must** still be postprocessed.



Source release did not use Role Maintenance



Source release (Role Maintenance can be used as of 3.1G)

Figure 78: Upgrade Considerations (2)

Upgrade scenario: Previous system (> 3.1G) uses Role Maintenance

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”, steps “2A” to “2D”.



- **2A:** Executes the Role Maintenance comparison program. Compares the new tables *USOBX* and *USOBT* with *USOBX_C* and *USOBT_C*.
- **2B:** Adds any new transactions/updates to tables *USOBX_C* and *USOBT_C*.
- **2C:** Updates the existing roles and flags all roles with new authorization objects.
- **2D:** Displays all roles for which there are changed transaction codes.



Caution: When executing transaction “SU25” you should keep in mind that the customer might have changed table *USOBX_C* or *USOBT_C* in the source release. **Step 1** in transaction “SU25” **may not** be executed for this reason as it would completely overwrite the tables.

Rather, a comparison procedure is required, which is performed using steps 2A to 2D.

Step 2A

This compares the Role Maintenance data from the previous release with the data for the current release. New default values are written in the customer tables for the Role Maintenance. You only need to perform a manual adjustment later (in step 2B) for transactions in which you changed the settings for check indicators and field values. You can also display a list of the roles to be checked (step 2C).

Step 2B

If you have made changes to the check indicators or field 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 can make an adjustment, if desired. You can assign the check indicators and field values by double-clicking the relevant line.



Hint: Steps 2A and 2B make changes to the customer tables of the Role Maintenance. If you want to transport these changes, choose step 3 in transaction “SU25”.

Step 2C

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.



Caution: These changes are not recorded in step 3 (transport) and must therefore be transported separately.

Step 2D

Occasionally, transactions in the SAP system are replaced by one or more other transactions. In step 2D, you create a list of all roles that contain transactions that were replaced by other transactions. The old and new transaction codes are listed. If necessary, you can replace the transactions in the roles. It is also possible to jump directly to role maintenance in this step.

If you are performing an upgrade from a release status older than SAP R/3 4.6, there are a number of helpful SAP Notes, such as SAP Notes 156250 or 156196.

New functionality in SU25: Deactivating merge mode in step 2C

Transaction SU25 is required after an upgrade to update the customer-specific authorization default values and roles. Step 2C provides a list of roles which are affected by the newly added or changed authorization default values. The roles which authorization data must be merged will get the "Profile comparison required" status (merge mode) and are marked with red traffic lights. The merge mode will trigger 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 2C, 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 will get a new yellow status. When you now navigate back to transaction PFCG, the system will no longer merge the roles automatically, but will display 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 2C 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 2C are not identical to the authorization statuses of roles in the Authorizations of the Role Maintenance. Step 2C 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 2C. As a result, the functions for changing the merge mode and the selection functions are not available.

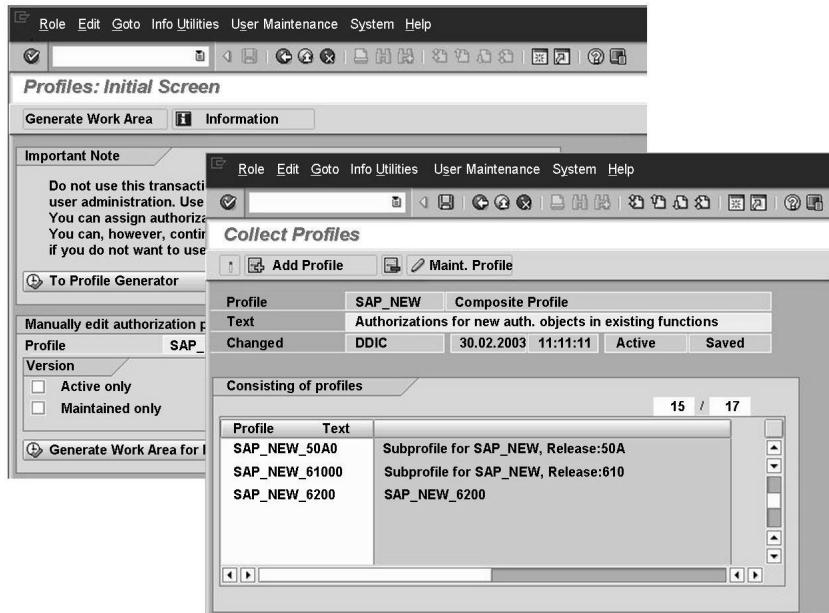


Figure 79: Upgrade Profile: SAP_NEW

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 *SAP_NEW* profile to the users manually.

The profile *SAP_NEW* is delivered with every new release and contains authorizations for all new checks in existing transactions. You should only leave the subprofiles in the *SAP_NEW* profile that are relevant for your employees.

The *SAP_NEW* profile guarantees backward compatibility of the authorizations if a new release or an update or authorization checks introduces checks for previously unprotected functions.

SAP_NEW: 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 (“*”).

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.



Hint: If you are upgrading from release 4.5B to release 4.6C, for example, you require the following SAP_New profiles: *SAP_NEW_4.6A*, *SAP_NEW_4.6B* and *SAP_NEW_4.6C*. The simplest solution is to delete all other single profiles from *SAP_NEW* and to assign this newly created *SAP_NEW*.

Once you have included the new authorization checks in your authorization concept, delete the profile *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.

Exercise 8: Role Maintenance: Installation and Upgrade

Exercise Objectives

After completing this exercise, you will be able to:

- Explain the meaning of the authorization check indicators and know their difference
- Describe how authorization checks and default values for authorization fields are determined

Business Example

This exercise will reinforce the topics of default values for the Role Maintenance, check indicators, and steps after an upgrade.

Task 1:

Display the check indicators for transaction “PA30”.

1. In Customizing for SAP Web Application Server, choose *Work on SAP Check Indicators and Field Values* and then *Change Check Indicator* (transaction “SU24”).
Choose *Maintain check indicators for transaction codes* and enter transaction “PA30”.
2. Display the check indicators for the authorization objects of this transaction and check the following:
Are there any authorization objects with the check indicator “*Check with default to be set - Yes or No*” or “*Do not check with default - No*”?

To which authorization objects is the check indicator “*Check with default - Yes*” assigned?

3. Go to the field value display.

Which default values are assigned to which authorization fields of the authorization object *PLOG*?

Fill in the following table.

Continued on next page

Object	Field	Value (Interval)
PLOG		

Task 2:

Create a role and compare the automatically entered authorizations with the check indicators and the default values from the previous task.

1. Create a role GR##_HR_PA30.
Enter a short description, and save your role.
2. Go to the Menu tab and select the following activities:
- “PA30” - Maintain HR Master Data
Save the activities of your role.
3. Go to the Authorizations tab page. Select the normal mode (*Change authorization data*).
Define the organizational levels:
- Plan version: *01*
Why do you have to enter an authorization value for the plan version?

For which authorization objects did the system automatically generate authorizations?

Why is the status of the authorization objects PLOG and P_PCLX set to *Standard* and why is the traffic light symbol status set to *green*?

Continued on next page

- _____
- _____
- _____
4. Set full authorization for all open authorization values. Generate the profile, accept the proposed profile name, and exit role maintenance.
- _____

Task 3:

Convert the profile *A_ANZEIGE*.

1. Where can you convert profiles?

2. Which type of profiles can be used for this, and which types of conversion are available?

Types:

1.) _____

2.) _____

3. Convert the specified profile so that a menu may be automatically created. View the result. Could a menu be created?

4. Could all transactions from the profile be included in the menu?

Solution 8: Role Maintenance: Installation and Upgrade

Task 1:

Display the check indicators for transaction “PA30”.

1. In Customizing for SAP Web Application Server, choose *Work on SAP Check Indicators and Field Values* and then *Change Check Indicator* (transaction “SU24”).

Choose *Maintain check indicators for transaction codes* and enter transaction “PA30”.

- a) SAP Menu: *Tools* → *Customizing* → *IMG* → *Execute Project* , (transaction code:“SPRO”).

Choose *SAP Reference IMG*

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 check indicators for the authorization objects of this transaction and check the following:

Are there any authorization objects with the check indicator “*Check with default to be set - Yes or No*” or “*Do not check with default - No*”?

To which authorization objects is the check indicator “*Check with default - Yes*” assigned?

Continued on next page

-
- a) There are only authorization objects with the check indicator “*Do not check with default - No*” (formerly “N”). Also indicated by the “gray” icon in the *Status* column.
- b) To which authorization objects is the check indicator “*Check with default - Yes*” assigned?

PLOG

P_ORGIN

P_PCLX

P_PERNR

If the object and its values are all OK, a “green” icon is shown in the *Status* column.

3. Go to the field value display.

Which default values are assigned to which authorization fields of the authorization object *PLOG*?

Fill in the following table.

Object	Field	Value (Interval)
PLOG		

- a) Go to the field value display.

Object	Field	Value (Interval)
PLOG	INFOTYP	1001
	ISTAT	–
	OTYPE	C, O, P, Q, S
	PLVAR	\$PLVAR
	PPFCODE	–
	SUBTYP	–

Continued on next page

Task 2:

Create a role and compare the automatically entered authorizations with the check indicators and the default values from the previous task.

1. Create a role GR##_HR_PA30.

Enter a short description, and save your role.

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

Choose the “Basic Maintenance” view, create a short description, and save your role.

2. Go to the Menu tab and select the following activities:

- “PA30” - Maintain HR Master Data

Save the activities of your role.

- a) Select transaction “PA30” in the Menu tab page using the “Transaction” button or the “Select from the SAP Menu” button.

3. Go to the Authorizations tab page. Select the normal mode (*Change authorization data*).

Define the organizational levels:

- Plan version: 01

Why do you have to enter an authorization value for the plan version?

For which authorization objects did the system automatically generate authorizations?

Why is the status of the authorization objects PLOG and P_PCLX set to *Standard* and why is the traffic light symbol status set to *green*?

Continued on next page

- a) Because this has been created as an organizational level in the defaults of the Profile Generator (indicated by a dollar sign (\$) prefix; prerequisite is that technical names are shown).

b)

Green light:

S_TCODE
P_PCLX

Yellow light:

P_ORGIN
P_PERNR

Red light:

PLOG

- c) Because all fields of these authorization objects could be filled with default values. An organization level filled using the button is interpreted as a PG default value.

4. Set full authorization for all open authorization values. Generate the profile, accept the proposed profile name, and exit role maintenance.

-
- a) To do this, click the traffic light symbol at the top hierarchy level, and confirm the assignment of full authorization. Save your settings and generate the profile. Exit role maintenance.

Task 3:

Convert the profile *A_ANZEIGE*.

1. Where can you convert profiles?

- a) You can convert profiles in transaction “SU25” with *step 6* or using the Customizing path in the solution for task 1.1 (submenu *Copy SAP Check Indicators and Field Values*).

2. Which type of profiles can be used for this, and which types of conversion are available?

Types:

Continued on next page

1.) _____

2.) _____

- a) Only **manually created profiles** can be converted. Generated profiles are not available for selection.

You can choose between two options:

1. Optimized
2. Identical to profile

3. Convert the specified profile so that a menu may be automatically created.
View the result. Could a menu be created?

a) Yes.

4. Could all transactions from the profile be included in the menu?

a) No.

The transactions that describe an area could not be resolved. In the authorization object *S_TCODE*, field *TCD*, there is still a specification with the value “SU5*”. This area could not be resolved and would therefore also not appear in the menu for the role.



Lesson Summary

You should now be able to:

- Perform the steps necessary to install the Role Maintenance
- Find default values and check indicators in the system
- Modify, delete, or extend the default values of the Role Maintenance
- Perform the necessary steps after an upgrade for postprocessing old and new authorization values
- Describe new functionality in transaction SU25

Lesson: Access Control and User Administration

Lesson Overview

This lesson will provide an overview of the password rules and special users, and introduce 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.



Lesson Objectives

After completing this lesson, you will be able to:

- Define password rules and system profile parameters
- Protect special users in the SAP system
- Protect SAP functions with authorization object S_TCODE
- Protect tables and views using authorization groups
- Protect programs with authorization groups
- Describe tasks in user and authorization administration
- List options for separating functions of user and authorization administration
- Describe options for decentralization of user administration
- Create user and authorization administrators with limited rights (using authorization objects)

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.

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.

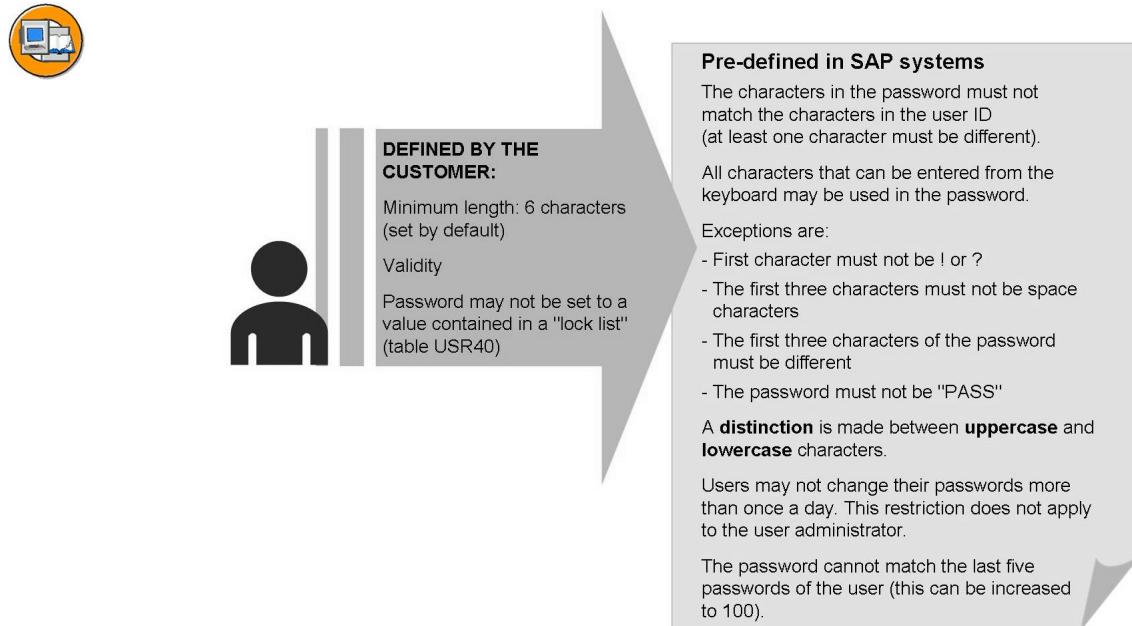


Figure 80: Password Rules

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 the users have to 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 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>	6*	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 *

* New default value and value range since SAP NetWeaver 7.0

Figure 81: Password Checks with System Profile Parameters 01

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 (transaction “RZ11”) or the online documentation.

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 maximum length was previously “8” characters. 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.

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.

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 1 character



Hint: The setting that determines that users must create a new password that differs from the previous 5 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.

You can define additional password restrictions in table *USR40*.

SAP Web Application Server 6.20 and 6.40 offered the parameters *login/password_max_new_valid* and *login/password_max_reset_valid*. They specified for how long an initial password for a newly created user or a password that was reset by an administrator was valid. With SAP NetWeaver AS 7.0, they have been replaced by the parameter *login/password_max_idle_initial*.



Hint: 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.

Another new parameter that was introduced after SAP Web AS 6.40 is *login/password_max_idle_productive*. This 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.

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	

* New default value and value range since SAP NetWeaver 7.0

Figure 82: Password Checks with System Profile Parameters 02

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.

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.



Hint: 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).

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.

Other new features with NetWeaver Application Server 7.00

The following parameters are new. They add a new level of detail to the implementation of the password policy in the SAP system.

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: The parameter value defines the minimum number of uppercase letters a password must have. The default value is “0”.

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: 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: 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”.



Initial Logon Procedure in SAP Clients

Client	000	001	066	Client (new)
User	SAP*	DDIC	EarlyWatch	SAP*
Initial Password			support	pass
	06071992	No longer 19920706		

! Since these users are public information, they must be protected against unauthorized access.
NEW: You are prompted for SAP* and DDIC during the installation in clients 000/001.

Figure 83: 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, the clients *000* and *066* are created (the client *001* is not always created during an SAP installation; it is also created, for example, during an SAP R/3 installation). 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.

The 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.

The 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.

The 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.

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 on the following pages.

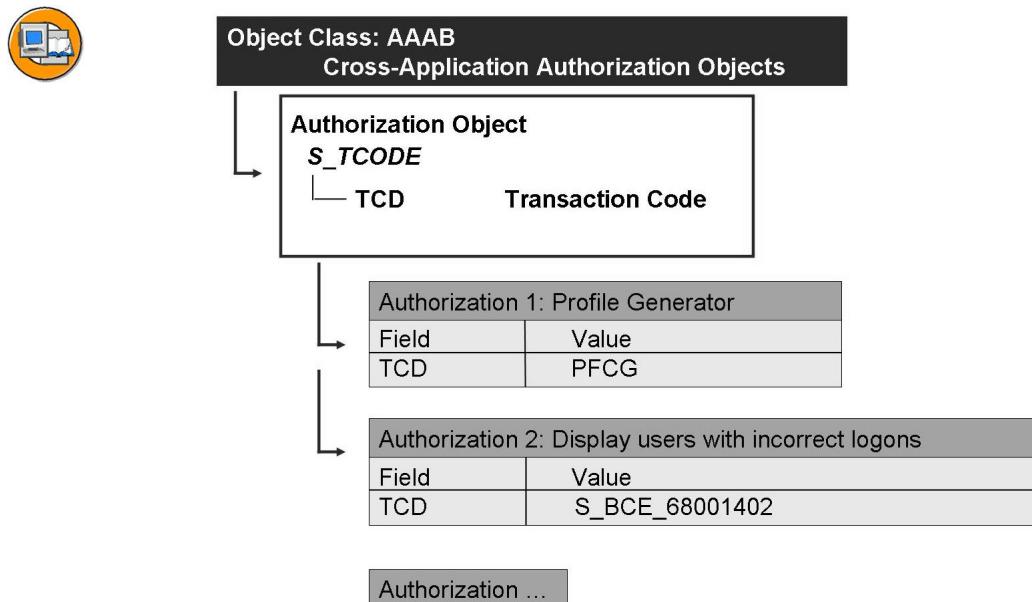


Figure 84: Authorization Check for Transaction Start



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 the Role Maintenance if he 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. He can only execute this report if he 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).

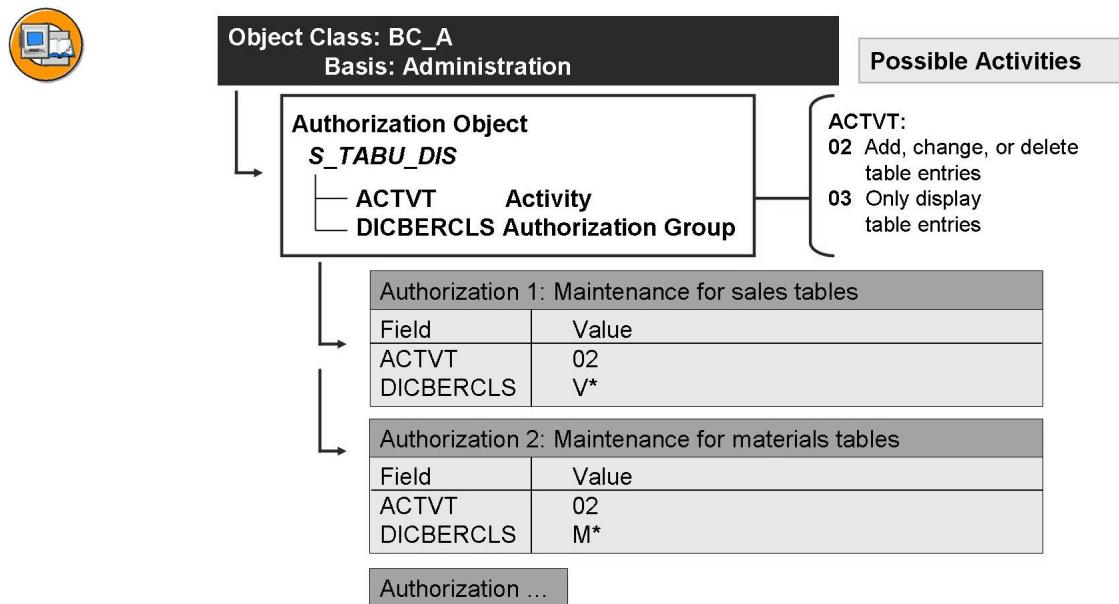


Figure 85: Table Maintenance Authorization

You can use the row-oriented authorizations introduced with SAP R/3 4.6C to restrict access to tables with business organizational units. Previously, only the authorization objects *S_TABU_DIS* and *S_TABU_CLI* were available.

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 - max.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 afterwards.

The important tables are:

- *V_DDAT_54*: Assignment of authorization group to tables/view.
- *V_BRG_54*: Assignment of authorization groups to tables/views.



Hint: You maintain these differently, depending on the release status.

- **up to SAP Web Application Server 6.20**

You can use the transaction “SM30” to display or process the table values for *V_DDAT* directly or use the parameter transaction “SUCU” and the parameter for the view *V_DDAT*.

- **As of SAP Web Application Server 6.40**

Use the views *V_DDAT_54* and *V_BRG_54*. The transaction “SUCU ” fails and the system displays the error message “Table/View *V_DDAT* is not in the Dictionary”.

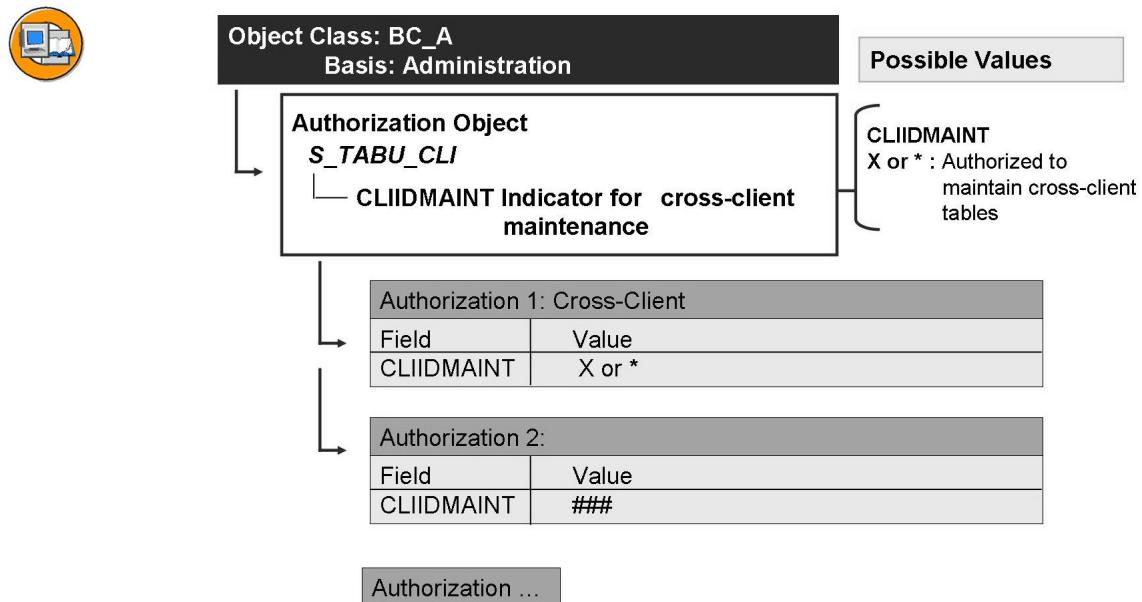


Figure 86: Table Maintenance Authorization (Cross-Client)

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. 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.

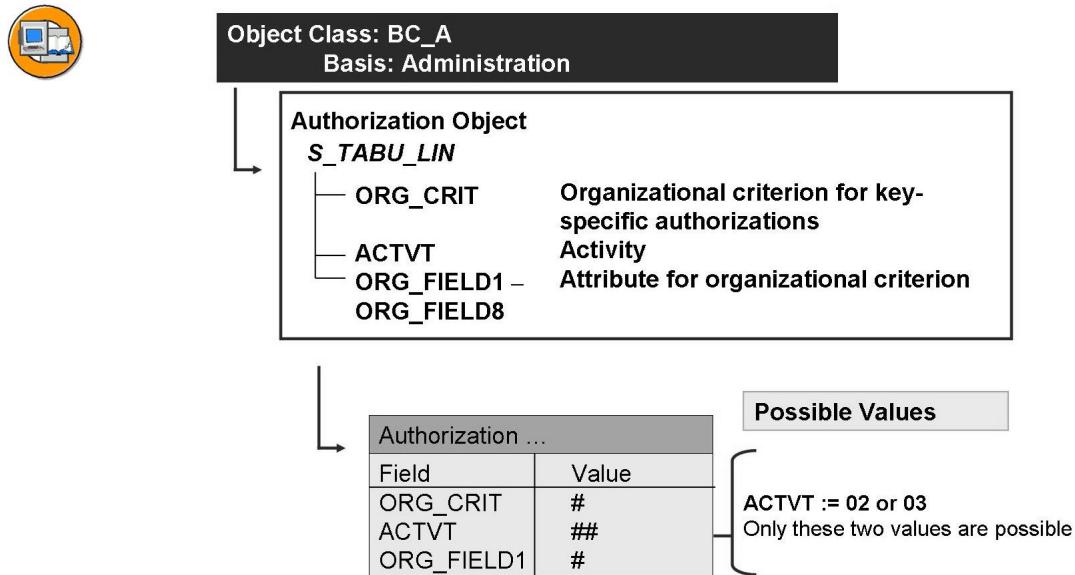


Figure 87: Row-Oriented Authorizations for Tables

New developments for the topic of row-oriented authorizations.

Up to now, you could only use the authorization objects *S_TABU_DIS* and *S_TABU_CLI* to allow or forbid access to complete tables (SAP R/3 4.6C, row-oriented authorizations).

Through the introduction of organization criteria, you can restrict a user's access rights to specific parts of a table. A possible use for *S_TABU_LIN* would be 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:

- 1. Attributes 1 to 8 for the organizational criterion, each attribute for a certain table key field.

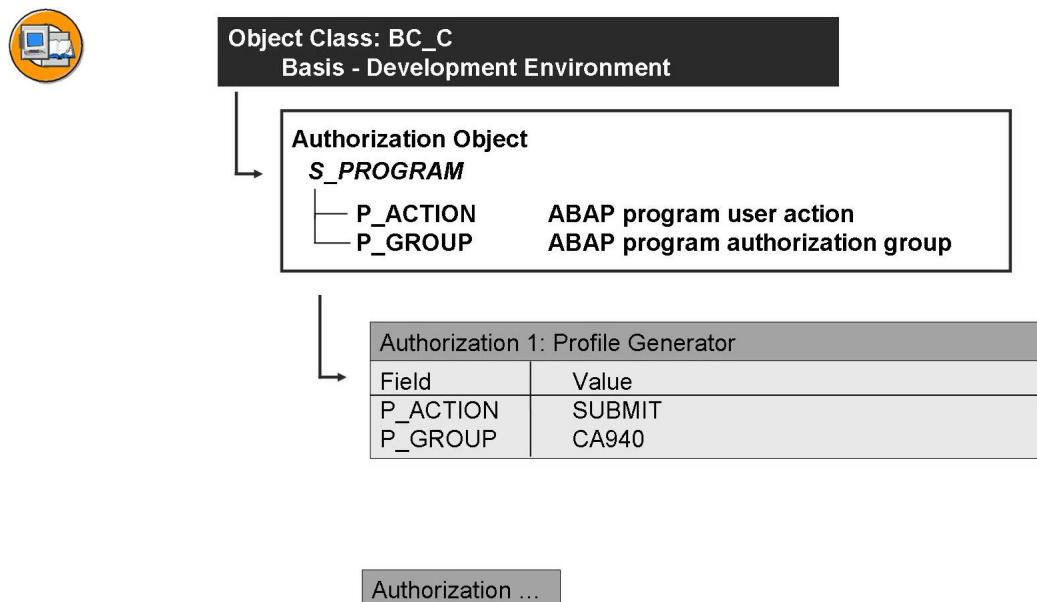


Figure 88: ABAP: Program Flow Check

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*)

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.

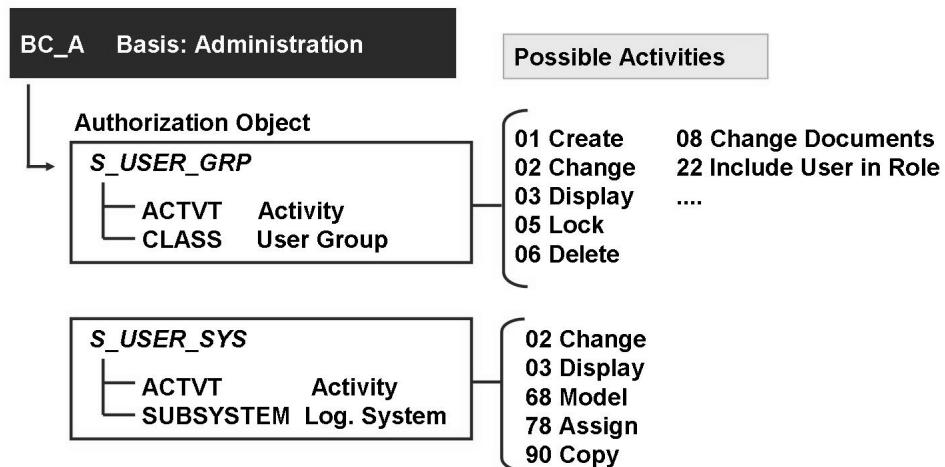


Figure 89: Authorization Objects: Users

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.

The object User Master Record Maintenance: System for Central User Maintenance (*S_USER_SYS*) defines which system a user administrator can access from the central user administration and the activities that are allowed.

The 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_SAS* can be used to check system-specific role and profile assignments for users in Central User Administration (CUA). You must enable the checks for the object in the transactions SU01 and PFCG using the Customizing switch *CHECK_S_USER_SAS* (SM30, view *PRGN_CUST*).

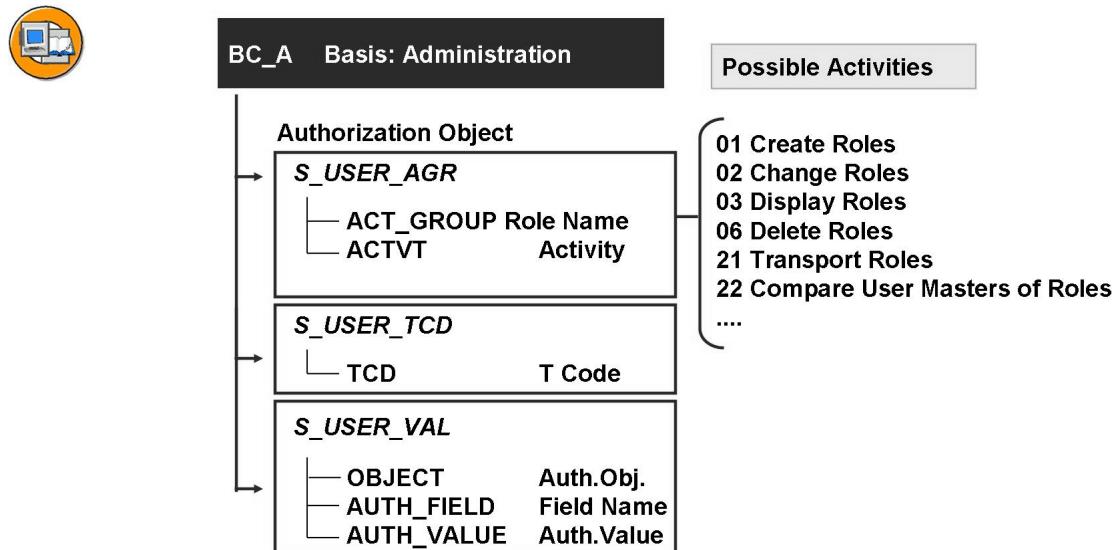


Figure 90: Authorization Objects: Roles

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 to access 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.

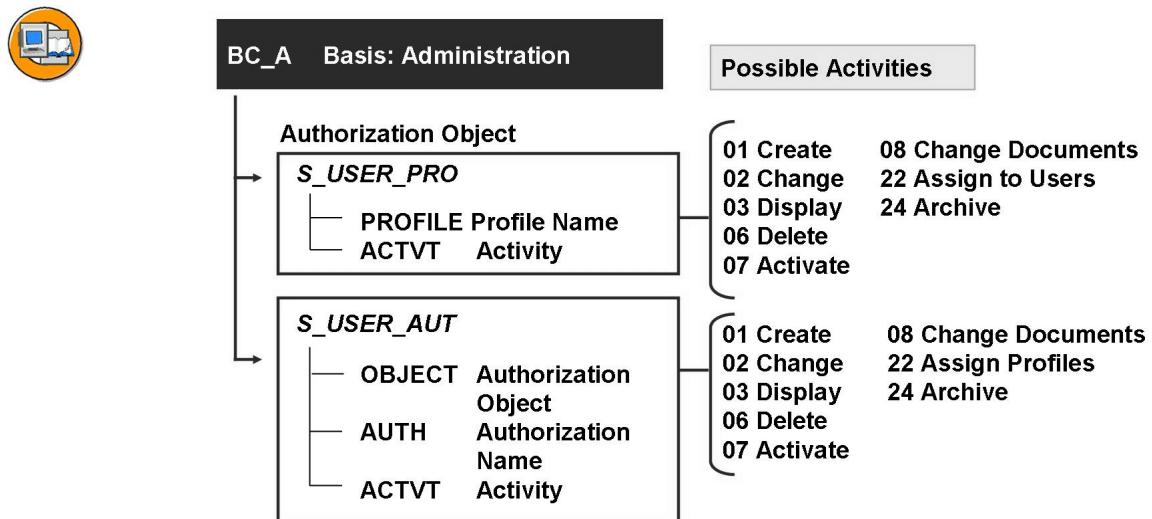


Figure 91: Authorization Objects: Profiles and Authorizations

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.

Options for Decentralization of User Administration



- 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 a maximum in 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.

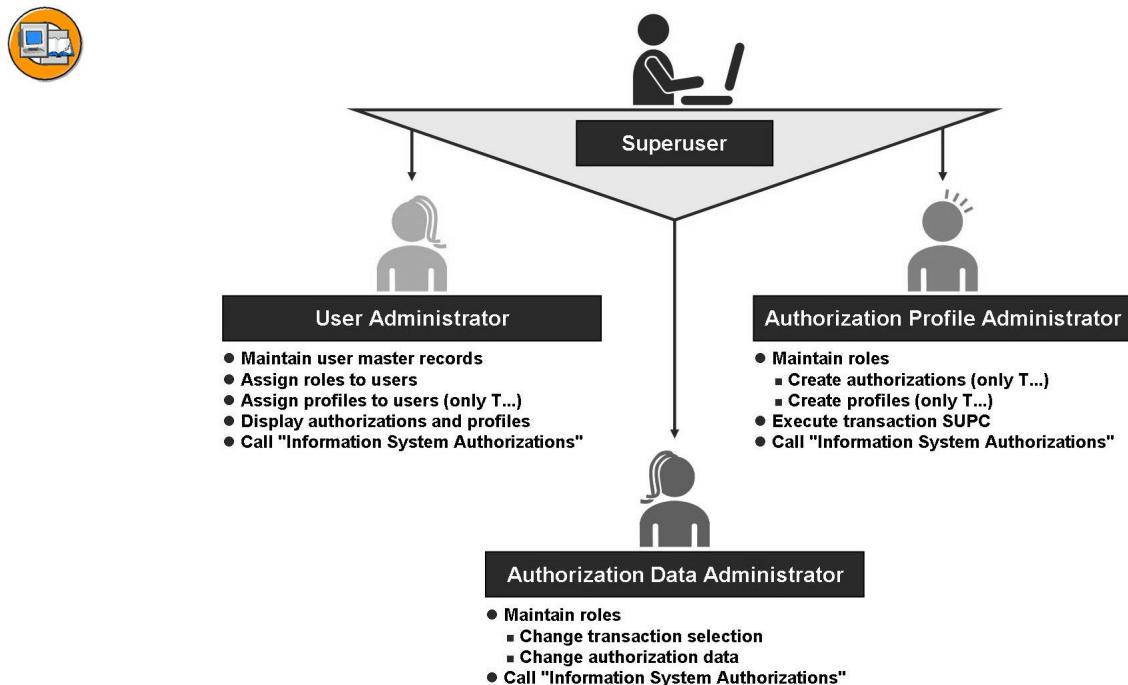


Figure 92: Separation of Functions

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 the Role Maintenance since he 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 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.

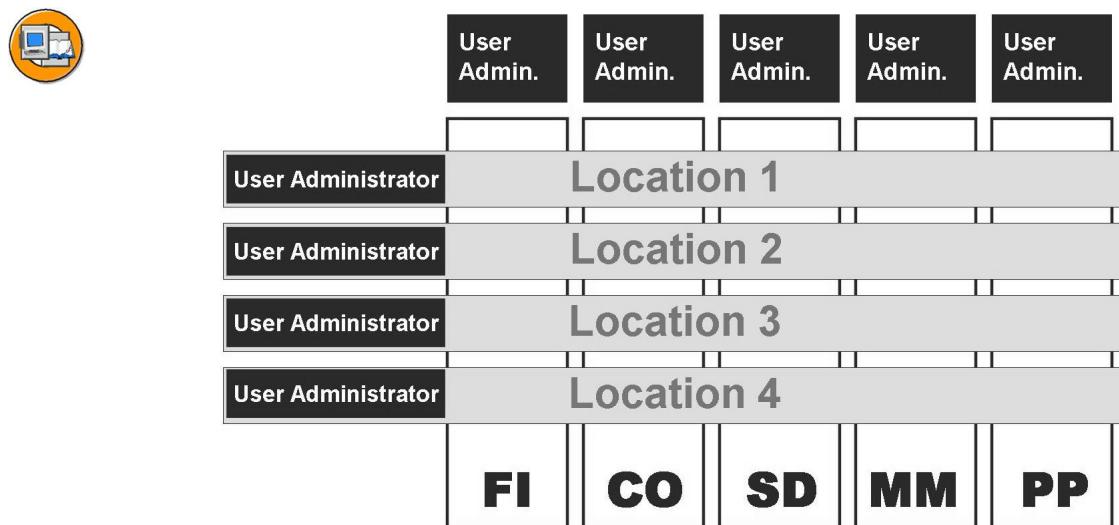


Figure 93: Decentralized User Administration

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 Admin. and Authorization Profile Admin.	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 94: 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 Admin.	Authorization Profile Admin.	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 95: 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 Admin.	Authorization Profile Admin.	FI User Administrator	MM User Administrator	Central User Admin.
S_USER_GRP						
ACTVT	*	03, 08	03, 08	02, 03, 05, 22 FI_USER	02, 03, 05, 22 MM_USER	01, 03, 06, 08
CLASS	*	*	*			*
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	*	*	*	*	*	*
OBJECT	*	*	*	*	*	*

Figure 96: 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*).

Exercise 9: Access Control and User Administration

Exercise Objectives

After completing this exercise, you will be able to:

- Create a role to grant authorizations for user maintenance within your user group
- Test the settings you made
- Determine authorization groups for protecting tables
- Restrict table accesses

Business Example

In the course of their daily work, users may receive a message: *You are not authorized to....* This system behavior is to be recreated here using an example, and then analyzed.

Task 1:

Create a role for user administration activities.

1. Create the role GR##_BC_USR_ADMIN by **selectively copying (without user assignments)** the role ADM940_BC_ADMIN.
2. Change the description for your group and save the role.
3. Change to the Authorizations tab page and choose *Change authorization data*.

Restrict the authorization values so that a user who is assigned at a later time may only assign roles and profiles beginning with *GR##* or *ADM940*.

Ensure that only user group *ZGR##* may be assigned and maintained. If there are other unmaintained fields, assign full authorization for them.

4. Generate the profile. Accept the proposed profile name.
5. What is the status of the User tab and why?
6. Exit the transaction and change the user master record of user administrator GR##-ADM.

Remove the role ADM940_BC_ADMIN.

Add the role that you have just created, GR##_BC_USR_ADMIN to the user master record.

Continued on next page

Save the user master record and go to the maintenance transaction for the roles.

Task 2:

Log onto the system with user GR##-ADM.

1. Create a test user GR##-TEST and try to assign this user your neighbor's user group. Can you save the user master record?

If not, why does the assignment fail?

2. What can be implemented by assigning user groups?

3. Assign the role ADM940_PLUS to the test user GR##-TEST.

Can you assign a role delivered by SAP?

(Such as SAP_HR_...)

If not, why does the assignment fail?

Task 3:

Create authorizations so that a user can view specific tables in transaction "SM30". The user must be able to display two tables: the company code table and the business area table. Those table names are V_T001 (company code) and V_TGSB (business area).

1. Find out about authorization object S_TABU_DIS.

Display the documentation for the authorization object S_TABU_DIS.

What is the main function of this authorization object?

2. Which activities are allowed?

Continued on next page

3. What is stored in table V_DDAT_54?

4. What is stored in table V_BRG_54?

Task 4:

Find the authorization group assigned to tables V_T001 or V_TGSB.

1. The authorization group for table V_T001 is:

2. The authorization group for table V_TGSB is:

Task 5:

Create a role for reading tables V_T001 and V_TGSB.

1. Create the role GR##_FI_TAB_ANZ and write a short description.
2. Assign authorizations for transaction “SM30” (Extended Table Maintenance) in the menu, and use the authorization objects to allow only read access to the above tables.

Generate the profile and accept the proposed name.

3. Assign the role to your user GR##-FI1. Perform a user master comparison and exit role maintenance.

Task 6:

Log on as GR##-FI1. Call transaction “SM30”, and answer the following questions:

1. Can you display table V_T001? Why?

2. Can you change table V_T001? Why?

3. Can you display table V_TGSB? Why?

Continued on next page

-
4. Can you display table V_TVKO? Why?
-
-

Solution 9: Access Control and User Administration

Task 1:

Create a role for user administration activities.

1. Create the role GR##_BC_USR ADM by selectively copying (**without user assignments**) the role ADM940_BC_ADMIN.

- a) **SAP Menu:**

Tools → Administration → User Maintenance → Roles, (transaction code “PFCG”). “PFCG”).

Copy with the relevant icon. In the dialog box, choose *Copy selectively* (without user assignment).

2. Change the description for your group and save the role.
- a) Enter a description for your role.
3. Change to the Authorizations tab page and choose *Change authorization data*.

Restrict the authorization values so that a user who is assigned at a later time may only assign roles and profiles beginning with *GR##* or *ADM940*.

Ensure that only user group *ZGR##* may be assigned and maintained. If there are other unmaintained fields, assign full authorization for them.

- a) The field values have to be changed for the following authorization objects (by clicking on the pencil icon).

Object	Field	Value (Interval)
S_USER_PRO	ACTVT	same values
	PROFILE	change <i>GR*</i> to <i>GR##*</i>
S_USER_GRP	ACTVT	same values
	PROFILE	change <i>Z*</i> to <i>ZGR##*</i>
S_USER_AGR	ACTVT	same values
	ACT_GROUP	change <i>GR*</i> to <i>GR##*</i>

4. Generate the profile. Accept the proposed profile name.
- a) Use the *Generate* button or choose the menu path *Authorizations → Generate*.
5. What is the status of the User tab and why?

Continued on next page

-
- a) The status display is *red*, since the user assignment was not copied with the selective copy.
 - 6. Exit the transaction and change the user master record of user administrator GR##-ADM.

Remove the role ADM940_BC_ADMIN.

Add the role that you have just created, GR##_BC_USR_ADMIN to the user master record.

Save the user master record and go to the maintenance transaction for the roles.

- a) **SAP Menu:**

Tools → Administration → User Maintenance → Users, (transaction code “SU01”).

Save the user master record and go to the maintenance transaction for the roles.

SAP Menu:

Tools → Administration → User Maintenance → Roles, (transaction code “PFCG”). “PFCG”).

Task 2:

Log onto the system with user GR##-ADM.

- 1. Create a test user GR##-TEST and try to assign this user your neighbor's user group. Can you save the user master record?
-

If not, why does the assignment fail?

- a) **SAP Menu:**

Tools → Administration → User Maintenance → Users, (transaction code “SU01”).

No, because the authorization for your own user group was restricted, resulting in an error in the authorization check.

- b) The authorization was restricted to your own user group, resulting in an error in the authorization check.
- 2. What can be implemented by assigning user groups?

Continued on next page

- a) A decentralized user administration, since each administrator may only maintain the users of his or her “own” user group.
3. Assign the role ADM940_PLUS to the test user GR##-TEST.
Can you assign a role delivered by SAP?
(Such as SAP_HR_...)

If not, why does the assignment fail?

-
- a) No.
- b) You are not authorized for entries that begin with “SAP...” (authorization object S_USER_AGR).

Task 3:

Create authorizations so that a user can view specific tables in transaction “SM30”. The user must be able to display two tables: the company code table and the business area table. Those table names are V_T001 (company code) and V_TGSB (business area).

1. Find out about authorization object S_TABU_DIS.
Display the documentation for the authorization object S_TABU_DIS.
What is the main function of this authorization object?

Continued on next page

a) **SAP Menu:**

Tools → Administration → User Maintenance → Role Administration → Roles, (transaction code “PFCG”).

Environment → Authorizations Objects → Display

Choose the *Find* icon and enter the authorization object S_TABU_DIS. The result is the object class BC_A (Basis - Administration). Find the authorization object S_TABU_DIS in the object class BC_A. To display the documentation, choose the i button next to the technical name of the authorization object.

What is the main function of this authorization object?

S_TABU_DIS

Authorizations for displaying or maintaining table contents.

2. Which activities are allowed?

a) S_TABU_DIS:

- 02: - 02: Add, change, or delete table entries
- 03: Only display table contents.

3. What is stored in table V_DDAT_54?

a)



Hint: Depending on the release level, a display error may occur. See the note that appears after graphic 86: “Table Maintenance Authorization”.

Assignment of authorization group to tables/view (display).

4. What is stored in table V_BRG_54?

Continued on next page

a)



Hint: If problems arise, see the note in the previous solution (subtask 3).

Assignment of authorization groups to tables/views (overview).

Task 4:

Find the authorization group assigned to tables V_T001 or V_TGSB.

1. The authorization group for table V_T001 is:
-

- a) **Menu:**

System → Services → Table Maintenance → Extended Table Maintenance, (transaction code: “SM30”). “SM30”).

Enter table V_DDAT_54 and choose *Display*.

Use the *Position...* button to search for table V_T001. Note the authorization group.

FCOR.

2. The authorization group for table V_TGSB is:
-

- a) Use the same search option as in the previous task for table V_TGSB. Note the authorization group.

FCOR.

Task 5:

Create a role for reading tables V_T001 and V_TGSB.

1. Create the role GR##_FI_TAB_ANZ and write a short description.

- a) **SAP Menu:**

Tools → Administration → User Maintenance → Role Administration → Roles, (transaction code “PFCG”).

Create the role GR##_FI_TAB_ANZ and enter a short description (Description tab page).

Continued on next page

2. Assign authorizations for transaction “SM30” (Extended Table Maintenance) in the menu, and use the authorization objects to allow only read access to the above tables.

Generate the profile and accept the proposed name.

- a) Go to the Menu tab page and use the *Transaction* button to add transaction “SM30”.

Go to the Authorizations tab and choose *Change authorization data*.

Enter the value *FCOR* in the open authorization group field in authorization object *S_TABU_DIS* and change the Activity field (*ACTVT*) to 03. Set the authorization object *S_TRANSLAT* to inactive.

Choose *Authorizations* → *Generate* or the corresponding pushbutton.

3. Assign the role to your user GR##-FI1. Perform a user master comparison and exit role maintenance.

- a) On the *User* tab page, enter the user GR##-FI1 and perform a user master comparison (*User comparison* button). Close role maintenance and exit the transaction.

Task 6:

Log on as GR##-FI1. Call transaction “SM30”, and answer the following questions:

1. Can you display table V_T001? Why?

- a) Yes. Because when this table is displayed, authorization group *FCOR*, which is in the user master record, is checked.

2. Can you change table V_T001? Why?

- a) No, because authorization to change (*ACTVT* = 02) was not assigned.

3. Can you display table V_TGSB? Why?

- a) Yes. Because the same authorization group (*FCOR*) is checked as for table V_T001, which is in the user master record.

4. Can you display table V_TVKO? Why?

Continued on next page

-
-
- a) No. The user does not have authorization for authorization group *VCOR*.



Lesson Summary

You should now be able to:

- Define password rules and system profile parameters
- Protect special users in the SAP system
- Protect SAP functions with authorization object S_TCODE
- Protect tables and views using authorization groups
- Protect programs with authorization groups
- Describe tasks in user and authorization administration
- List options for separating functions of user and authorization administration
- Describe options for decentralization of user administration
- Create user and authorization administrators with limited rights (using authorization objects)

Lesson: Troubleshooting and Administration Aids

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.



Lesson Objectives

After completing this lesson, you will be able to:

- Analyze authorization checks in various ways
- Use transaction “SU53” to find missing authorizations (also for other users)
- Run the authorization trace (“ST01”)
- Apply the features of the information system and use them for different tasks
- Understand and apply the **new** functions of the Audit Information System (AIS)

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.

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 authorization trace “ST01”

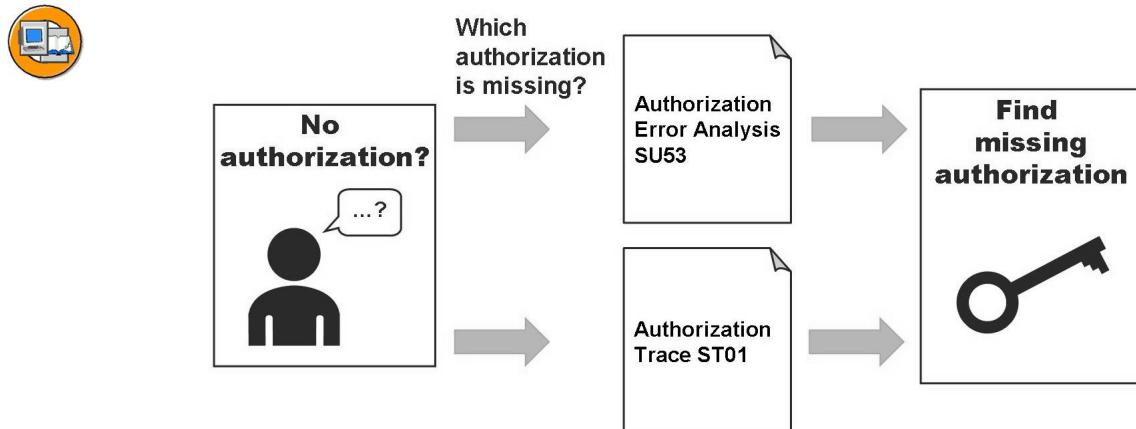
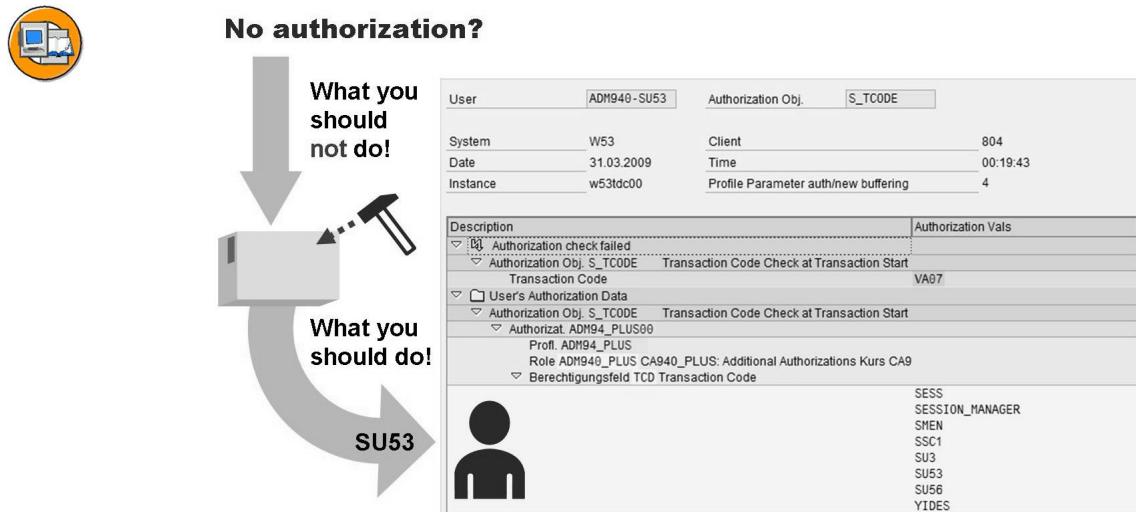


Figure 97: Analyzing Authorization Checks

In the next example, a transaction from the *FI* 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 the transaction code “SU53” in the command field.



Analyze which authorizations are missing and pass this information on to the authorization administrator.

Figure 98: “SU53” Authorization Error Analysis

You now can 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 figure above, user BLITZ calls transaction “FD02” (Change Customer). The message “You are not authorized for transaction FD02” appears. User BLITZ then enters transaction code “/NSU53” in the command field and the system displays the authorization object that caused the last failed authorization check. The system displays the value of the object that the program required (at the top of the display) and the value that the user BLITZ has in his or her user master record (below the required value).

In this case the authorization object *F_KNA1_APP* exists, but instead of the required activity “02” (Change), user BLITZ is only authorized for activity “03” (Display).

The user can also use transaction “SU56” to view which authorizations are currently in his or her buffer.



Caution: The display called with transaction “SU53” always shows the **last** failed authorization check for the user. This can be a long time ago. If, for example, the **current** problem did not occur due to missing errors, but “SU53” still displays something, the display could describe a problem which the user generated when calling a transaction hours earlier. Incorrect values are often then assigned to the new problem.

This incorrect interpretation can be avoided with a few simple steps.

If the user logs off and then **logs in again**, all entries that can be called using transaction “SU53” are reset. If the user now starts the authorization error analysis, the display is empty.



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 trace (“ST01”).

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 (transaction ST01) to record authorization checks in your own and in external sessions, if the trace and the transaction to be traced are running on the same application server. The trace records each authorization object that is tested, along with the object's fields and the values tested.

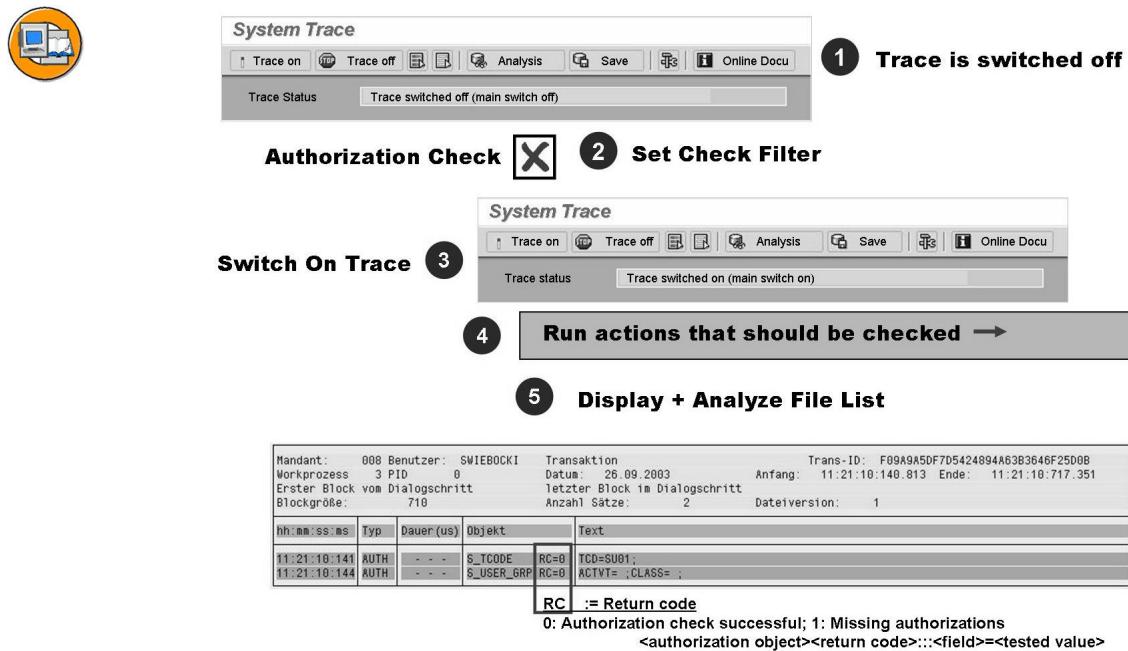


Figure 99: Authorization Trace ST01

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 last 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 a 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:

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 you determine which authorizations you consider critical and regularly review which users have these authorizations in their profiles.

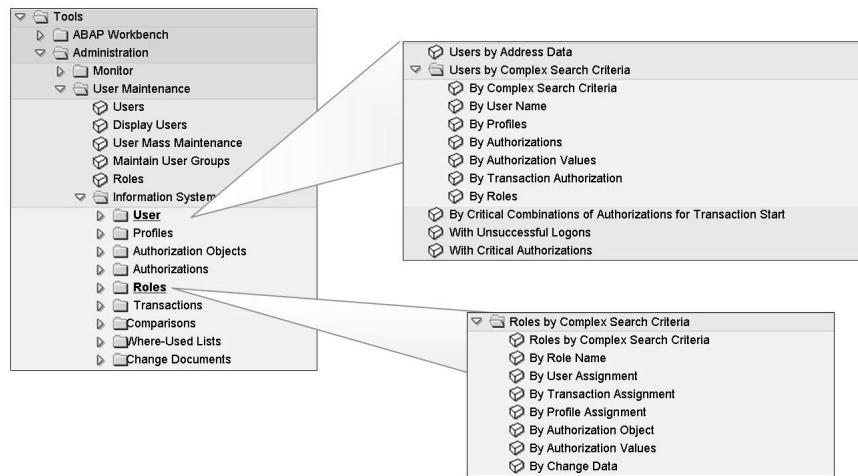


Figure 100: Information System

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/dscsap/revis/index.htm>.

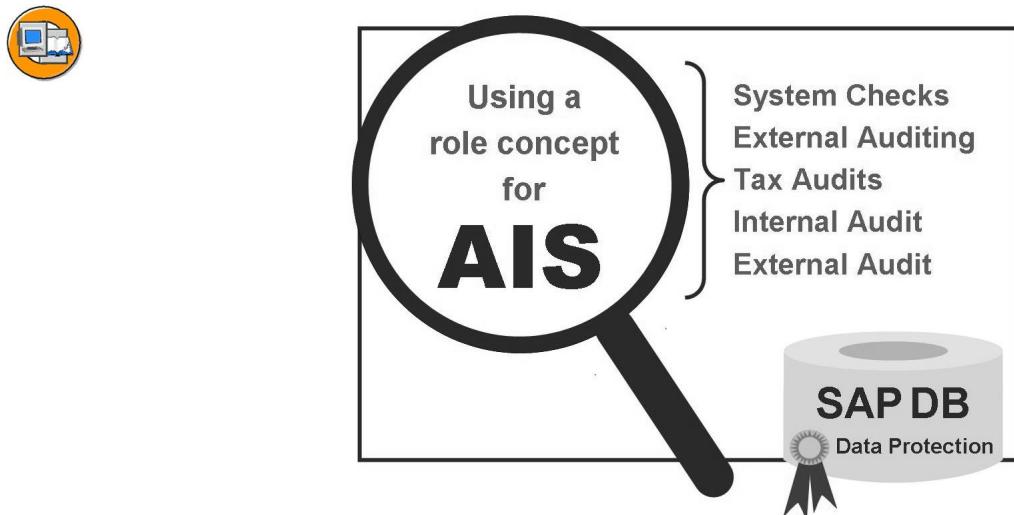


Figure 101: Audit Information System

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 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. 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***”.

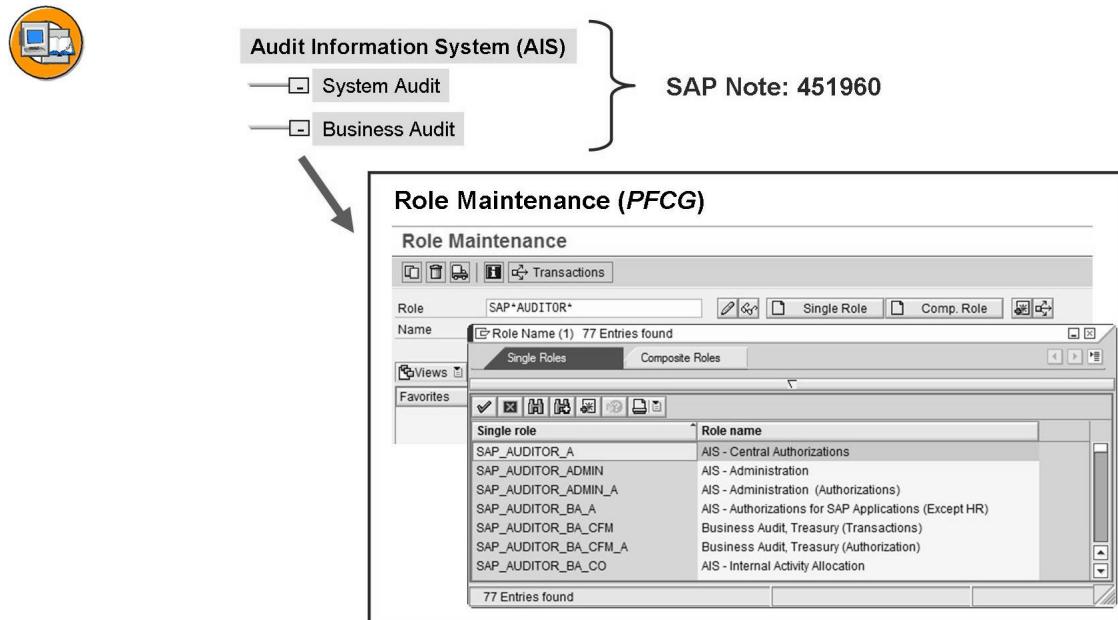


Figure 102: Excerpt from the search results “SAP*AUDITOR*” in role maintenance

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

Exercise 10: Troubleshooting and Administration Aids

Exercise Objectives

After completing this exercise, you will be able to:

- Use the Audit Information System (AIS)
- Use reports in the authorization information system
- Analyze the created authorization concept
- Answer practical questions

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 system using corresponding links in the system and are available in the AIS and information system.

Task 1:

You are the data protection officer and want to check the SAP system's assignment of authorizations and security. For this reason, you must add the role "ADM940_AUDITOR_SA_BC_CCM_USR" to your course user *ADM940-##* and run the master record comparison. Then familiarize yourself with the enhancements to the user menu. If you cannot find the entries required for the following tasks right away, use the "Find" icon.

1. Display all the users with incorrect logons.

How often did your users (GR##... or ADM940-##) log on incorrectly?

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? If yes, when?

Exit the search and continue with task 2.

Continued on next page

Task 2:

You are authorization administrator and are in the consolidation phase after the start of production.

1. Compare the settings of the authorizations between your user GR##-ADM and user GR??-ADM of your neighbor.

Are there differences? If yes, which?

2. Find out which users may execute transaction “MB1C”.

If user GR??-MM1 of your neighbor is displayed, find out the date and time when it was created.

3. Display all the users assigned to the role GR##_MM_MAT_ANZ.

List three of these users.

4. Display an overview of all the users you created (GR##...) with their assigned roles.

Which users still do not have module-specific roles?

Task 3:

You have an additional task as the authorization administrator, in the consolidation phase after production operation begins.

1. The sales manager with user ID GR##-SD1 calls you. He tells you that he cannot run any SD transactions (the composite role GR##_SD_SALMGR is missing). His SAP Easy Access Menu only contains general transactions.

Look at this problem. Then make a small test and tell the sales manager his new initial password, which you set up after the test.

2. You get a mail from the production manager immediately thereafter. The production manager has employed a new senior store person who must only be able to post in plant 1000 (role GR##_MM_IM_POST1000)..

Look at this problem. Then make a small test and tell the new senior store person his or her new initial password, which you set up after the test.



Hint: Use existing master data to solve this problem.

Solution 10: Troubleshooting and Administration Aids

Task 1:

You are the data protection officer and want to check the SAP system's assignment of authorizations and security. For this reason, you must add the role "ADM940_AUDITOR_SA_BC_CCM_USR" to your course user *ADM940-##* and run the master record comparison. Then familiarize yourself with the enhancements to the user menu. If you cannot find the entries required for the following tasks right away, use the "Find" icon.

1. Display all the users with incorrect logons.

How often did your users (GR##... or ADM940-##) log on incorrectly?

- a) *User Menu → Information System Users and Authorizations → Users*, entry: "Users with Invalid Logons".

The number of incorrect logons is displayed in the last column.

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? If yes, when?

Continued on next page

Exit the search and continue with task 2.

- a) You can request information about special users by following **User Menu → Authentication → Special Users**, entry: “Check Passwords and Special Users” (or by using the program RSUSR003). All “login*” parameters are displayed with this call too.

How many characters are set for the minimum password length?

System parameter: **login/min_password_lng := “6”**

- b) After how many incorrect logons is the user locked?

System parameter: **login/fails_to_user_lock := “5”**

- c) Is the user automatically unlocked? If yes, when?

System parameter: **login/failed_user_auto_unlock :=“yes or no -> at midnight”**

You can view the descriptions of the system parameters in transaction RZ11. “The user is automatically unlocked at midnight”.

Task 2:

You are authorization administrator and are in the consolidation phase after the start of production.

1. Compare the settings of the authorizations between your user GR##-ADM and user GR??-ADM of your neighbor.

Continued on next page

Are there differences? If yes, which?

-
- a) **User Menu → Information System Users and Authorizations → Comparisons**, entry: “Comparisons of Users”.

Enter your user GR##-ADM and the user of your neighbor GR??-ADM and choose execute.

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.

Are there differences? If yes, which?

Object	Field	Value (Interval)
S_USER_PRO	ACTVT	same values
	PROFILE	different values (GR##* < > GR??*)
S_USER_GRP	ACTVT	same values
	PROFILE	different values (ZGR##* < > ZGR??*)
S_USER_AGR	ACTVT	same values
	ACT_GROUP	different values (GR##* < > GR??*)

2. Find out which users may execute transaction “MB1C”.

If user GR??-MM1 of your neighbor is displayed, find out the date and time when it was created.

-
- a) **User Menu → Information System Users and Authorizations → Users**, entry: “Users by Authorization Values”.

Enter the authorization object S_TCODE and choose *Enter Values*.

Enter transaction code “MB1C” (in uppercase) and choose *Execute*.

If user GR??-MM1 of your neighbor is displayed, find out the date and time when it was created.

Select user GR??-MM1 and choose *Change documents*.

You can find the date of creation at the top of the right column.

3. Display all the users assigned to the role GR##_MM_MAT_ANZ.

List three of these users.

Continued on next page

- a) **User Menu → Information System Users and Authorizations → Users**, entry: “Users by Roles”.
- Enter the role GR##_MM_MAT_ANZ and choose *Execute*.
4. Display an overview of all the users you created (GR##...) with their assigned roles.

Which users still do not have module-specific roles?

-
- a) **User Menu → Information System Users and Authorizations → Roles**, entry: “Roles by User Assignment”.

Enter “GR##*” and execute the report.

Choose the Roles or *Activity Groups* button.

Which users still do not have module-specific roles?

GR##-FI1	GR##-FI2
GR##-SD1	GR##-SD2

The users could vary depending on whether you have performed the optional tasks.

Task 3:

You have an additional task as the authorization administrator, in the consolidation phase after production operation begins.

1. The sales manager with user ID GR##-SD1 calls you. He tells you that he cannot run any SD transactions (the composite role GR##_SD_SALMGR is missing). His SAP Easy Access Menu only contains general transactions.

Continued on next page

Look at this problem. Then make a small test and tell the sales manager his new initial password, which you set up after the test.

a) **SAP Menu:**

Tools → Administration → User Maintenance → Users (SU01)

Display the user master record of user GR##-SD1 and check the assigned roles. The roles for the menu entries requested by the sales manager are missing.

Assign the composite role GR##_SD_SALMGR to the user GR##-SD1 (on the Roles tab page) and save the user master record.

Log on with the user to test the user and check that the user menu contains the desired functions.

Then set a new initial password, such as *ADM940*, and mail it to the sales manager in the Business Workplace (transaction code “SBWP”).

2. You get a mail from the production manager immediately thereafter. The production manager has employed a new senior store person who must only be able to post in plant *1000* (role GR##_MM_IM_POST1000)..

Continued on next page

Look at this problem. Then make a small test and tell the new senior store person his or her new initial password, which you set up after the test.



Hint: Use existing master data to solve this problem.

- a) In the exercise *Working with the Role Maintenance Part 1* you created a role GR##_MM_IM_POST1000 that exactly corresponds to the requirements.

Path:

Tools → Administration → User Maintenance → Users, (transaction code “SU01”). “SU01”).

Create a new user master record (GR##-MM3) and assign the role GR##_MM_IM_POST1000 to it. You should also assign the role GR##_MM_MAT_ANZ to it. Log on and test transaction “MB1C” (Enter Other Goods Receipts).

To test the transaction, try to make a posting both in plant 1000 and in plant 1200. If you have set everything correctly, the system will only allow you to post in plant 1000.

Use the following data to test transaction “MB1C”

Movement type	561
Plant:	1000 or 1200
Storage location	0001
Choose <i>Enter</i> .	
Material	P-100
Quantity	10
Choose:	<i>Post (Save)</i>

Then set a new initial password, such as *ADM940*, and mail it to the new senior store person in the Business Workplace (transaction code “SBWP”).



Lesson Summary

You should now be able to:

- Analyze authorization checks in various ways
- Use transaction “SU53” to find missing authorizations (also for other users)
- Run the authorization trace (“ST01”)
- Apply the features of the information system and use them for different tasks
- Understand and apply the **new** functions of the Audit Information System (AIS)



Unit Summary

You should now be able to:

- Perform the steps necessary to install the Role Maintenance
- Find default values and check indicators in the system
- Modify, delete, or extend the default values of the Role Maintenance
- Perform the necessary steps after an upgrade for postprocessing old and new authorization values
- Describe new functionality in transaction SU25
- Define password rules and system profile parameters
- Protect special users in the SAP system
- Protect SAP functions with authorization object S_TCODE
- Protect tables and views using authorization groups
- Protect programs with authorization groups
- Describe tasks in user and authorization administration
- List options for separating functions of user and authorization administration
- Describe options for decentralization of user administration
- Create user and authorization administrators with limited rights (using authorization objects)
- Analyze authorization checks in various ways
- Use transaction “SU53” to find missing authorizations (also for other users)
- Run the authorization trace (“ST01”)
- Apply the features of the information system and use them for different tasks
- Understand and apply the **new** functions of the Audit Information System (AIS)

Unit 6

Transporting Authorizations

Unit Overview

This unit describes the transport of authorization data. Starting with user master records, through roles up to check indicators and customer default values for the Role Maintenance.



Unit Objectives

After completing this unit, you will be able to:

- Copy user master records to other clients
- Transport roles and describe the behavior in the system: With and without profile information, with and without user assignments, in a CUA landscape or without CUA
- Transport check indicators using Transaction “SU25”
- Describe the transport behavior of composite, reference, and derived roles
- List other transport options

Unit Contents

Lesson: Transporting Authorization Components	272
Exercise 11: Transporting Authorization Components.....	279

Lesson: Transporting Authorization Components

Lesson Overview

This lesson will provide an overview about how to transport user master records, roles, and check indicators.



Lesson Objectives

After completing this lesson, you will be able to:

- Copy user master records to other clients
- Transport roles and describe the behavior in the system: With and without profile information, with and without user assignments, in a CUA landscape or without CUA
- Transport check indicators using Transaction “SU25”
- Describe the transport behavior of composite, reference, and derived roles
- List other transport options

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.

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 following transport contents.

Which Authorization Components Can Be Transported?



- User master records
- Roles
- Authorization profiles
- Check indicators

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 further discussed.

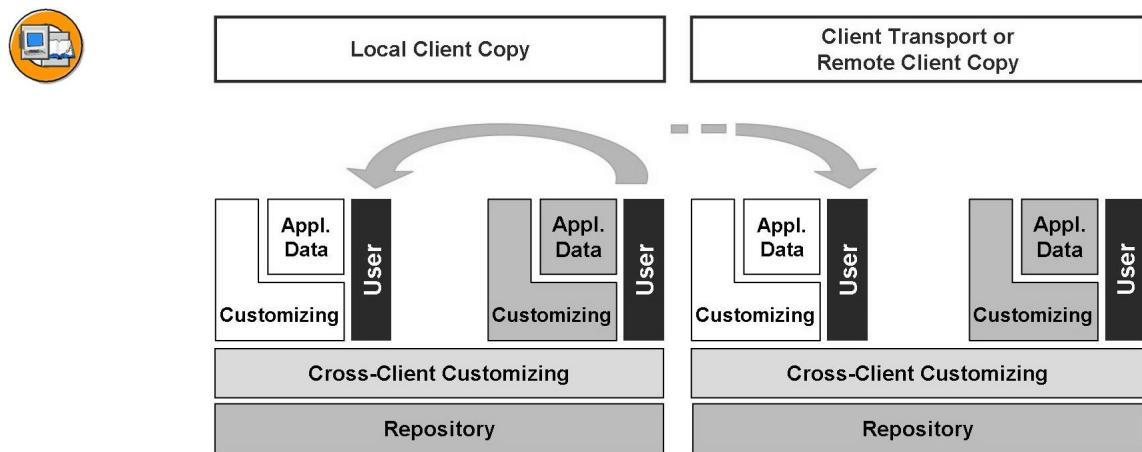


Figure 103: Transporting User Master Records

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 “SCCL” 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 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.

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.

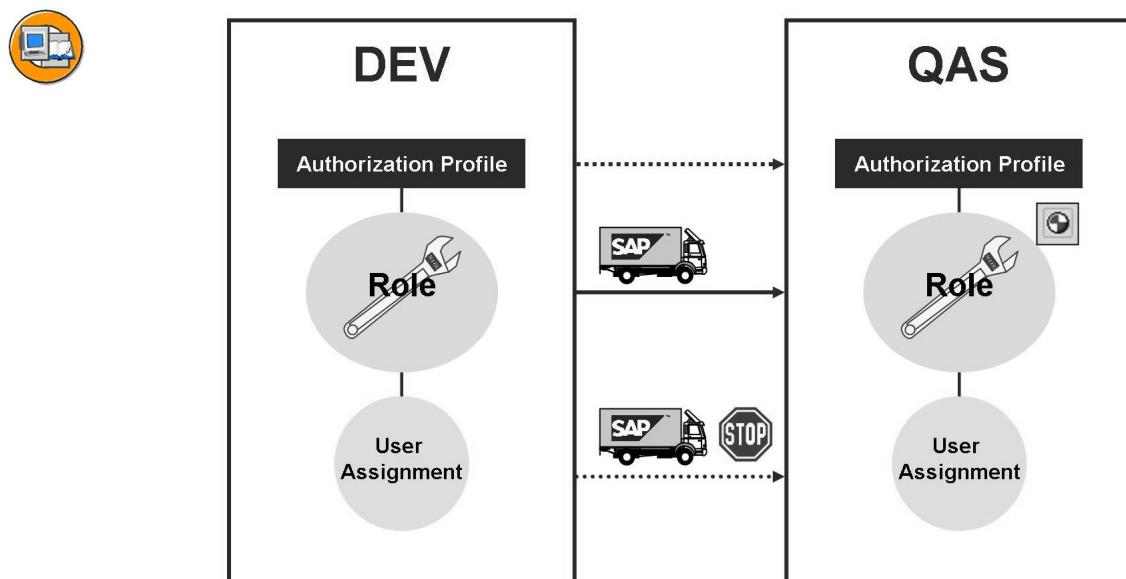


Figure 104: Transporting Roles Without Central User Authorization

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 the 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 the 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 (since SAP R/3 4.6C). 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 the 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”

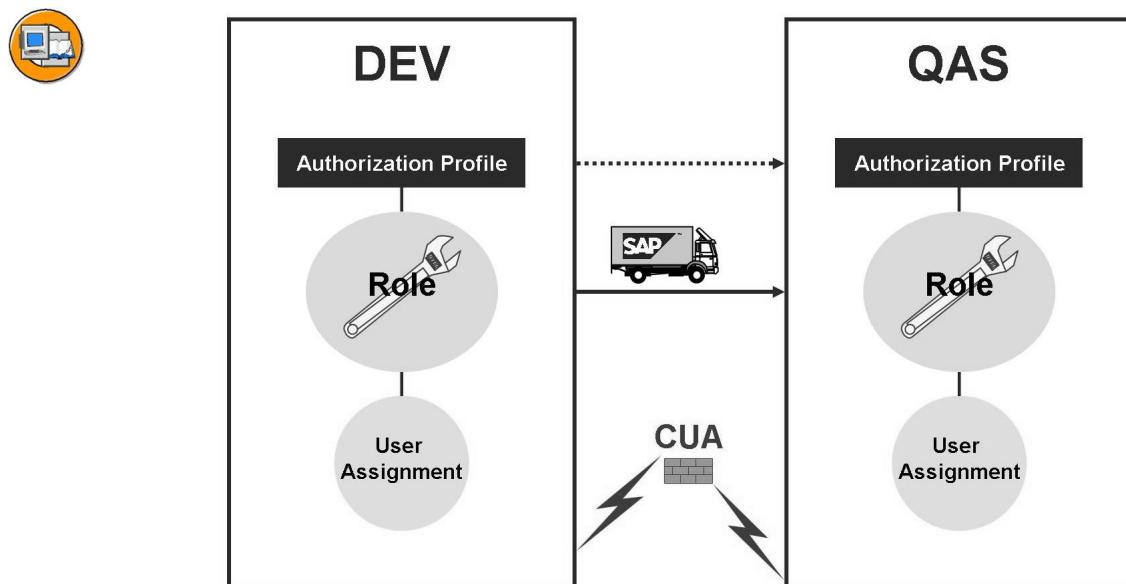


Figure 105: Transporting Roles With Central User Authorization

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 might have to be edited and generated. You can choose to upload or download in the Role Maintenance by choosing *Role → Upload/Download*. Since **SAP R/3 4.6C**, you can save multiple roles in a local file at the same time by choosing *Utilities → Mass download*.

Transporting the Customer Check Indicators

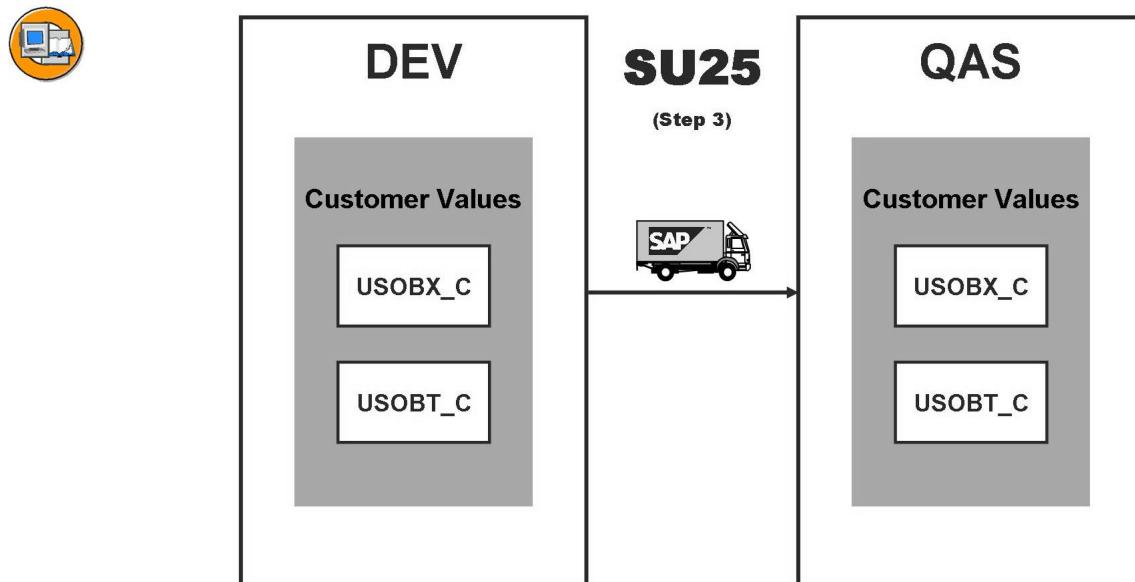


Figure 106: Transporting Check Indicators

The customer tables *USOBX_C* and *USOBT_C*, which control the behavior of the Role Maintenance, must be filled in each system in which the 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, check indicators, 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 the Role Maintenance.
2. You can use transaction “SU24” to change individual check indicators. In this case, the system automatically 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 check indicators and field values in the target system are replaced, and steps 2a-2d cannot be used.

Exercise 11: Transporting Authorization Components

Exercise Objectives

After completing this exercise, you will be able to:

- Set an import lock for user assignments when transporting roles
- Create a transport request for a role
- Transport the contents of USOBX_C and USOBT_C

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:

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?

2. What would happen if the transport request had user assignments and no import lock had been set up?

Task 2:

Open transaction “PFCG” and enter *ADM940_SD_SALES*.

1. 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.

Note the transport request number:

Continued on next page

2. Which objects can be transported with the role during the transport?

Task 3:

Transport tables USOBX_C and USOBT_C.

1. Which transaction and which step is used to do this?

2. Which changes are included in this transport request? For more information, read the help, which appears after you choose the *Transport* icon (the truck). After reading the help, terminate the process and **do not** create a transport request.

Solution 11: Transporting Authorization Components

Task 1:

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?

a) 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?

- a) 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:

Open transaction “PFCG” and enter *ADM940_SD_SALES*.

1. 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.

Note the transport request number:

Continued on next page

a) **SAP Menu:**

Tools → Administration → User Maintenance → Role Administration → Roles, (or transaction code “PFCG”).

Enter the specified name for the role. Confirm your entry with *Enter*. Open the dialog for the transport request by choosing *Role → Transport* or the truck icon.

Transport request number (Example: <DEV>K900376)

2. Which objects can be transported with the role during the transport?
-

- a) After confirming that a transport request is to be created, another selection screen appears. In this dialog box, you can decide which objects are to be included in the transport. You can select the following here:

- User assignment
- Personalization objects

Task 3:

Transport tables USOBX_C and USOBT_C.

1. Which transaction and which step is used to do this?
-

- a) Use transaction “SU25” for this action. Enter this directly in the command field, or choose the menu path *Environment → Installation/Upgrade* in transaction “PFCG”.

You can write the tables to a transport request with *step 3*.

2. Which changes are included in this transport request? For more information, read the help, which appears after you choose the *Transport* icon (the truck). After reading the help, terminate the process and **do not** create a transport request.
-
-
-
-

Continued on next page

-
- a) The following content is included in this transport:

You use this to transport the customer tables of the Role Maintenance. This records all changes that you made in steps 1, 2a, and 2b in a transport request. Changes that you made to check indicators in transaction "SU24" are also recorded.



Lesson Summary

You should now be able to:

- Copy user master records to other clients
- Transport roles and describe the behavior in the system: With and without profile information, with and without user assignments, in a CUA landscape or without CUA
- Transport check indicators using Transaction “SU25”
- Describe the transport behavior of composite, reference, and derived roles
- List other transport options



Unit Summary

You should now be able to:

- Copy user master records to other clients
- Transport roles and describe the behavior in the system: With and without profile information, with and without user assignments, in a CUA landscape or without CUA
- Transport check indicators using Transaction “SU25”
- Describe the transport behavior of composite, reference, and derived roles
- List other transport options

Unit 7

Integration into the Company Landscape

Unit Overview

Some of the daily work for an administrator is the assignment of authorizations to end users. These are often connected to certain rules and processes that always follow the same schema. Two additional methods for user maintenance and authorization assignment are introduced here to help you optimize this regular process and the time spent. These are *Central User Administration* and the *Integration into Organizational Management*.

As an overview, SAP NetWeaver Identity Management is introduced here to give you an impression how the Central User Administration can be enhanced.



Unit Objectives

After completing this unit, you will be able to:

- Explain how the central user administration functions
- Specify the most important steps for setting up the central user administration
- Define distribution rules for user data
- Create, maintain and distribute users centrally
- Perform system comparisons for users that are not yet maintained centrally
- Create organizational units in HR Organizational Management
- Link roles with the organizational plan objects
- Link users with the organizational plan objects
- Perform a comparison of the indirect role and user assignments
- Compare user master record
- Assign roles for a specific period of time
- understand what SAP NetWeaver Identity Management is
- estimate the effort switching from CUA to SAP NetWeaver Identity Management

Unit Contents

Lesson: Central User Administration (CUA).....	289
Exercise 12: Working with Central User Administration.....	301
Lesson: Integration into Organizational Management	307
Exercise 13: Integration into Organizational Management	321
Lesson: SAP NetWeaver Identity Management	327

Lesson: Central User Administration (CUA)

Lesson Overview

This lesson will provide you with information about the principles of Central User Administration, to help you decide whether to implement Central User Administration.



Lesson Objectives

After completing this lesson, you will be able to:

- Explain how the central user administration functions
- Specify the most important steps for setting up the central user administration
- Define distribution rules for user data
- Create, maintain and distribute users centrally
- Perform system comparisons for users that are not yet maintained centrally

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.

Introduction to Central User Administration

In complex system landscapes with multiple systems and clients, the administration effort required to compare and update of the 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**

		200 266 300	010 066 666	005 745 845
SAP R/3 4.6C				
SAP R/3 Enterprise		070 090 500	004 066 520	000 066 770
SAP CRM		000 100 250	000 250 251	000 066 350
	Development		Quality Assurance	Production

Figure 107: 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. The user master records also cannot be automatically synchronized sequentially.



The users are administered in a central client, that is in a dedicated SAP NetWeaver Application Server 7.00 client

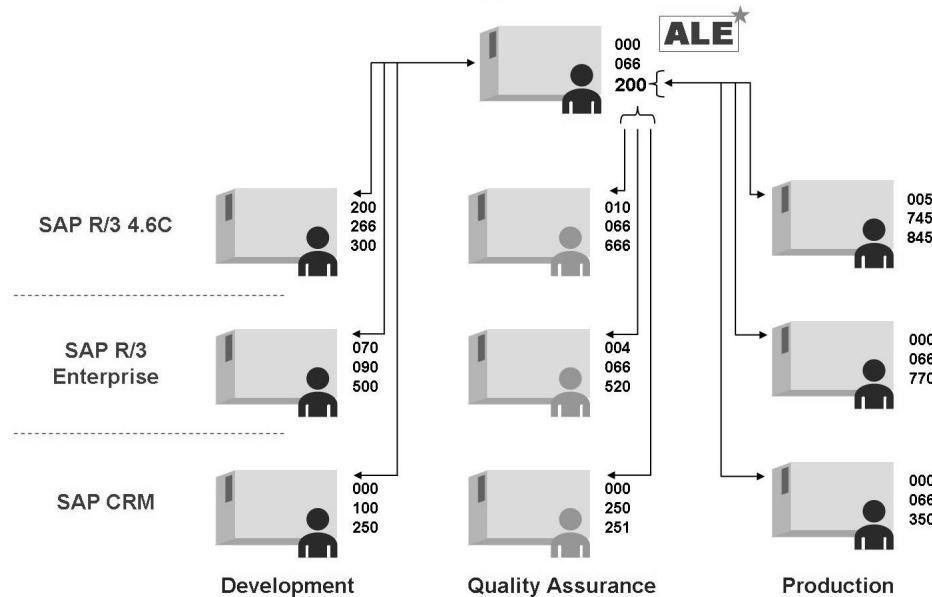


Figure 108: Central User Administration

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 the 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 the user himself or herself 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 the Central User Administration.

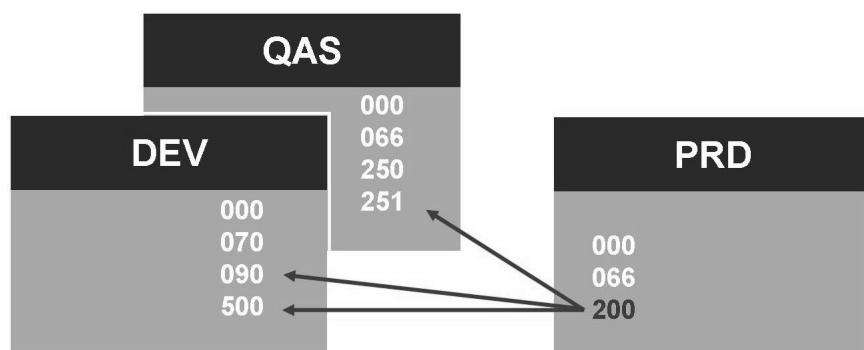


Figure 109: What Can be Distributed?

The following data can be distributed with the 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 in order 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

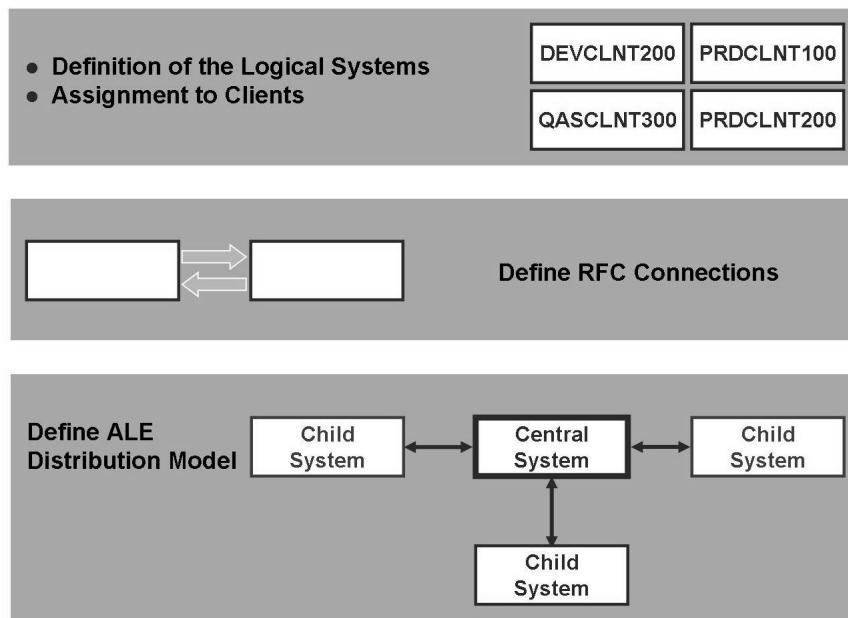


Figure 110: ALE Setup

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 2 ways:

- in the transaction “SALE” by choosing the menu path *IDoc Interface / Application Link Enabling (ALE) → Basic Settings → Logical Systems → Define Logical System*
- or simply 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 network level is performed using RFC (Remote Function Call). 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 the 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 Units 10 and 11 of *Authorizations Made Easy 4.6* in the SAP online documentation. SAP course ADM102, “SAP Web AS Administration II”, deals with the technical implementation.

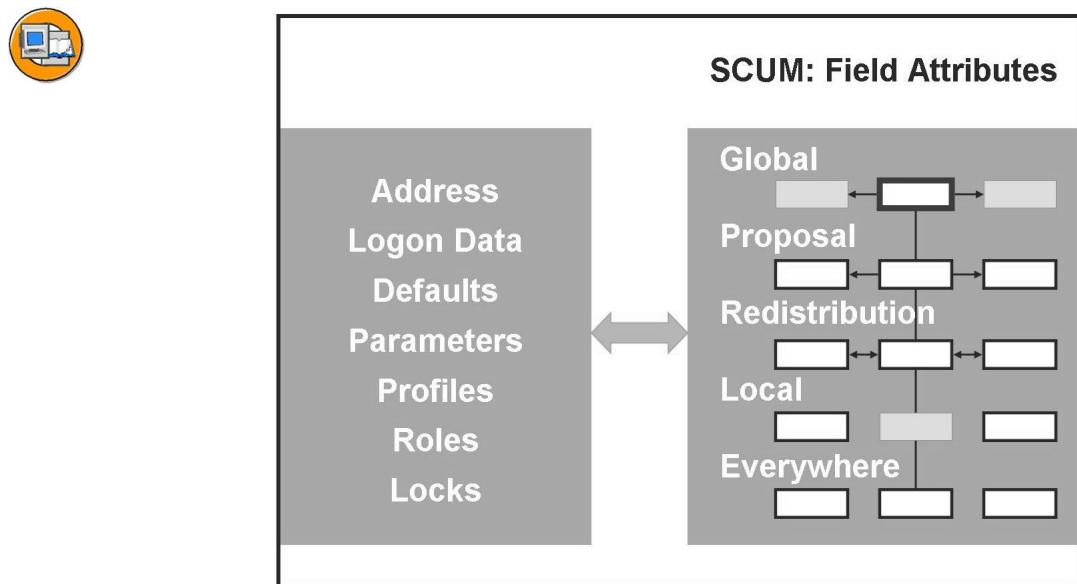


Figure 111: Setup of the Central User Administration

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 the 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 that 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

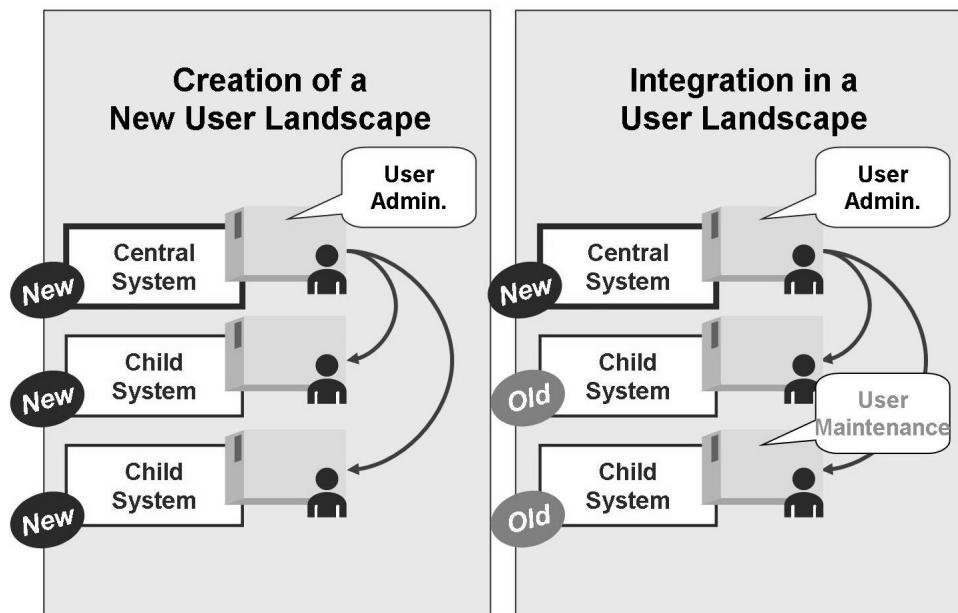


Figure 112: Integration of Existing Systems

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 the Central User Administration. Distribution ensures that the user data is consistent in all systems.

If the 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.

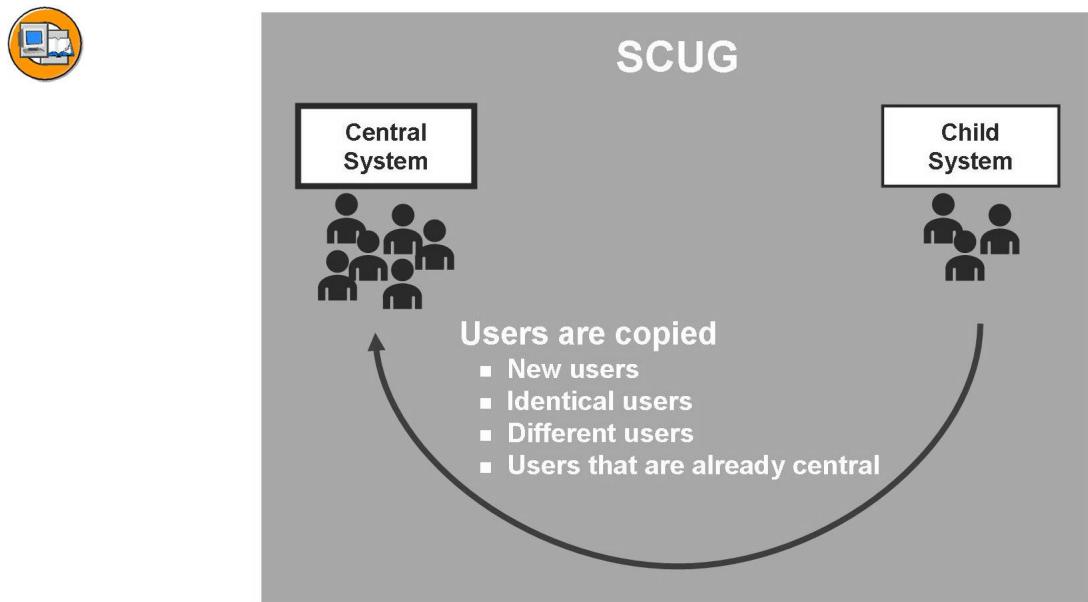


Figure 113: Copying User Master Records

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 the 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 the 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 the 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



Text Comparison					
...	Systems	Roles		Profiles	Groups
	DEVCLNT100 PRDCLNT200	DEVCLNT100 PRDCLNT200	Superuser Agent	T.....	Administrator

Figure 114: Central User Maintenance

After activating Central User Administration, the appearance of user maintenance transaction “SU01” changes.

An additional tab *Systems*, 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 *Save*.

Existing roles are still maintained and new roles are still built in the child systems. To be able 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.

Exercise 12: Working with Central User Administration

Exercise Objectives

After completing this exercise, you will be able to:

- Set up new users
- Check the settings for Central User Administration (CUA)

Business Example

As an administrator, you are to create users with Central User Administration.

Task 1: User Administration with the CUA

Use the user ZBVDEMO as a template to create your own user ZBVDEMO-##.

1. Log on to the central system of the CUA, as specified by the instructor.
2. Create the user ZBVDEMO-## in the child system. Use the last name “Samplename” and the initial password “initial”. Check the user group; this user must be entered in the group “Training”. Assign role ADM940_ZBV_DEMO to your new user and save the settings.



Hint: All systems that you have entered on the *Roles* tab page are automatically entered on the *Systems* tab page. You do not need to enter them there separately.

3. Use the distribution log to check whether the new user was correctly created in the child system.

Task 2: Test the Newly Created User

Check the settings for the new user in the system.

1. Log on to the relevant child system as user ZBVDEMO-##, and edit the relevant user master record with transaction “SU01”. What do you notice on the initial screen of the transaction?
2. Why can you not edit some fields, although you are in change mode?

Task 3: CUA Settings

Check the CUA settings in the central system.

1. Check whether the logical systems that your trainer lists are entered.

Continued on next page

2. Check whether the logical systems have been assigned to the clients in the current system.
3. Check the RFC destinations that connect the central and child systems. What are the names of the RFC destinations?
4. Check the ALE distribution model. Which model is used for the CUA?
5. Check the distribution parameters for the fields. Which fields can be changed in child systems?

Solution 12: Working with Central User Administration

Task 1: User Administration with the CUA

Use the user ZBVDEMO as a template to create your own user ZBVDEMO-##.

1. Log on to the central system of the CUA, as specified by the instructor.
 - a) See task description. Your group-specific user ADM940-## may still have its initial password.
2. Create the user ZBVDEMO-## in the child system. Use the last name “Samplename” and the initial password “initial”. Check the user group; this user must be entered in the group “Training”. Assign role ADM940_ZBV_DEMO to your new user and save the settings.



Hint: All systems that you have entered on the *Roles* tab page are automatically entered on the *Systems* tab page. You do not need to enter them there separately.

- a) Choose *Tools* → *Administration* → *User Maintenance* → *User* or call transaction “SU01”. Create the user ZBVDEMO-##. On the *Logon data* tab page, enter the password “init”. On the *Roles* tab page, perform a *Text comparison from child sys.* so that the F4 help in the central system is updated. After the text comparison has been successfully complete, first enter the child system on the *Role* tab page and then choose role “ADM940_ZBV_DEMO”.
3. Use the distribution log to check whether the new user was correctly created in the child system.
 - a) You can call the distribution log in various ways: in transaction “SU01” by choosing *Environment* → *Distribution Log*, or by choosing *Tools* → *Administration* → *User Maintenance* → *Central User Administration* → *Log Display*.
(transaction “SCUL”). In the *User* field, enter ZBVDEMO-##, make the selection for successful distribution and set the time range to 00:00 to 23:59. Then choose *F8*. If an error occurred during distribution or if it was incomplete, choose *Resend User (F7)*.

Continued on next page

Task 2: Test the Newly Created User

Check the settings for the new user in the system.

1. Log on to the relevant child system as user ZBVDEMO-##, and edit the relevant user master record with transaction “SU01”. What do you notice on the initial screen of the transaction?
 - a) The initial password is “init”. On the initial screen of “SU01” in the child system, the buttons to *Create* and *Copy* users are missing.
2. Why can you not edit some fields, although you are in change mode?
 - a) The fields that cannot be changed are set in such a way that they can only be maintained in the central system.

Task 3: CUA Settings

Check the CUA settings in the central system.

1. Check whether the logical systems that your trainer lists are entered.
 - a) Call transaction “SALE”. Choose *IDoc Interface / Application Link Enabling (ALE)* → *Basic Settings* → *Logical Systems* → *Define Logical System* or call transaction “BD54” directly. Confirm a dialog box with the *Continue* button.
2. Check whether the logical systems have been assigned to the clients in the current system.
 - a) Call transaction “SALE”. Choose *IDoc Interface / Application Link Enabling (ALE)* → *Basic Settings* → *Logical Systems* → *Assign Logical System to Client* or call transaction “SCC4” directly. Confirm a dialog box with the *Continue* button. Select the clients in question and show the detailed display (*Details* button). There should be an entry in the *Logical System* field.
3. Check the RFC destinations that connect the central and child systems. What are the names of the RFC destinations?
 - a) Call transaction “SALE”. Choose *IDoc Interface / Application Link Enabling (ALE)* → *Communication* → *Create RFC Connections* or call transaction “SM59”. View the SAP R/3 connections. The RFC destinations have the same names as the logical systems to which they are connecting.

Continued on next page

4. Check the ALE distribution model. Which model is used for the CUA?
 - a) Call transaction “SALE”. Choose *IDoc Interface / Application Link Enabling (ALE) → Modelling and Implementing Business Processes → Configure Predefined ALE Business Processes → Cross-Application Business Processes → Central User Administration → Select Model View for Central Administration*, or call transaction “SCUA”. The system displays the model view used.
5. Check the distribution parameters for the fields. Which fields can be changed in child systems?
 - a) Call transaction “SALE”. Choose *IDoc Interface / Application Link Enabling (ALE) → Modelling and Implementing Business Processes → Configure Predefined ALE Business Processes → Cross-Application Business Processes → Central User Administration → Set Distribution Parameters for Fields*, or call transaction “SCUM”. All parameters that are not set to *global* can be changed in the child system.



Lesson Summary

You should now be able to:

- Explain how the central user administration functions
- Specify the most important steps for setting up the central user administration
- Define distribution rules for user data
- Create, maintain and distribute users centrally
- Perform system comparisons for users that are not yet maintained centrally

Lesson: Integration into Organizational Management

Lesson Overview

This lesson will give you an impression of the advantages and possibilities that Organizational Management offers for assigning authorizations to users in a company.



Lesson Objectives

After completing this lesson, you will be able to:

- Create organizational units in HR Organizational Management
- Link roles with the organizational plan objects
- Link users with the organizational plan objects
- Perform a comparison of the indirect role and user assignments
- Compare user master record
- Assign roles for a specific period of time

Business Example

If employees in your company often change position within the company, authorization administration can be significantly simplified through a link to organizational units from HR Organizational Management.

Basic Concept of “Indirect Role Assignment”

Requirements for daily administration

Imagine that you must set up and assign authorizations for a trainee. During his or her training, this trainee works with various departments (procurement, controlling, HR department, and so on).

Over time, the trainee “collects” authorizations, and after some time has been assigned various roles. He or she has successively received ever more authorizations, because the administration team has forgotten to remove the authorizations that are no longer relevant for the trainee after he or she changes department.



- Managing role assignments directly for users can become cumbersome in large implementations.
- Since users move or change jobs in your organization, their authorizations must be reviewed.

Solution to reduce the administration effort required:

If the roles are now assigned to the objects of the organizational plan, such as positions, the employees, who are **indirectly** assigned to these positions through the organizational plan, can inherit the roles.

Advantage: As soon as an employee changes position, he or she also loses the corresponding authorizations (since these depend not on the user, but on the position).



- Create roles based on organizational objects, such as positions in your organization. For example: Sales manager, accountant, and secretary.
- Assign the roles to your organizational plan. Users then inherit the authorizations (indirectly) in accordance with their position in the organizational plan.

Advantages:

Substitution and Transfers

- If roles were assigned directly to specific employees, then each time the user's responsibilities change, the corresponding assignment of roles would have to be changed
- If, however, the assignments are based on the notion of positions, then no adjustments will have to be made within the agent assignments of roles.

Time-Dependent Planning in Reorganization Processes

- SAP Organizational Management allows both the validity and the assignment of organizational objects to be planned and activated according to the time available. You must schedule the User Master Record Update program so that profiles can be added or removed based on changes to the organizational plan.

Structure of an SAP Organizational Management

An organizational plan is a set of information that dynamically describes the structural and personal environment of your company. Using the tools provided by the *Organizational Management* component, you can create an organizational plan.

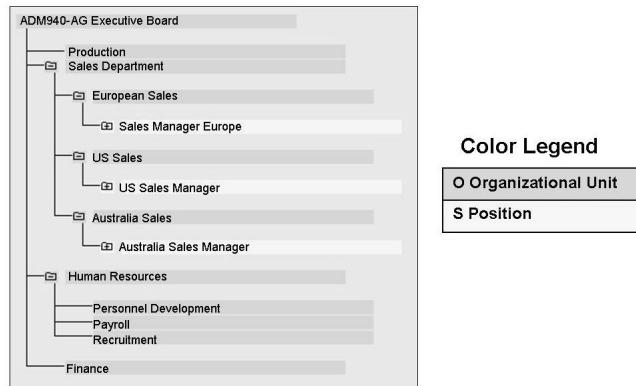


Figure 115: Organizational Plans

Normally, organizational plans are built by linking **objects** of the following **types** with each other:

- **Organizational unit:** This can be, for example, a functional unit in the company (such as Sales and Distribution).
- **Position:** Represents a position in the staff assignments of an organizational unit that is to be occupied by a person (employee), such as Sales Manager Europe.
- **Job:** While positions represent the concrete posts in a company that are to be occupied by holders (such as Sales Manager Europe), jobs are general classifications of functions in a company (such as sales manager) that are to be further specified by assigning properties. Jobs provide job descriptions that are applicable to multiple positions with similar tasks and properties.
- **Task:** Description of an activity that is to be performed within organizational units.

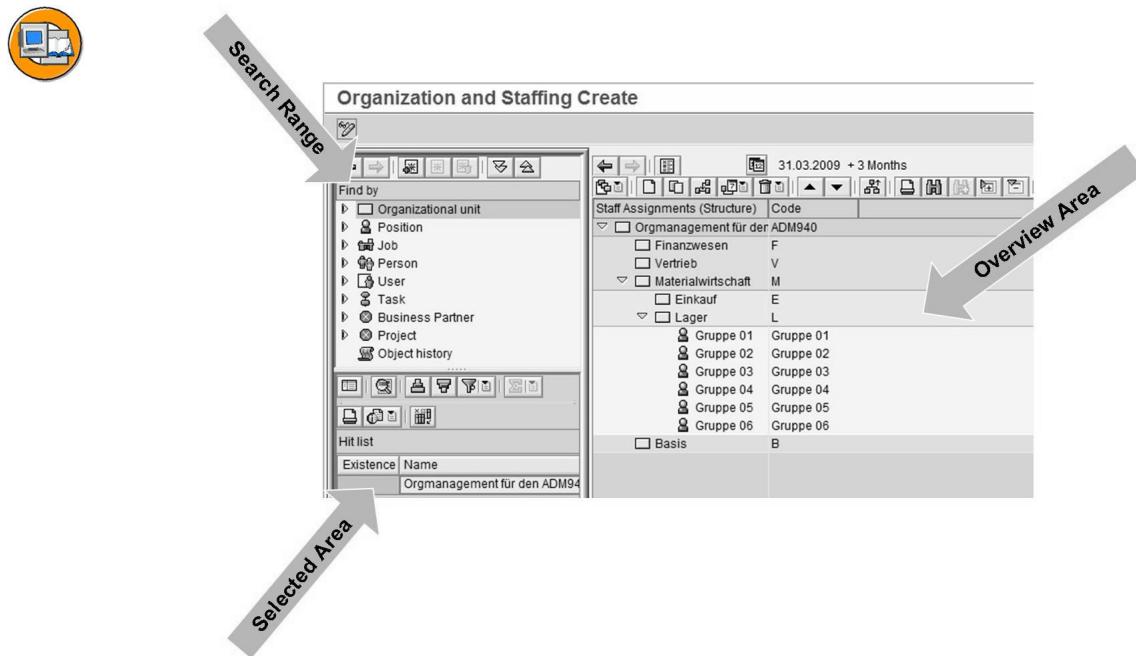


Figure 116: Organization Plan User Interface

By choosing the menu path *SAP Menu → Human Resources → Organizational Management → Organizational Plan → Organization and Staffing*, you have three options for editing organizational plans:

- *Create*, transaction code: “**PPOCE**”,
- *Change*, transaction code: “**PPOME**”,
- *Display*, transaction code: “**PPOSE**”.



Hint: You can, however, still use the **simple maintenance mode** to edit organizational plans (as in previous releases). To switch from the **new maintenance interface** to the **simple maintenance mode**, choose the following menu path: *Settings → Maintenance interface*.

The new user interface consists of several screen areas:

- In the **search area**, you can find one or more objects that you want to display or edit (for example, a complete organizational structure, or all objects of a specific object type, such as all positions).
- The **selection area** lists the objects found. You choose one of these objects:
 - By double-clicking it to display the object and its environment in the overview area and its properties in the detail area
 - By clicking it once to assign it to another object through Drag&Drop, for example, a position to an organizational unit.
- The **overview area** displays the selected object and its environment.

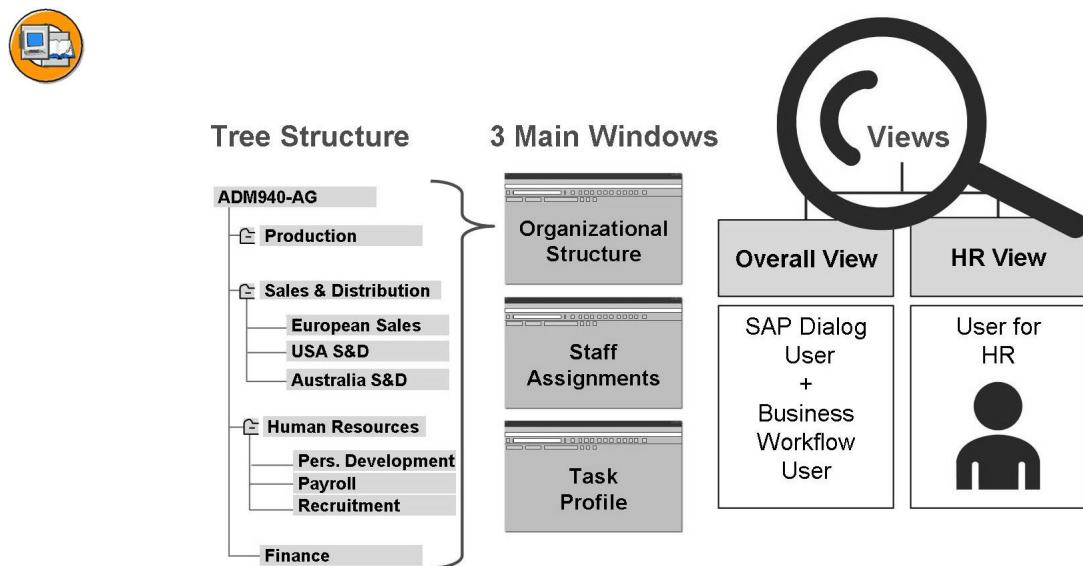


Figure 117: Simple Maintenance of an Organizational Plan

In the **simple maintenance** mode, you can edit organizational plans either in the *Overall view* or in the *Human Resources view*. The *Overall view* provides specific functions for users of the authorization system and SAP Business Workflow. In this view you can, for example, work with roles. The *Human resources view* provides specific functions for HR users.

The simple maintenance method uses a tree structure, which allows you to rapidly put together a basic framework for organizational plans. You use optimized procedures to do this.

You work in three main windows. Each window covers specific maintenance activities:

- The **Organizational Structure** window allows you to build up and maintain the organizational structure for your organizational plan.
- The **Staff Assignments** window allows you to identify the fundamental staffing details required for an organizational plan.
- The **Task Profile** window allows you to assign roles to jobs, positions, organizational units, and holders of positions (users). Workflow Tasks are also assigned at this level, however, these are not related to authorizations.

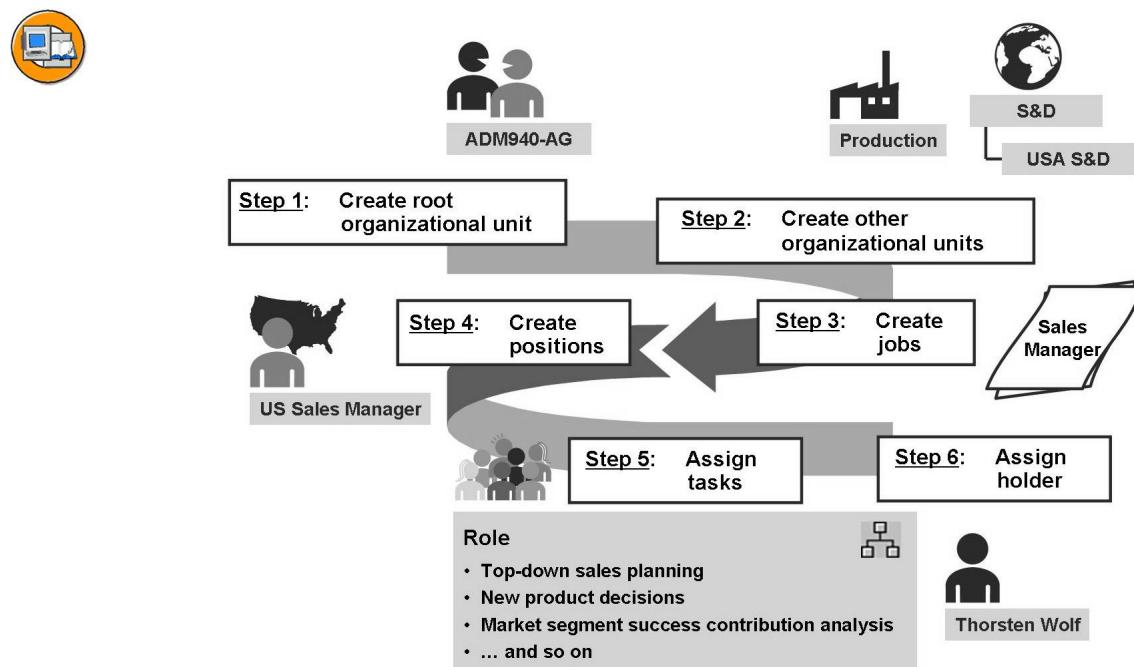


Figure 118: Creating an Organizational Plan in Simple Maintenance

The above figure illustrates that the first step in Simple Maintenance is to create a root organizational unit. All other organizational units are then defined in the organizational structure.

You can define organizational units and jobs in any order you like. However, they should be defined before you define the relevant positions.

Positions are created after the appropriate job(s) are created in the job index.

Holders are assigned to positions, not to jobs.

Having set up the organizational plan, you can assign **roles** to organizational units, jobs, positions, and holders of positions (users).



Executive Board



Organizational Unit Abbreviation	ADM940-AG
Name	ADM940-AG Exec. Board
Validity Period	24.09.2003 to 31.12.9999

Figure 119: Step 1: Defining the Root Organization

When you want to build a new organizational plan, you must first create a root organizational unit. The root organizational unit is the top-level unit of an organizational structure, for example, the executive board. The root organizational unit is also your starting-point for enhancing the organizational structure by adding lower-level units.

The date specified on the initial screen is used as the default for the validity periods of all objects and relationships to be defined.

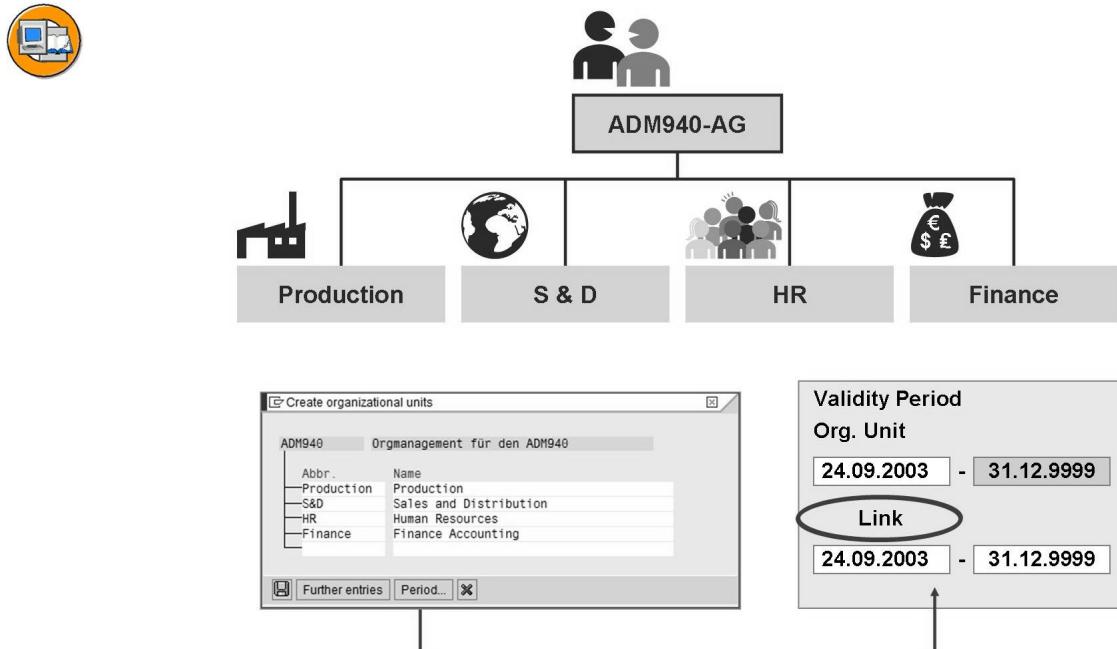


Figure 120: Step 2: Creating Additional Organizational Units

Using the root organizational unit as your starting-point, you create additional lower-level organizational units. In the above example, the Board constitutes the higher-level object, while the organizational units *Production*, *Sales*, *HR* and *Accounting* are lower-level objects.

To create organizational units in simple maintenance, you select the organizational unit under which you want to add new organizational units. The relevant relationship records (A/B 002) between the lower-level and the higher-level organizational unit are automatically created by the system.

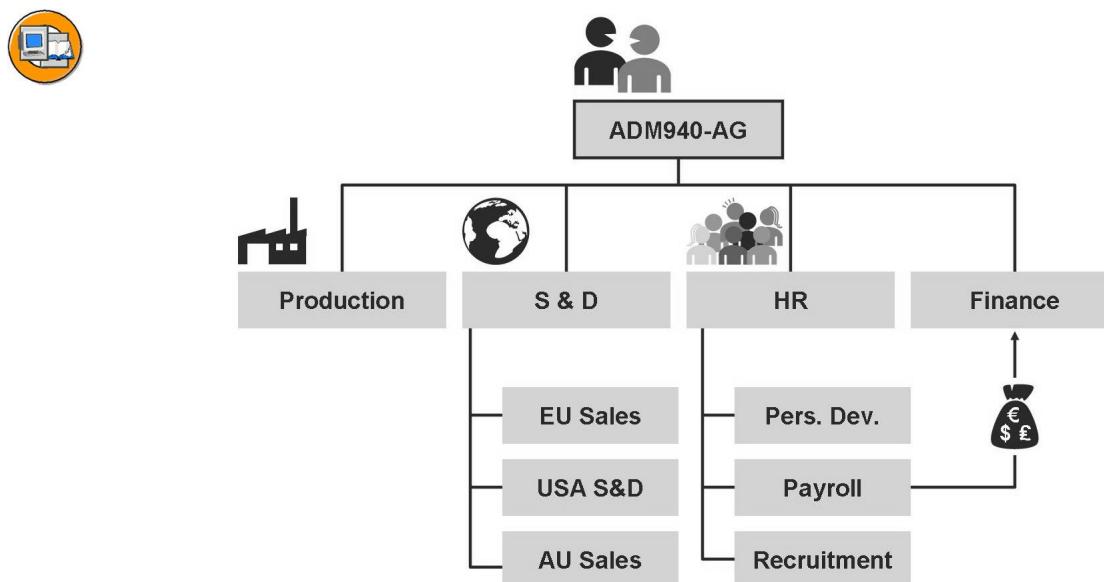


Figure 121: Step 2: Editing the Organizational Structure

To change the hierarchical position of an organizational unit in the organizational structure, you can reassign the relevant unit. If you reassign a unit, the relationships between the organizational units are changed. This means that the current relationship records are automatically delimited and new relationship records are created based on the reassignment process.

To change the short or long text, use the *Rename* function.

Other functions include:

- Deleting objects and relationships
- Delimiting objects and relationships
- Determining the order of the organizational units

If required, you can show or hide other information, for example, the abbreviation, the object period, and the object key.

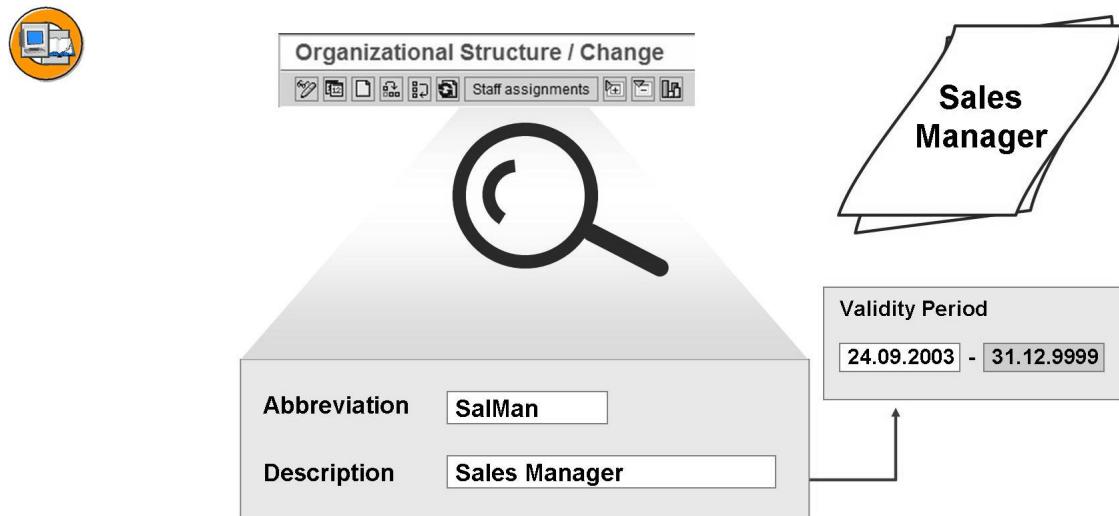


Figure 122: Step 3: Creating Jobs

To create jobs, go to the *Staff Assignments* screen and choose *Edit → Create → Jobs* there.



Figure 123: Step 4: Creating Positions

To create a position in simple maintenance, you select the organizational unit in the staff assignments under which you want to add the new position. The relevant relationship record (A/B 003) between the position and the higher-level organizational unit is automatically created by the system.

As part of the basic concept, you should link each position with a job. As a result, the position automatically inherits the tasks and properties assigned to the describing job, considerably reducing the maintenance effort.

When you create a position in simple maintenance, you can choose a describing job from the job index or directly create a new one. The relevant relationship record (A/B 007) between the describing job and the position is automatically created by the system. By default, the job description is used as the position description.

You can create several positions simultaneously.

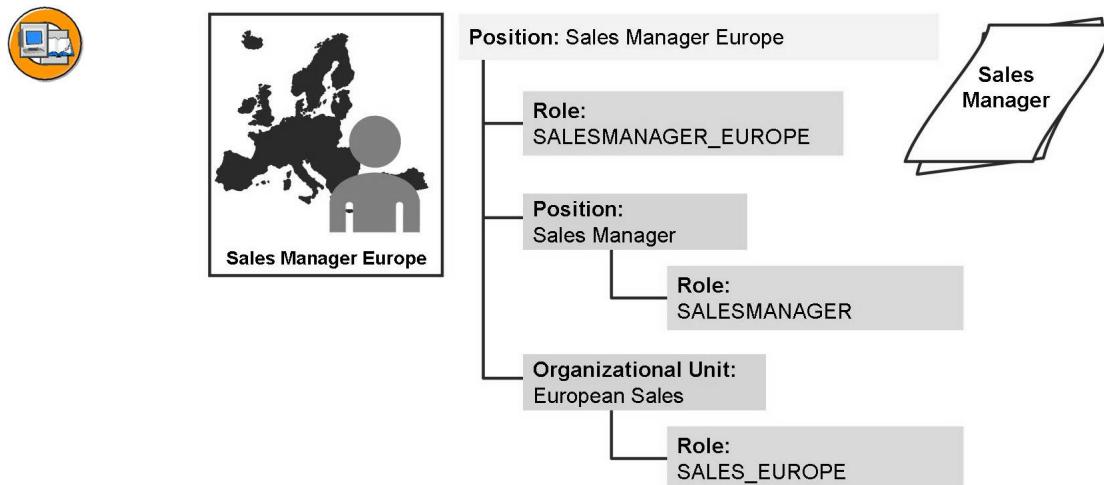


Figure 124: Step 5: Assigning Tasks

A position (such as Sales Manager Europe) can be assigned directly to a role. You can also assign roles using the job (such as sales manager) and/or the organizational unit (such as European Sales). The user assigned to this position then inherits all authorization profiles of these roles.

The user assigned inherits the authorization profiles related to the following:

- **Role: SALESMANAGER_EUROPE**
Through the relationship: Position -> Holder of Position.
- **Role: SALESMANAGER**
Through the relationship: Job -> Position -> Holder of Position.
- **Role: SALES_EUROPE**
Through the relationship: Organizational Unit -> Position -> Holder of Position.

You can also assign roles directly to a user. However, we recommend that you do not do this since you lose the benefits of an assignment using an organizational plan.



Hint: Roles cannot be inherited across organizational units. Positions belonging to an organizational unit cannot inherit the roles assigned to a higher-level organizational unit.

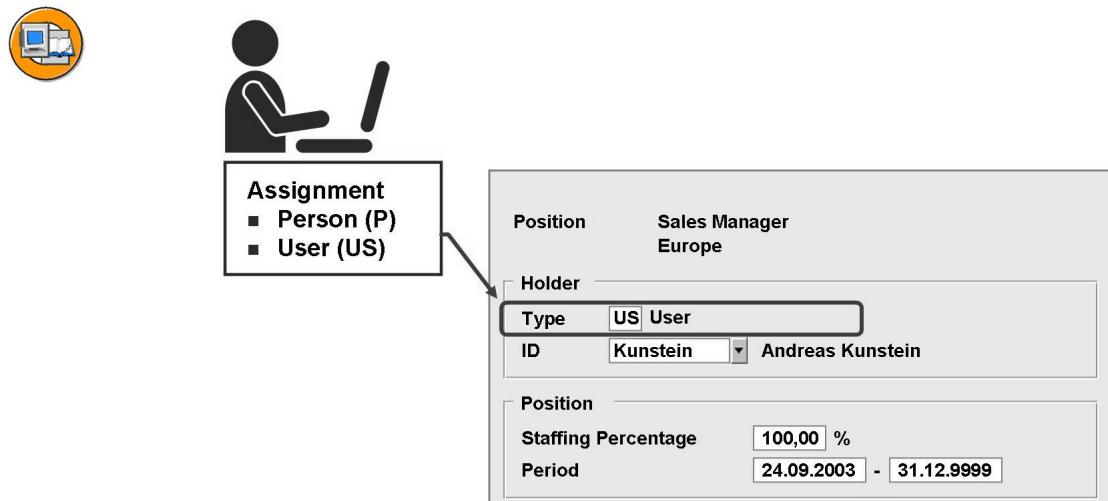


Figure 125: Step 6: Assigning Holder

Positions can be held either by persons or by users.

- Information on the *Person* object type is maintained in the HR master data. Persons are employees of the company.
- Users, on the other hand, are not necessarily employees. Users have authorizations to access the SAP system. They can occupy positions without being registered as an employee. This assignment is of importance in the context of the Workflow.

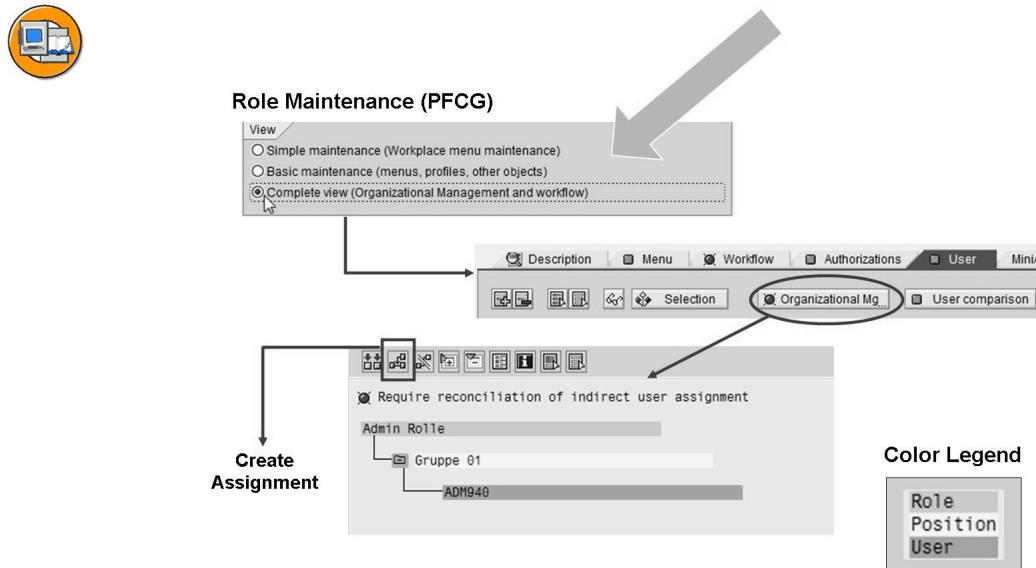


Figure 126: Agent Assignment View (Role)

In order to assign roles to users, you can also use the role maintenance transaction. You can access this using the menu path *SAP Menu → Tools → Administration → User Maintenance → Roles*, or with transaction code “PFCG”.

To be able to assign components of your organizational plan, you must select the “Complete View” when entering the role maintenance transaction (“PFCG”).

By choosing the *Organizational Mgmt* button, you jump to the screen *Role: Change Agent Assignment*. The “Indirect User Assignments” that have already been maintained are displayed here.

Here you can use positions to assign users to a role (such as SALESMANAGER).

By choosing *Create assignment*, you can also define the following relationships:

- Role / Organizational unit
- Role / Position
- Role / User

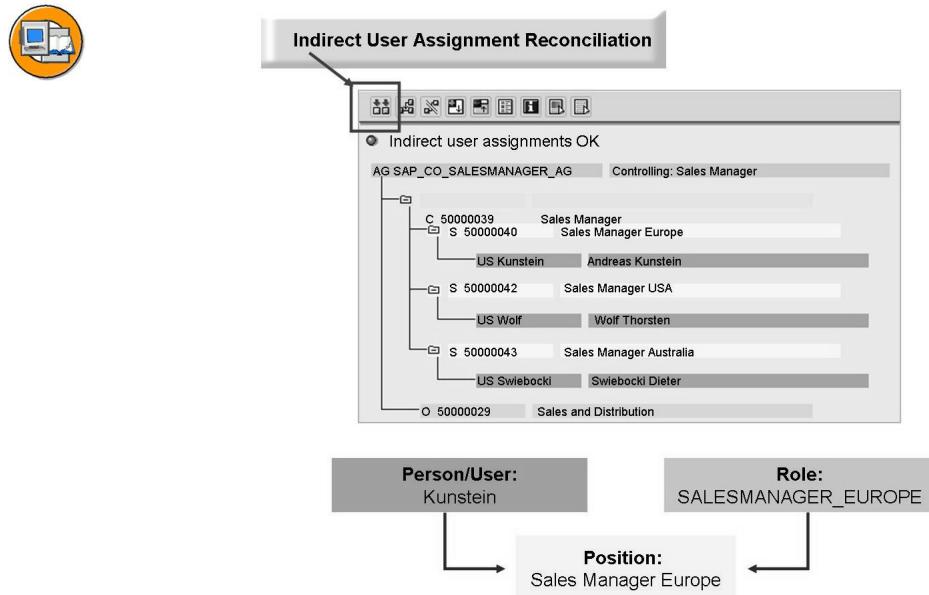


Figure 127: Indirect User Assignment Reconciliation

If you choose the “Indirect user assignment reconciliation” button, the system reconciles the positions and the users assigned. Users that were added newly are entered, and user assignments that are no longer current are deleted.

During the reconciliation process, the users assigned on the basis of positions are entered as *indirect user assignments* for the role.

Since assignments in Organizational Management are time-dependent, you must take this restricted validity into account when you assign users. During the reconciliation process, the relationship period from Organizational Management is copied for the indirect user assignments.

If you perform a user master comparison (see next figure), the *indirect user assignment* is automatically reconciled. The same applies when running the report *PFCG_TIME_DEPENDENCY*.

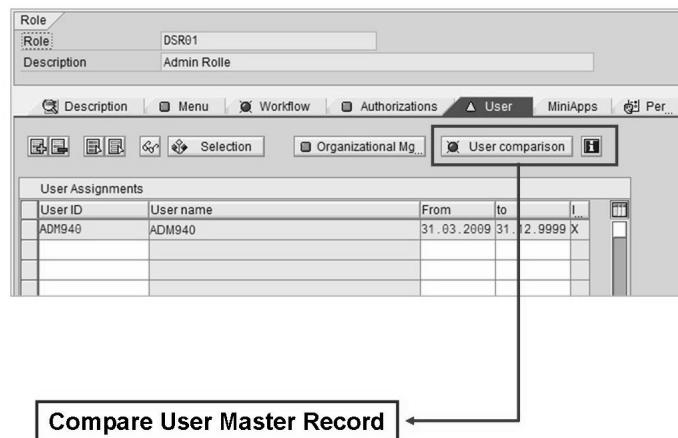


Figure 128: User master record comparison

If you change the users assigned to the role or generate an authorization profile, you must compare the user masters (*User Comparison* button). The system compares the authorization profiles with the user master records. This means that profiles that are no longer current are removed from the user master records, and the current profiles are entered in the user master records.

Exercise 13: Integration into Organizational Management

Exercise Objectives

After completing this exercise, you will be able to:

- Display organizational units in HR Organizational Management
- Link roles and users with HR organizational units
- Reconcile the relationships

Business Example

This exercise runs through the assignment of authorizations through the integration of Organizational Management. Only the last stages of the indirect user and role reconciliation are performed; the system settings required for this integration are not part of this exercise.

Task 1:

A composite role and a user are to be assigned to the previously created organizational plan *ADM940*. The indirect relationships are then to be displayed and reconciled, so that the user receives the appropriate authorizations.

1. Navigate in the SAP menu to Organizational Management and there, in expert mode, to the “simple maintenance”. Display the organizational plan *ADM940*.



Hint: SAP Menu: Human Resources → Organizational Management → Expert Mode → Simple Maintenance → Change.

2. Go to the Staff assignments window. Select the root node and display the structural graphics.
3. Expand everything under the *Materials Management* node. Place the cursor on the group ## position, and assign the holder GR##-MM2 of type US to the position.
4. Select the group ## position and choose *Task Profile*. Link the position with the composite role GR33_MM_WHOUSR (from the exercise in the lesson *Working with the Role Maintenance Part 2*).

Continued on next page

Task 2:

Perform a direct reconciliation.

1. Change your composite role GR##_MM_WHOUSE.



Hint: Caution: Choose Complete View on the initial screen of the function.

2. Go to the User tab page.

Is the user from exercise 1-3 assigned to your role?

3. Go to Organizational Management by choosing the *Organizational Management* entry in the *Goto* menu (or by clicking the appropriate button).

Reconcile the indirect user assignments of the role.

4. Go back.

Is the user from exercise 1-3 assigned to your role?

What is the traffic light status of the Organizational Management area?

Display the user master record of user GR##-MM2.

Go to the *Roles* tab page.

How many roles are there?

How many profiles are entered?

5. Change your composite role GR##_MM_WHOUSE.

Perform a complete user compare.

Display the user master record of user GR##-MM2 again.

How many roles are there now?

And how many profiles?

Solution 13: Integration into Organizational Management

Task 1:

A composite role and a user are to be assigned to the previously created organizational plan *ADM940*. The indirect relationships are then to be displayed and reconciled, so that the user receives the appropriate authorizations.

1. Navigate in the SAP menu to Organizational Management and there, in expert mode, to the “simple maintenance”. Display the organizational plan *ADM940*.



Hint: SAP Menu: Human Resources → Organizational Management → Expert Mode → Simple Maintenance → Change.

a)



Hint: This menu path leads to the **old** simple maintenance, transaction code “PPOM_OLD”. The lesson also described why this old maintenance transaction is used, and not the new transaction. Brief recap: Since this lesson deals only with the possibilities for assigning authorizations using Organizational Management, we have forgone the new maintenance interface. With this interface, a few more steps would be required than with the simple maintenance, and these would go beyond the scope of the exercise. This deals only with the possibility of assigning authorizations.

2. Go to the Staff assignments window. Select the root node and display the structural graphics.
 - a) Go to the staff assignments window by choosing the appropriate button. Select the root node and display the structural graphics by choosing the relevant button.
3. Expand everything under the *Materials Management* node. Place the cursor on the group ## position, and assign the holder GR##-MM2 of type US to the position.
 - a) Expand everything under the *Materials Management* node. Place the cursor on the group ## position (this is under the *Warehouse*) and assign the holder GR##-MM2 of type US to the position (choose the *Assign holder* button).

Continued on next page

4. Select the group ## position and choose *Task Profile*. Link the position with the composite role GR33_MM_WHOUSR (from the exercise in the lesson *Working with the Role Maintenance Part 2*).
 - a) Select the group ## position and choose the *Task Profile* button. Link the position with the composite role GR##_MM_WHOUSE (from the exercise for the lesson *Working with the Role Maintenance Part 2*), by placing the cursor on the group ## position and choosing the *Role* button.

Task 2:

Perform a direct reconciliation.

1. Change your composite role GR##_MM_WHOUSE.



Hint: Caution: Choose Complete View on the initial screen of the function.

- a) **SAP Menu:** *Tools* → *Administration* → *User Maintenance* → *Role Administration* → *Roles*, (transaction code “PFCG”).
2. Go to the User tab page.
Is the user from exercise 1-3 assigned to your role?

a) No.
3. Go to Organizational Management by choosing the *Organizational Management* entry in the *Goto* menu (or by clicking the appropriate button).
Reconcile the indirect user assignments of the role.
 - a) Go to Organizational Management by choosing the *Organizational Management* entry in the *Goto* menu (or by clicking the appropriate button).

Reconcile the indirect user assignments of the role by choosing the icon *Indirect user assignment reconciliation*. The status icon then changes from *Red* to *Green*.
4. Go back.
Is the user from exercise 1-3 assigned to your role?

What is the traffic light status of the Organizational Management area?

Continued on next page

Display the user master record of user GR##-MM2.

Go to the *Roles* tab page.

How many roles are there?

How many profiles are entered?

-
- a) Yes.
 - b) green.
 - c) **SAP Menu:** Tools → Administration → User Maintenance → Users, (transaction code “SU01”).
1 (3) roles (*)
 - d) 0 (2) profile(s) (*)



Hint: (*) What does the number in parentheses mean?

This number can vary depending on whether you have performed all optional tasks from the ADM940 course (the roles GR##_BC_PORTALS and ADM940_PLUS may be missing).

5. Change your composite role GR##_MM_WHOUSE.

Perform a complete user compare.

Display the user master record of user GR##-MM2 again.

How many roles are there now?

And how many profiles?

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

SAP Menu: Tools → Administration → User Maintenance → Users, (transaction code “SU01”).

3 (5) roles; what does (*) mean? → last solution.

- b) 2 (4) profile(s); what does (*) mean? → last solution but one.



Lesson Summary

You should now be able to:

- Create organizational units in HR Organizational Management
- Link roles with the organizational plan objects
- Link users with the organizational plan objects
- Perform a comparison of the indirect role and user assignments
- Compare user master record
- Assign roles for a specific period of time

Lesson: SAP NetWeaver Identity Management

Lesson Overview

SAP NetWeaver Identity Management provides the functions and services needed to integrate distributed identity data in the system landscape for efficient, heterogeneous identity lifecycle management.



Lesson Objectives

After completing this lesson, you will be able to:

- understand what SAP NetWeaver Identity Management is
- estimate the effort switching from CUA to SAP NetWeaver Identity Management

Business Example

Today identity management is becoming a key challenge as your organization needs to ensure that users have the right access to applications in a timely manner while ensuring the security of your organization's data. The SAP NetWeaver Identity Management component helps you address those challenges and align identity management with your organization's key business processes.

SAP NetWeaver Identity Management Features

You use the central user administration (CUA) tool to manage users across multiple SAP software systems that are based on the ABAP programming language. Moving to the SAP NetWeaver Identity Management component from CUA provides the following advantages:



- **Identity virtualization** – Gain an integrated, unified view of the virtual identity of users, as well as identity services to leverage identity information and access rights across networks
- **Data synchronization** – Transform and propagate changed user and identity information to other related applications to maintain data consistency and quality
- **Provisioning, workflow, and approvals** – Assign and maintain user access rights across multiple systems, as well as provision employees and business partners; audit all changes
- **Password management** – Provide password self-service functionality and password synchronization across all connected target systems
- **Roles and entitlements** – Align roles with business processes rather than technical directory structures
- **Reporting and auditing** – Produce reports based on current access and past events

SAP NetWeaver Identity Management supports LDAP directories and databases, as well as standards such as SPML and DSML.

Example: Provisioning

One of the main problems of identity management is the manual maintenance of the identity data of most applications. A provisioning system will automate this process by defining users in the applications based on a central repository (the identity store). Normally the authoritative source to determine whether a person should exist in the identity store is the HR system, as this is also responsible for authorizing salary payment for the employee. Often the HR system also contains information such as the e-mail address and phone number, but this information is in many cases not maintained after the first registration of the employee. The e-mail system must know the e-mail address of the employee to deliver the e-mail and is thus the authoritative source of e-mail addresses. If an electronic telephone switchboard is deployed, this may be queried for the telephone numbers. Customers may be provisioned from a completely different set of business applications.



Role Definition (design, one-time task)

- Read system access information (roles, groups, authorizations, etc.) from target systems
- Define a business role hierarchy
- Assign technical roles to business roles
- Develop rules for role assignments

Provisioning (regularly)

- Assign or remove roles to/from people
 - Through request approval workflow
 - Manually (administrator)
 - Automatically e.g. HR-driven
- Automatic adjustment of master data and assignments of technical authorizations in target systems

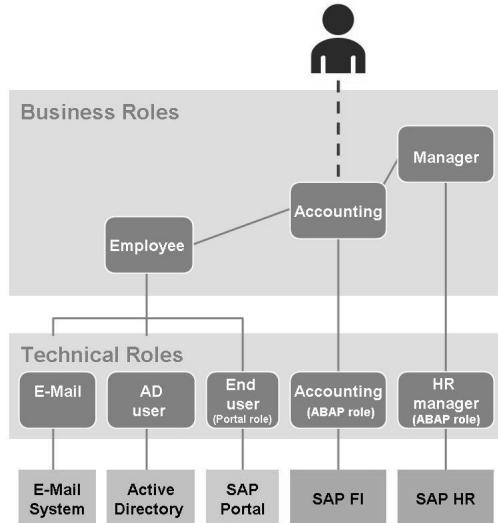


Figure 129: Role Definition and Provisioning

The provisioning solution will, based on information from the authoritative systems, automatically create the user in the required repositories, and provide the necessary access rights. And even more important, when a user leaves the organization the accounts are disabled, and access rights are revoked. Similarly when a user moves between departments, access rights are granted and revoked accordingly. It will now also be easier to have an overview of all the employees within the organization, and of the applications in which the employees are defined. Provisioning can be used for handling much more than employees joining and leaving the organization.

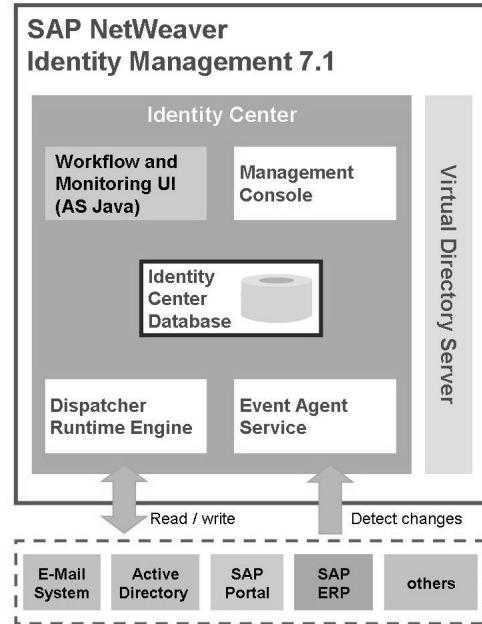
In a project-based organization, the provisioning system can be engineered to create the necessary accounts and project web space automatically when a new project is started. It can also make sure the project members have access to the project archive, and create e-mail lists of the people involved. It can be used to start a workflow that equips traveling salespersons with a mobile phone, a laptop computer, and remote access to the company network and web resources. Some of these provisioning tasks are in themselves workflows with ordered and dependent sub-tasks. If the workflow fails, it may be necessary to roll back tasks that had previously been completed successfully. This requires a high degree of sophistication in the chosen provisioning solution.

Architecture of SAP NetWeaver Identity Management

SAP NetWeaver Identity Management 7.1 consists of the following components:

**IC database**

- Core of the IC product
- Tables, stored procedures and triggers
- Holds
 - jobs
 - logs
 - audit data
 - delta information
 - status
 - scheduling
- Identity Store
 - Dynamic storage of identity data
 - Rendezvous point for all identities

**Figure 130: Identity Center Database**

The **Identity Center** is the primary component used for identity management. The Identity Center includes functions for identity provisioning, workflow, password management, logging, and reporting. It uses the **Identity Center Database** with the **Identity Store**, to provide a uniformed view of the data, regardless of the data's original source. The Identity Center retrieves the data from these various repositories, consolidates it, transforms it into the necessary formats, and publishes it back to the various decentralized repositories.

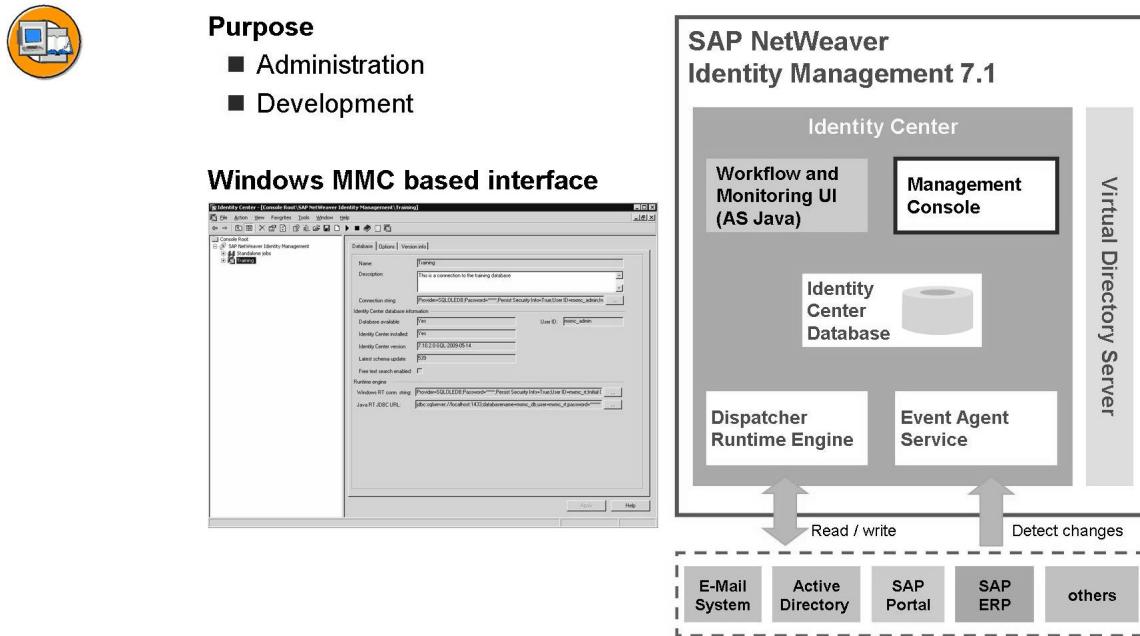


Figure 131: Management Console

The administrator manages the Identity Center configuration through the Management Console. Besides the managing functions, the Management Console offers monitoring and analysis functionality like the dispatcher status, job log, job status and system log. To get an overview of the Identity Center database, there is a system diagnostics report available in the Management Console as a job template.

**Purpose**

- Evaluate container-tasks
- Starts runtime engine when tasks and jobs are to be executed

Runs as a service on each machine executing jobs

Runtime engine

- Responsible for doing the work
- Advanced version of the runtime
- Same basics
- Windows/Java

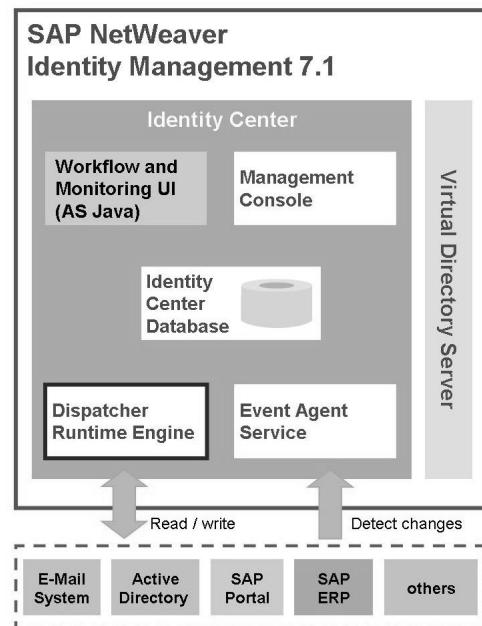


Figure 132: Dispatcher Runtime Engine

The Dispatcher(s) are connected to the Identity Center database and check for jobs that are ready to be run. A dispatcher is running on each computer where a Runtime engine is installed. The dispatcher is responsible for starting the runtime engine when a job is ready for execution, as well as performing some basic provisioning logic.



Purpose

- Reduce data transfer latency

Detects changes in repositories

- Database triggers
- LDAP change log
- Java object

Schedules jobs for execution

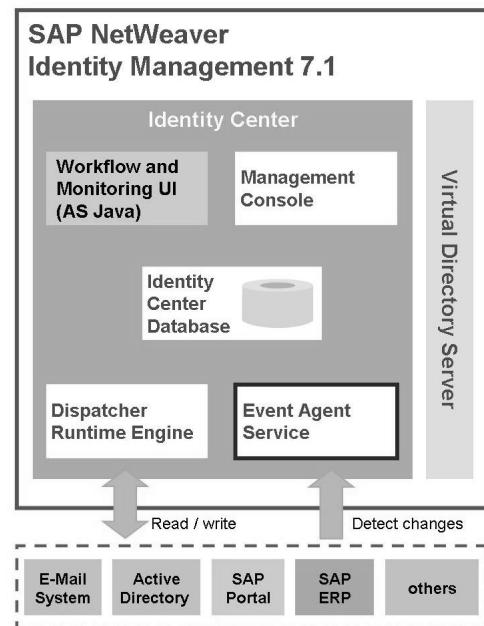


Figure 133: Event Agent

Event agents can be configured to take action based on changes in different types of repositories such as directory servers, message queues, or others. This mechanism is optional and its only purpose is to initiate synchronization based on changes in repositories in addition to the scheduled operations.



Identity Management UI

- Main workflow interface for users and managers
 - Web interface for registration and approvals
 - Self-service interface
 - Password reset
- Monitoring and audit interface for administrators
 - Logs
 - Queues
- Based upon Web Dynpro Java

SAP NetWeaver Identity Management 7.1

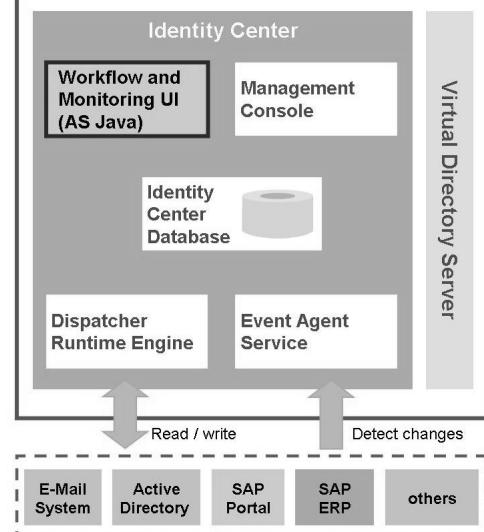


Figure 134: Identity Management User Interface

The Identity Management User Interface is available as a standalone Webdynpro application as well as a Portal integration application. It is a workflow interface that is used for listing web-enabled tasks, for example Self-service, delegated service, password-management, and approvals.

The **Virtual Directory Server** is a component provided by SAP NetWeaver Identity Management that acts as a single access point for clients retrieving or updating data in multiple data repositories, as it provides a uniformed view of the data in real-time. It also takes care of access control among other tasks. The virtual directory itself has no data storage, but contains knowledge about the location and format of data stored elsewhere. Sometimes the source data may be spread over different systems and platforms. In effect it transforms the incoming LDAP requests either to LDAP requests to other directory servers or to SQL statements sent to one or several relational databases.

The Identity Management User Interface

- „Self Services“ tab: All Self Service tasks (= tasks which operate on someone's own entry) and administrative tasks (= tasks which do not operate on any specific entry) will be listed here. A descriptive text can be edited.
Prerequisite: synchronization of the users between Identity Store and user store of the AS Java
- „To Do“ tab: Display pending tasks for example requests waiting for approval by the logged in user. You can view pending tasks with the Universal Worklist (UWL) of the NetWeaver Portal, too
- „Manage“ tab: Search and advanced search for objects of a selected entry type Displaying details on the selected entry in the search result table Execute other delegated tasks on the selected entry
- „History“ tab: The user can search for tasks executed in the past (“Manage”, “Self-Service”), and check the outcome. Either tasks initiated by her/himself or tasks executed upon her/him by another user (“Approvals”)
- „Monitoring“ tab: Monitoring of approval queue, dispatcher status, job log, job status, provision audit, provision queue, system log

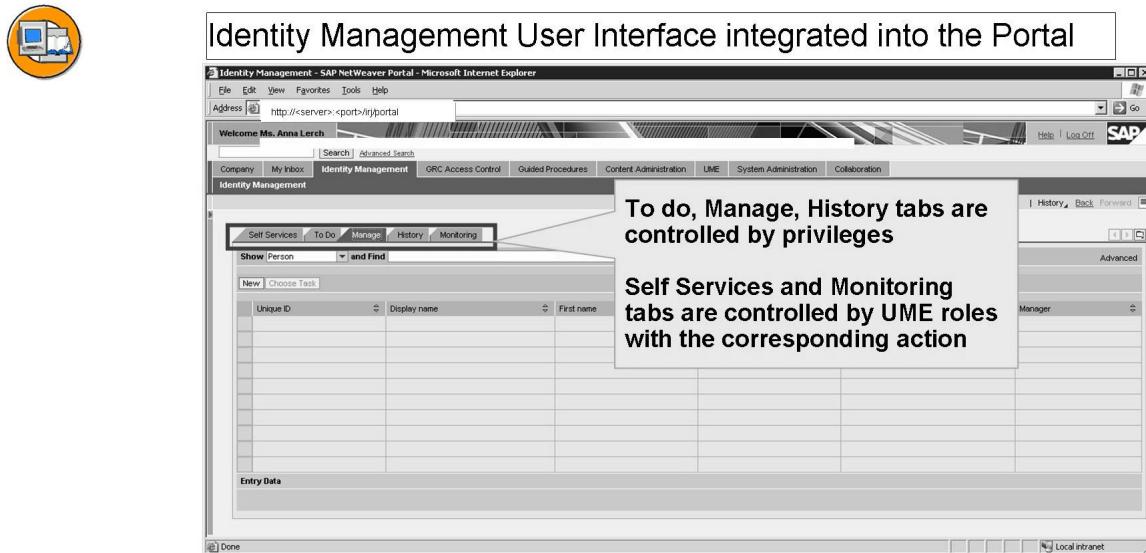


Figure 135: UI Portal Integration

Migration to SAP NetWeaver Identity Management

As of Release 7.0 SPS 2, SAP NetWeaver Identity Management supports the integration of a central user administration (CUA) system. In this case, connect the CUA central system to the Identity Center as a target system in the same way as any other ABAP-based SAP system. The Identity Center provisions the identity data to the CUA central system, which in turn provisions the data to its child systems. This model works regardless of what system is used as the leading system for the identity management landscape.

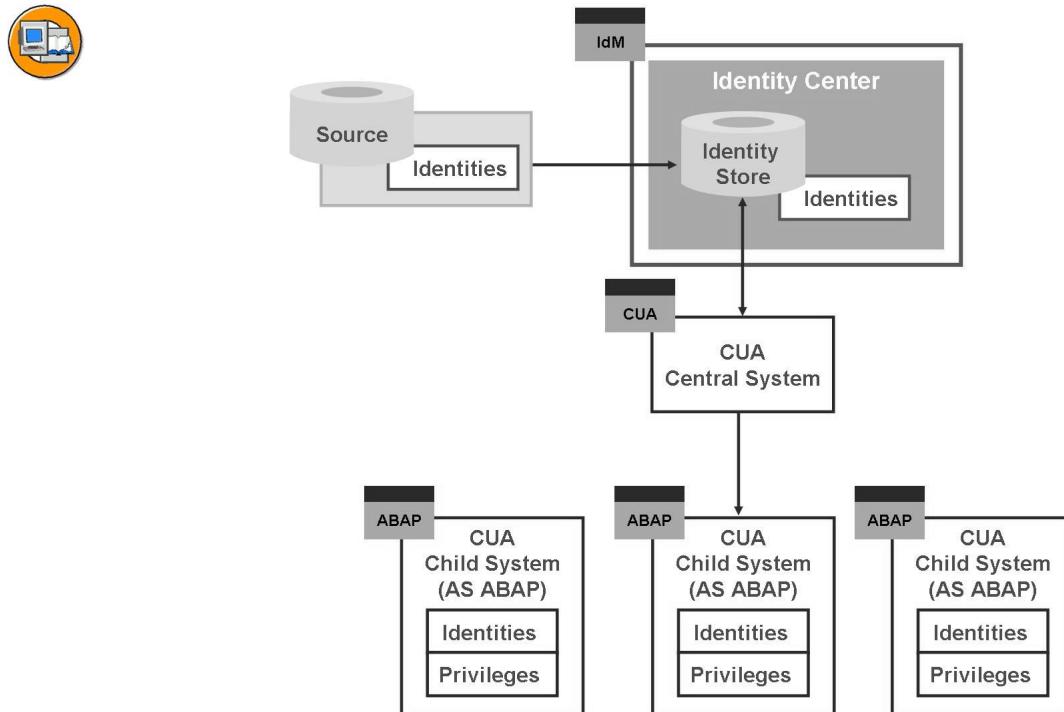


Figure 136: Integrating a Central User Administration System

This allows for a smooth installation of SAP NetWeaver Identity Management into an existing CUA landscape without any modifications, and at the same time, provides support for additional AS Java or other third-party systems. You can also continue with migration steps to remove the child systems from the CUA landscape and connect them directly to SAP NetWeaver Identity Management.

Installation of SAP NetWeaver Identity Management 7.1

To install SAP NetWeaver Identity Management 7.1, the following installation steps have to be performed:



- Installing the Management Console and Runtime Components
- Installing the Identity Center Database
- Installing Workflow
- Installing Monitoring
- Installing the Virtual Directory Server

For detailed information on the installation steps see the Support Portal
<http://service.sap.com> → *Release & Upgrade-Info* → *Installation and Upgrade Guides* → *SAP NetWeaver Identity Management 7.1*.



Lesson Summary

You should now be able to:

- understand what SAP NetWeaver Identity Management is
- estimate the effort switching from CUA to SAP NetWeaver Identity Management

Related Information

- http://help.sap.com/saphelp_nwidmic71/en/dse.htm
- To learn more about SAP NetWeaver Identity Management, participate in the classroom training TZNWIM.



Unit Summary

You should now be able to:

- Explain how the central user administration functions
- Specify the most important steps for setting up the central user administration
- Define distribution rules for user data
- Create, maintain and distribute users centrally
- Perform system comparisons for users that are not yet maintained centrally
- Create organizational units in HR Organizational Management
- Link roles with the organizational plan objects
- Link users with the organizational plan objects
- Perform a comparison of the indirect role and user assignments
- Compare user master record
- Assign roles for a specific period of time
- understand what SAP NetWeaver Identity Management is
- estimate the effort switching from CUA to SAP NetWeaver Identity Management



Test Your Knowledge

1. What is Central User Administration used for?

Choose the correct answer(s).

- 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



Answers

1. What is Central User Administration used for?

Answer: C

For answer A) CUA does not cover central password administration in SAP systems.

For B) Printer landscapes are not maintained with CUA.

For C) CUA is used to administer user master records.

For D) No profiles are created centrally with CUA.



Course Summary

You should now be able to:

- List the elements and objects of the authorization concept
- Explain the use and purpose of the Role Maintenance
- Analyze authorizations
- Describe special objects for administrators

Appendix 1

SAP Notes About Authorizations

Finally, a number of SAP Notes on the topic of authorizations are listed below. You should also use the SAP Internet pages to keep yourself informed, as changes could take place at any time. The following list is only intended to support you in finding out about various topics.

The structure is <SAP Note number><Text/description>

Release-Dependent

SAP Note Number	Text/Description
7642	Authorization protection of ABAP/4 programs
16466	Customer Namespace for SAP Objects
66687	Use of Network Security Products
169469	List of all activity groups with a manual S_TCODE
68048	Deactivating the Automatic User SAP*
82390	Generating Profile SAP_ALL
156250	Responsibilities Replaced as of Release 4.5A
198598	Profiles and References in Roles as of Release 4.6B
156196	Activity Groups Renamed as of Release 4.5A
80210	Profile Generator: Documentation
91721	Problem with org. levels in Profile Generator

SAP Note Number	Text/Description
323817	Creating organizational level fields for Profile Generator
314513	Org. level in Profile Generator
85234	Missing authorization when using Profile Generator
313587	Mass deletion of Activity Groups
203994	Changed behavior: User menus in 4.6
301344	Performance problems during menu editing in PFCG
167466	IMG authorizations with Profile Generator in 4.5
184906	Renaming users: Activity groups are missing
355364	SU01 Role assignment: Changing validity period impossible
203617	High memory consumption with Easy Access Menu
66056	Authorization trace with Transaction ST01
205771	Migration of report trees in area menus
193251	Customer enhancements in area menus
65968	ABAP/4 Debugging authorizations as of Release 3.1G
314843	Authorization object S_TABU_LIN
67766	S_TCODE: Authorization check on start transaction
142724	Prevention of multiple dialog logons
159885	CUA: Collective Note for Central User Administration
171316	PFCG/SU03: F4 help for authorization values

Release Independent

SAP Note Number	Text/Description
31395	System parameters: Defined where? Displayed how? Docu?
39267	Availability of the SAP Security Guide
30724	Data protection and Security in R/3
23611	Collective Note: Security in SAP Products
20534	Authorization Check – A Short Introduction
20643	Naming Conventions for Authorizations
28175	Questions Regarding the Authorization Concept
2467	Password Rules and Preventing Unauthorized Logons
12466	Logon Restrictions in R/3
28186	What Does the Profile SAP_NEW Do?
29276	SAPCPIC: At which points are passwords visible
2383	Documentation: Description of "super user" SAP*
113290	PFCG: Merge process when maintaining authorization data
77503	Audit Information System (AIS)
139418	Logging user actions
179145	Authorization checks for numeric values
23342	You are not authorized to ... Analysis
15253	Authorization check during transaction start
303468	Global User Manager: Frequently Asked Questions
93769	Additional Documentation Regarding the Authorization Concept – Documentation on Profile Generator (Authorization made easy for Releases 3.0F, 3.1G and 3.1H, 4.0B)

Appendix 2

Glossary

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.

ALE

Application Link Enabling

APO

Advanced Planning and Optimization

AUTH_DISPLAY_OBJECTS

Display active authorization objects

AUTH_SWITCH_OBJECTS

Switch on/off authorizations

authorization

Each 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 field

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 object

Authorization objects allow 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 object class

Authorization classes are the organizational grouping of authorization objects.

authorization profile

Grouping 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.

BD64

Distribution model maintenance

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.

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.

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.

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.

ITS

Internet Transaction Server

PFCG

Role maintenance

PFUD

User master data reconciliation

PPOC

Create organizational plan

PPOCE

Create organization and staffing

PPOM

Maintain organizational plan

PPOM_OLD

Create organizational plan (old)

PPOME

Change organization and staffing

RFC

Remote Function Call

Role Maintenance

Tool for generating authorization profiles in role maintenance. You use the Role Maintenance to generate an authorization profile based on the activities in a role.

RTTREE_MIGRATION

Report tree migration

RZ10

Maintain profile parameters

RZ11

Maintain profile parameters

SA38

ABAP/4 Reporting

SALE

Display ALE Customizing

SAP Easy Access

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.

SARP

Execute reporting (tree structure)

SBWP

SAP Business Workplace

SCC4

Client administration

SCC8

Client export

SCC9

Remote client copy

SCCL

Local client copy

SCUA

Central user administration

SCUG

Transfer users

SCUL

Central user administration log

SCUM

Central user administration

SE16

Data Browser

SE43

Area menu maintenance

SE93

Maintain transaction codes

SM30

Call view maintenance

SM36

Schedule background job

SM37

Overview of job selection

SPRO

Customizing project editing

SPRO_ADMIN

Customizing project management

SSM2

Set initial area menu

ST01

System trace

SU01

User maintenance

SU10

User mass maintenance

SU20

Maintain authorization fields

SU21

Authorization object maintenance

SU24

Authorization object check under transactions

SU25

Upgrade tool for the Role Maintenance

SU3

Maintain user's own data

SUIM

User Information System

TMS

Transport Management System

user buffer

Buffer from which the data of a user master record is loaded when a user logs on.

UTC

Universal Time Coordinated

Index

A

Access Control, 6
Audit Information System (AIS), 257
auth/no_check_in_some_cases, 192
authorization, 43
authorization checks
 at transaction start, 64
 in programs, 65
authorization concept
 decentralization of user administration, 231
 implementation method, 12
 principle of dual control, 234
 principle of treble control, 235
 step 1: preparation, 15
 step 2: analysis & conception, 17
 step 3: implementation, 23
 step 4: quality assurance & tests, 24
 step 5: cutover, 25
 strategy for user and authorization administration, 26
authorization error analysis, 251
 transaction code: ST01, 254
 transaction code: SU53, 252
authorization field, 43
authorization object, 43
 S_PROGRAM, 227

S_TABU_CLI, 225
S_TABU_DIS, 223
S_TABU_LIN, 226
S_TCODE, 222
S_USER_AGR, 229
S_USER_AUT, 230
S_USER_GRP, 228
S_USER_PRO, 230
S_USER_SYS, 228
S_USER_TCD, 229
S_USER_VAL, 229
authorization object class, 43
authorization profile, 43

C

Central User Administration (CUA), 289
central user maintenance (transaction code: SU01), 299
copying user master records (transaction code: SCUG), 298
distribution of field attributes (transaction code: SCUM), 296
graphical model, 291
integration into existing systems, 297
Check with default
 No, 196
 Yes, 196
Check with default to be set -
 Yes or No, 196
composite role, 145
Customizing role, 144

D

decentralizing user administration, 231

- Derived role, 150
Do not check with default -
No, 195
- E**
error analysis, 251
- G**
general password rules and
profile parameters, 215
- I**
indirect role assignment, 307
Information System, 256
Information System: AIS, 257
information systems for
administrators and audit,
255
- O**
organizational management,
307
organizational plan, 307
 assigning jobs, 315
 assigning organizational
 units, 314
 assigning positions, 315
 assigning tasks, 316
 assigning users/persons,
 317
 basic structure, 308
 create root organizational
 unit, 313
 reconcile indirect user
 assignment, 319
 user master comparison,
 320
- P**
pfcg_time_dependency (user
master comparison), 122
Principle of dual control, 234
Principle of treble control
(example 1), 235
Principle of treble control
(example 2), 236
- profile parameters for
password and logon rules,
216
- R**
reference role, 150
Role Maintenance
 status texts for
 authorization
 maintenance, 177
- Role Maintenance
 basic setting: default
 values, 193
 basic setting: parameter,
 192
 basic settings, 191
 central tool for creating
 roles [PFCG], 108
 compare user master
 record, 123
 generate authorization
 profile, 120
 icon legend, 174
 manual insertion of
 authorizations, 119
 the yellow traffic light
 problem, 177
 traffic light legend, 173
 upgrade, 197
 views (maintenance
 options for roles), 111
- Role Maintenance default
values
 green, 193
 not maintained, 193
 red, 193
 yellow, 193
- Role Maintenance tab page
 Authorizations, 117
 Description, 112
 Menu, 114
 User, 121
- role types
 composite role, 145
 Customizing role, 144
 reference (root) roles and
 derived roles, 150

- single role, 112
 - role-based authorization
 - concept, 7
 - root role, 150
- S**
- sample authorization concept
 - job role, 36
 - role distribution, 38
 - SAP* special user, 221
 - single role, 112
 - special users in SAP systems, 219
 - status texts for authorization maintenance
 - changed, 177
 - inactive/reactivate, 176
 - maintained, 177
 - new, 178
 - old, 178
 - standard, 177
 - System Access Control, 6
- T**
- table usage
 - SSM_CUST, 149
 - TACT, 44
 - TACTZ, 45
 - TSTCA, 64
 - USOBT, 194
 - USOBT_C, 194
 - USOBT_C → upgrade, 200
 - USOBX, 194
 - USOBX_C, 194
 - USOBX_C → upgrade, 200
 - USR40, 215
 - traffic light legend
 - green, 173
 - red, 173
 - yellow, 173
 - transport of
 - authorization components, 272
 - customer check indicators, 277
- roles with CUA, 276
 - roles with upload and download, 276
 - roles without CUA, 274
 - user master records, 273
- U**
- upgrade
 - adjust default tables, 200
 - Upgrade
 - convert manually created profiles, 199
 - Role Maintenance already used, 200
 - Role Maintenance not yet used, 198
 - using the profile: SAP_NEW, 203
 - user administration
 - principle of dual control, 234
 - principle of treble control, 235
 - user and role menu
 - display in SAP Easy Access, 48
 - structure, 47
 - user buffer, 66
 - user data
 - change documents, 90
 - individual maintenance [SU01], 77
 - mass maintenance [SU10], 90
 - User Information System, 255
 - user master record tab page
 - address, 78
 - defaults, 83
 - groups, 87
 - license data, 88
 - logon data, 79
 - parameters, 84
 - personalization, 88
 - profiles, 86
 - roles, 85
 - SNC, 82
 - user type

communication, 81
dialog, 81
reference, 82

service, 81
system, 81

Feedback

SAP AG has made every effort in the preparation of this course to ensure the accuracy and completeness of the materials. If you have any corrections or suggestions for improvement, please record them in the appropriate place in the course evaluation.