

SAP BASIS Introductory Training Program

DAY 7

July 2018

TRAINING

Day 7: Agenda

User Master and Authorization Object – As ABAP

Break

Role Management – AS ABAP

Lunch Break

User Information and Troubleshooting – AS ABAP

Exercise and Break Out Session



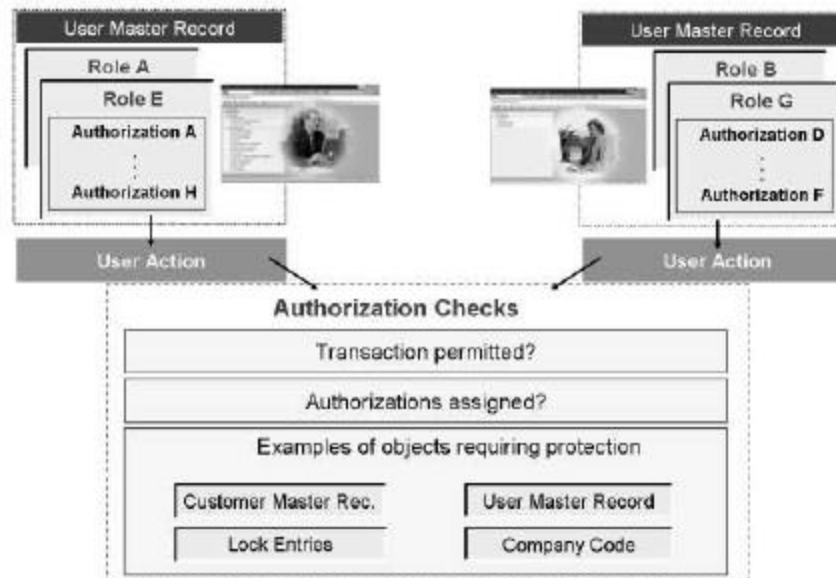
User Master and Authorization Object Concept – AS ABAP

Overview of Security and Authorizations

- Concept of Roles in AS ABAP
- Concept of Authorization Objects
- User & Role Management in AS ABAP
- Troubleshooting Authorization issues
- Concept of UME in AS JAVA
- Concept of Roles in AS JAVA
- User and Role Management in AS JAVA

User Concept

- Every SAP user requires a unique user ID to login into the system
- The user can login with the user ID only in the SAP application. The user does not gain access to the underlying database instance or the Operating system
- Users and Authorization Data are client-dependent
- Therefore every user in SAP will have a unique user master record
- In the system there is an authorization check every time any transaction is called or certain functions within the transaction are called



Types of SAP Users

Dialog Users

A normal dialog user is used for all logon types by just one person. During a dialog logon, the system checks for expired/initial passwords, and the user has the opportunity to change his or her own password. Multiple dialog logons are checked and, if appropriate, logged.

System Users

Use the System user type for dialog-free communication within a system or for background processing within a system, or also for RFC users for various applications, such as ALE, Workflow, Transport Management System, Central User Administration. It is not possible to use this type of user for a dialog logon. Users of this type are excepted from the usual settings for the validity period of a password. Only user administrators can change the password.

Communication Users

Use the communication user type for dialog-free communication between systems. It is not possible to use this type of user for a dialog logon. The usual settings for the validity period of a password apply to users of this type.

Types of SAP Users (Contd.)

Service User

A user of the type Service is a dialog user that is available to a larger, anonymous group of users. In general, you should only assign highly restricted authorizations to users of this type. Service users are used, for example, for anonymous system accesses using an ITS or ICF service. The system does not check for expired/initial passwords during logon. Only the user administrator can change the password. Multiple logons are permitted.

Reference User

Like the service user, a reference user is a general non-person-related user. You cannot use a reference user to log on. A reference user is used only to assign additional authorizations. You can specify a reference user for a dialog user for additional authorization on the Roles tab page.

User Type	Dialog
	Communication
	System
	Service
	Reference

SAPGUI compatibility with different user types

	SAP GUI-compatible	Not SAP GUI-compatible
Password change: Yes	Dialog	Communication
Password change: No	Service	System

User Creation using SU01 Transaction

You can create a new user master record by copying an existing user master record or creating a completely new one. The user master record contains all data and settings that are required to log on to a client of the SAP system. This data is divided into the following tab pages:

- Address: Address data
- Logon data: Password and validity period of the user, and user type. For further information about the password rules for special users, refer to SAP Note 622464
- Defaults: Default values for a default printer, the logon language
- Parameters: User-specific values for standard fields in SAP systems
- Roles and Profiles: Roles and profiles that are assigned to the user
- Groups: For the grouping of users for mass maintenance.

You must maintain at least the following input fields when creating a user: Last name on the Address tab page, initial password and identical repetition of password on the Logon Data tab page.

SU01 Tabs

Address
Tab

Display User

User: TEST USER
Last Changed On: 11/3/01 21.03.2009 14:54:51 Status: Saved

Address Login data SNC Defaults Parameters Roles Profiles

Person

Title Mr. 5
Last name Test
First name Test
Academic Title D.E.
Format B.E. TestTest
Function Test
Occupation Automobile
Room Number 104 Floor 11 Building JPL-EXPO

Communication

Language English Other communication...
Telephone Extension
Mobile phone Extension
Fax Extension
E-Mail
Custom Mail Remote Mail

Company
TATA Consultancy Services / /

Login
Data
Tab

Display User

User: TEST USER
Last Changed On: 11/3/01 21.03.2009 14:54:51 Status: Saved

Address Login data SNC Defaults Parameters Roles Profiles

Alias
User Type Dialing
Password
Password Status Initial password (set by administrator)
User Group for Authorization Check
User group ESSUSER User group for ESS user
Validity Period
Valid from 02.07.2007
Valid through 03.07.2007
Other Data
Accounting Number
Cost center

Defaults
Tab

Display User

User: TEST USER
Last Changed On: 11/3/01 21.03.2009 14:54:51 Status: Saved

Address Login data SNC Defaults Parameters Roles Profiles

Start menu /VIRSA/2VFA1_TOOLS
Login Language
Decimal Notation 1.234.567.89
Date Format DD.MM.YYYY
Time Format (12/24) 24 Hour format (Example: 1205:10)
Short Control
Output Device defht
Output mode indicator
Display Mail output
Personal Time Zone
of the User INDIA
Sys. Time Zone CET
CATT
Check indicator

Roles
Tab

Display User

User: TEST USER
Last Changed On: 11/3/01 21.03.2009 14:57:40 Status: Saved

Address Login data SNC Defaults Parameters Roles Profiles

Reference user for additional rights

Role Assignments

Rt	Role	Type	Valid From	Valid to	Name
✓	TCS-CONTROLLING_COSTING	3	21.03.2009	31.12.9999	TCS-CONTROLLING_COST
✓	TCS-DOCUMENT-MANAGEMENT	3	21.03.2009	31.12.9999	TCS-DOCUMENT-MANAG
✓	TCS-ESSUSER_EMP	3	21.03.2009	31.12.9999	Employee Self-Service (S4)
✓	TCS-FI_ROLE_01	3	21.03.2009	31.12.9999	TCS-FI_ROLE_01

Adding Roles to a User in SU01

You can explicitly add roles to a user and save it as shown below. You should be in change mode when you add the roles

Maintain User

User: TEST_USER

Last Changed On: 119361 | 21.03.2009 | 18:25:04 | Status: Saved

Address | Logon data | SNC | Defaults | Parameters | Roles | Profiles

Role

Reference user for additional rights:

St.	Role	Type	Valid From	Valid to	Name
<input checked="" type="checkbox"/>	TCS:CONTROLLING_COSTING		21.03.2009	31.12.9999	TCS:CONTROLLING_COST
<input checked="" type="checkbox"/>	TCS:DOCUMENT_MANAGEMENT		21.03.2009	31.12.9999	TCS:DOCUMENT_MANAG
<input checked="" type="checkbox"/>	TCS:ESSUSER_ERP		21.03.2009	31.12.9999	Employee Self-Service (HF
<input checked="" type="checkbox"/>	TCS:FI_ROLE_01		21.03.2009	31.12.9999	TCS:FI_ROLE_01
<input checked="" type="checkbox"/>	TCS:FI_ALL		21.03.2009	31.12.9999	TCS Finance & Controlling
<input checked="" type="checkbox"/>	TCS_PP_ALL		21.03.2009	31.12.9999	TCS Production PLanning

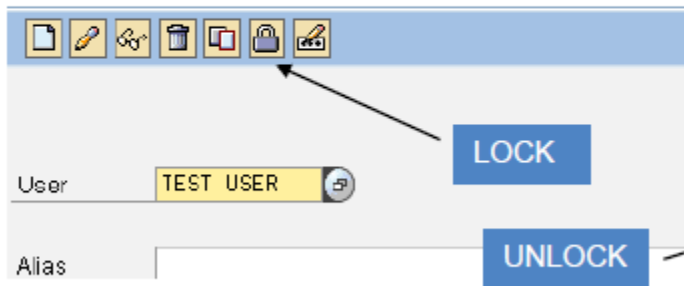
Break



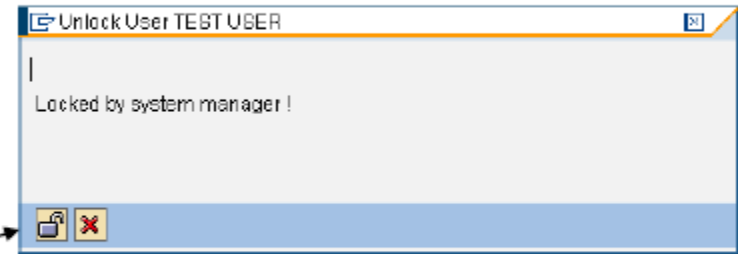
Managing a User Account

- You can lock and unlock a user in SU01. Once the user is locked the person is unable to login into the system, unless the system administrator explicitly unlocks the user ID

User Maintenance: Initial Screen



The screenshot shows the 'User Maintenance: Initial Screen' for user 'TEST USER'. At the top, there is a toolbar with icons for document, edit, delete, and others. Below the toolbar, the user name 'TEST USER' is displayed in a yellow box. To the right of the user name are two buttons: 'LOCK' and 'UNLOCK'. The 'UNLOCK' button is highlighted with a blue box and an arrow pointing to it.

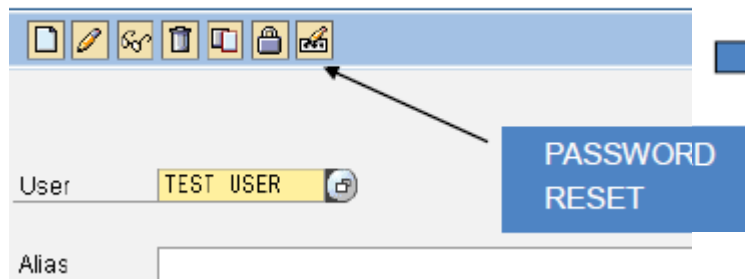


The screenshot shows the 'Unlock User TEST USER' dialog box. It contains the text 'Locked by system manager !' and a toolbar with a lock icon and a red 'X' icon. A blue arrow points from the 'UNLOCK' button in the previous screen to this dialog.

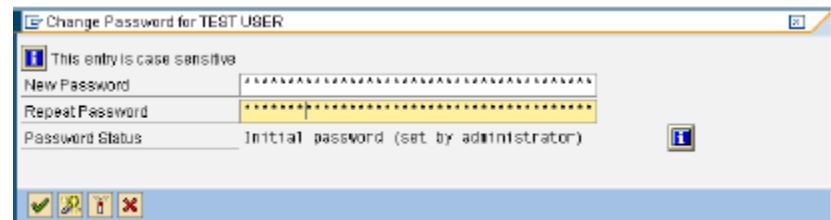
✓ User TEST USER unlocked, if this is permitted in this system

- It is possible to reset the password in case the user has forgotten the password

User Maintenance: Initial Screen



The screenshot shows the 'User Maintenance: Initial Screen' for user 'TEST USER'. At the top, there is a toolbar with icons for document, edit, delete, and others. Below the toolbar, the user name 'TEST USER' is displayed in a yellow box. To the right of the user name are two buttons: 'PASSWORD RESET' and 'UNLOCK'. The 'PASSWORD RESET' button is highlighted with a blue box and an arrow pointing to it.

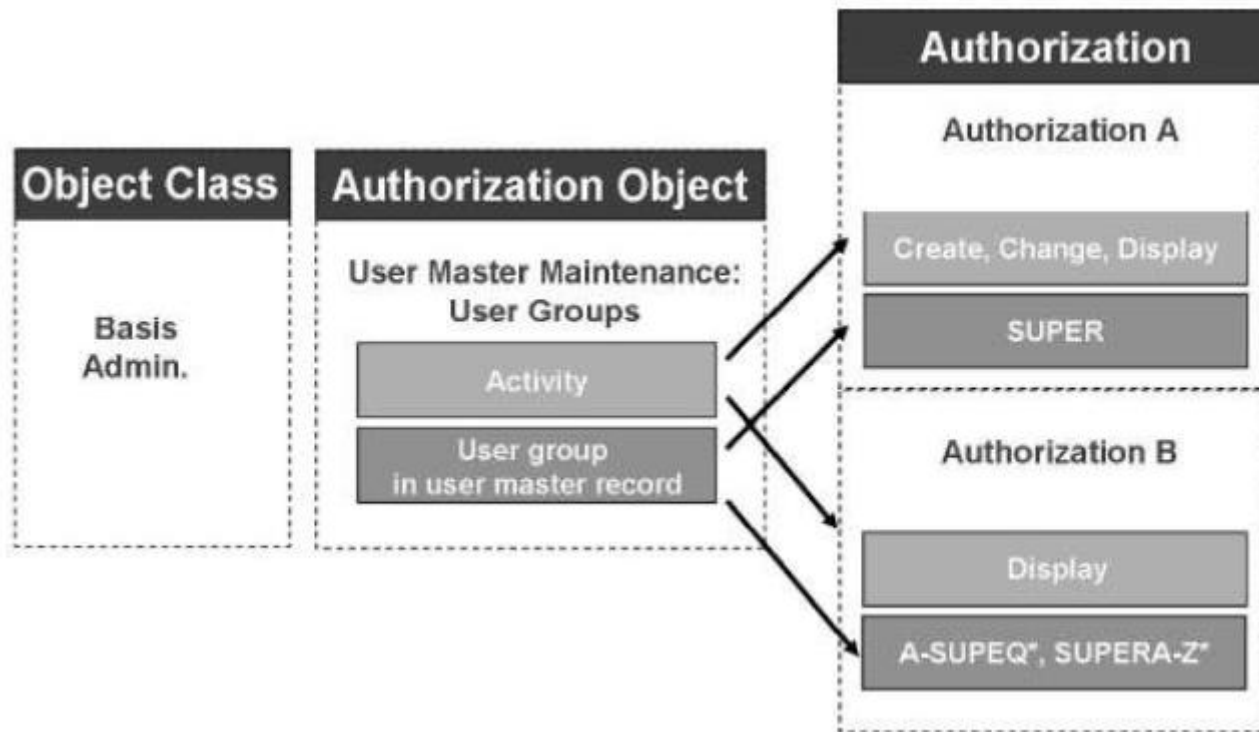


The screenshot shows the 'Change Password for TEST USER' dialog box. It contains a message 'This entry is case sensitive' and fields for 'New Password' and 'Repeat Password'. The 'Password Status' is 'Initial password (set by administrator)'. A blue arrow points from the 'PASSWORD RESET' button in the previous screen to this dialog.

✓ The password was changed

Authorization Concept

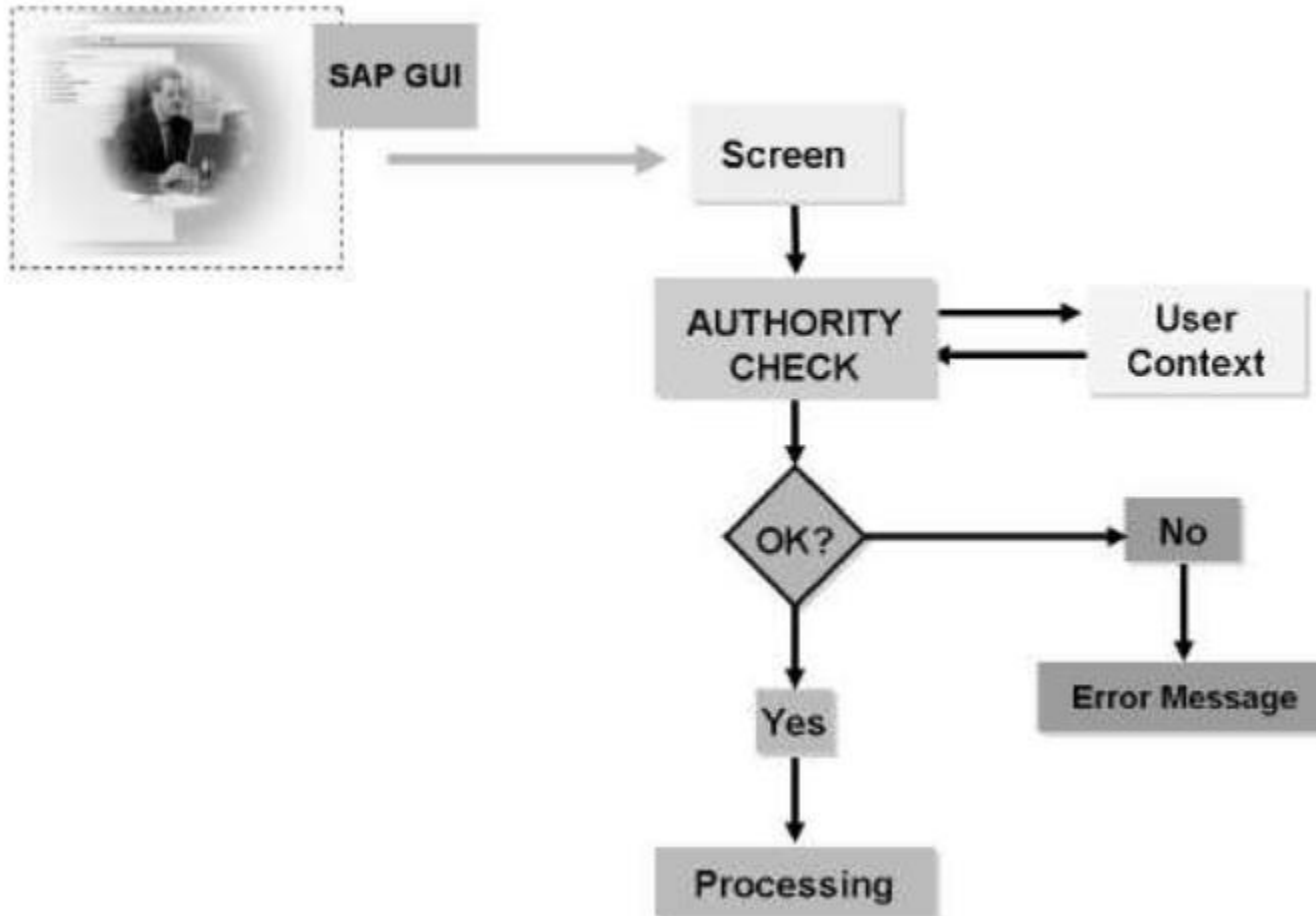
- The authorizations for users are created using roles and profiles. Administrators create the roles, and the system supports them in creating the associated authorizations
- Authorizations in SAP are built on the concept of Authorization Objects



Details on Authorization Objects

- Actions and the access to data are protected by authorization objects in the SAP system. To provide a better overview, authorization objects are divided into various object classes.
- Authorization objects allow complex checks that involve multiple conditions that allow a user to perform an action. The conditions are specified in authorization fields for the authorization objects and are AND linked for the check.
- Authorization objects and their fields have descriptive and technical names. In the example in the earlier slide, the authorization object "User master maintenance: User Groups" (technical name: S_USER_GRP) contains the two fields "Activity" (technical name ACTVT) and "User Group" in User Master (technical name: CLASS). The authorization object S_USER_GRP protects the user master record.
- An authorization object can include up to ten authorization fields. An authorization is always associated with exactly one authorization object and contains the value for the fields for the authorization object. An authorization is a permission to perform a certain action in the SAP system. The action is defined on the basis of the values for the individual fields of an authorization object. Example: Authorization B in the graphic for the authorization object S_USER_GRP allows the display of all user master records that are not assigned to the user group SUPER. Authorization A, however, allows records for this user group to be displayed.
- There can be multiple authorizations for one authorization object. Some authorizations are delivered by SAP, but the majority are created specifically for the customer's requirements.

Authorization Check Graphic



Authorization Check Details

- When a user logs on to a client of an SAP system, his or her authorizations are loaded in the user context. The user context is in the user buffer (in the main memory, query using transaction code SU56) of the application server.
- When the user calls a transaction, the system checks whether the user has an authorization in the user context that allows him or her to call the selected transaction. Authorization checks use the authorizations in the user context. If you assign new authorizations to the user, it may be necessary for this user to log on to the SAP system again to be able to use these new authorizations (for more information, see SAP Note 452904 and the documentation for the parameter auth/new buffering).
- If the authorization check for calling a transaction was successful, the system displays the initial screen of the transaction. Depending on the transaction, the user can create data or select actions. When the user completes his or her dialog step, the data is sent to the dispatcher, which passes it to a dialog work process for processing. Authority checks (AUTHORITY-CHECK) that are checked during runtime in the work process are built into the coding by the ABAP developers for data and actions that are to be protected. If the user context contains all required authorizations for the checks (return code = 0), the data and actions are processed and the user receives the next screen. If one authorization is missing, the data and actions are not processed and the user receives a message that his or her authorizations are insufficient. This is controlled by the evaluation of the return code. In this case, it is not equal to 0.
- All authorizations are permissions. There are no authorizations for prohibiting. Everything that is not explicitly allowed is forbidden. This can be described as a "positive authorization concept".

Maintaining Authorization Objects – SU24

Display Transaction SE11

Transaction Code: SE11 Saved

Selection Result

Na...	Text
SE11	ABAP Dictionary Maintenance

Maintain the Assignments of Authorization Objects

Download Upload Authorization Templates

Application Authorization Object

Selection

Type of Application

Transaction Code SE11

Authorization Objects

Status	Object	Object Description	Check Ind	Proposa
✓	S_ADMI_FCD	System Authorizations	Check	NO
✓	S_ALY_LAYO	ALV Standard Layout	Check	NO
✓	S_APPL_LOG	Applications log	Check	NO
✓	S_BCOS_BC	Authorization Object for Creating Support Message	Check	NO
✓	S_BDS_DS	BC-SRV-KPR-BDS: Authorizations for Document Set	Check	NO
✓	S_BTCH_ADM	Background Processing: Background Administrator	Check	NO
✓	S_BTCH_JOB	Background Processing: Operations on Background Jobs	Check	NO
✓	S_CTS_ADMI	Administration Functions in Change and Transport System	Check	NO
✓	S_DATASET	Authorization for file access	Check	NO
✓	S_DDSTCAUT	Structure Changes in Support Package Systems	Check	NO
✓	S_DEVELOP	ABAP Workbench	Check	YES
✓	S_DOKU_AUT	SE61 Documentation Maintenance Authorization	Check	NO
✓	S_GUI	Authorization for GUI activities	Check	NO
✓	S_PACKSTRU	Internal SAP Use: Package Structure	Check	NO
✓	S_PRO_AUTH	IMG: New authorizations for projects	Check	NO
✓	S_RFC	Authorization Check for RFC Access	Check	NO
✓	S_SPO_ACT	Spool: Actions	Check	NO
✓	S_SPO_DEV	Spool: Device authorizations	Check	NO
✓	S_TABU_CLI	Cross-Client Table Maintenance	Check	NO
✓	S_TABU_DIS	Table Maintenance (via standard tools such as SM30)	Check	NO
✓	S_TABU_RFC	Client Comparison and Copy: Data Export with RFC	Check	NO
✓	S_TCODE	Transaction Code Check at Transaction Start	Check	NO
✓	S_TRANSLAT	Translation environment authorization object	Check	NO

Maintaining Authorization Objects – SU24

Display Transaction SE11

Transaction Code: SE11 Saved

Selection Result

Na...	Text
SE11	ABAP Dictionary Maintenance

Field values for S_DEVELOP

Authorization Objects

Status	Object	Object Description	Check Ind.	Proposal
<input checked="" type="checkbox"/>	S_BDS_DS	BC-SRV-KPR-BDS: Authorizations for Document Set	Check	NO
<input checked="" type="checkbox"/>	S_BTCH_ADM	Background Processing: Background Administrator	Check	NO
<input checked="" type="checkbox"/>	S_BTCH_JOB	Background Processing: Operations on Background Jobs	Check	NO
<input checked="" type="checkbox"/>	S_CTS_ADMI	Administration Functions in Change and Transport System	Check	NO
<input checked="" type="checkbox"/>	S_DATASET	Authorization for file access	Check	NO
<input checked="" type="checkbox"/>	S_DDSTCAUT	Structure Changes in Support Package Systems	Check	NO
<input checked="" type="checkbox"/>	S_DEVELOP	ABAP Workbench	Check	YES
<input checked="" type="checkbox"/>	S_DOKU_AUT	SE61 Documentation Maintenance Authorization	Check	NO
<input checked="" type="checkbox"/>	S_GUI	Authorization for GUI activities	Check	NO
<input checked="" type="checkbox"/>	S_PACKSTRU	Internal SAP Use: Package Structure	Check	NO
<input checked="" type="checkbox"/>	S_PRO_AUTH	IMG: New authorizations for projects	Check	NO

Default Authorization Values (S_DEVELOP)

Object	Field Name	From	To
S_DEVELOP	ACTVT	01	
S_DEVELOP	ACTVT	02	
S_DEVELOP	ACTVT	03	
S_DEVELOP	ACTVT	06	
S_DEVELOP	ACTVT	07	

Check Indicator to activate/deactivate the authorization check for a particular object

Specifying Authorization Object Values

- The transaction SU24 is used to set authorization check status for individual transactions.
- Each transaction has underlying set of authorization objects
- Each object has a set of fields and values which permit certain functions.
- For example in transaction SE11 , the underlying object S_DEVELOP governs the rights of changes in table structure. When ACTVT field value is set to 1 , the user is able to modify the table structure.
- Note that changing the default values for fields in SU24 will result in changes which will affect all transactions that use the particular authorization object.

Lunch Break



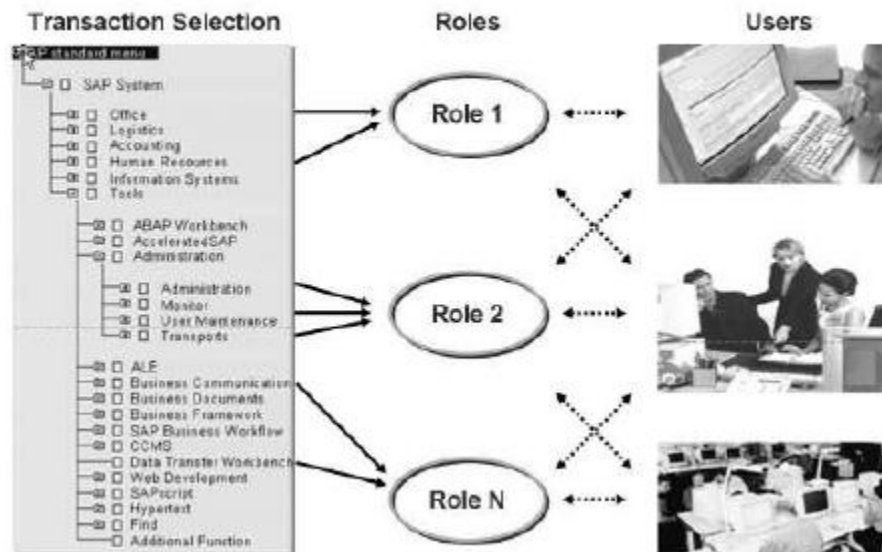


Role Management – AS ABAP

Role Management using PFCG

- Role Maintenance (transaction PFCG, previously also called Profile Generator or activity groups) simplifies the creation of authorizations and their assignment to users. In role maintenance, transactions that belong together from the company's point of view are selected. Role maintenance creates authorizations with the required field values for the authorization objects that are checked in the selected transactions.
- A role can be assigned to various users. Changes to a role therefore have an effect on multiple users. Users can be assigned various roles. The user menu comprises the role menu(s) and contains the entries (transactions, URLs, reports, and so on) that are assigned to the user through the roles.

Role Maintenance



Usage of PFCG

Role Maintenance

Transactions

Role: TCS_PP_ALL Single Role Comp. Role

Name: TCS Production PLanning

Views Show Documentation

Favorites Description Target Sys

Taking the example of the role TCS_PP_ALL, the next screens will indicate the structure of a role and the underlying authorization objects.

Tab "Authorizations" is where the object values need to be maintained

Display Roles

Other role

Role: TCS_PP_ALL
Description: TCS Production PLanning

Description **Authorizations** User MiniApps Personalization

Administration Information

	Created	Changed
User	TCSADM	222753
Date	02.01.2007	09.03.2009
Time	15:00:05	14:47:45

Transaction Inheritance

Derive from Role

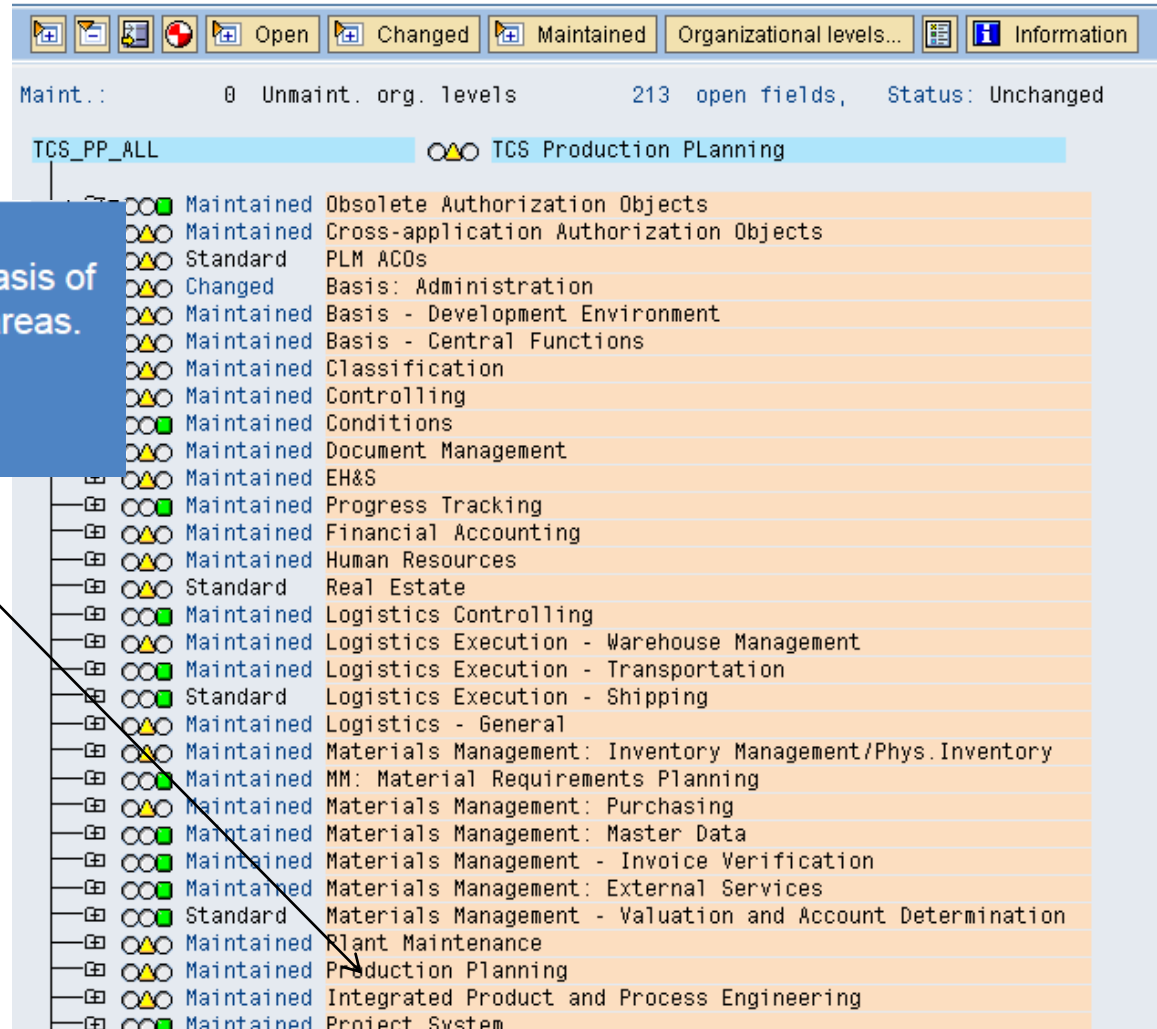
Long Text

This role is intended for all authorizations in Production Planning

Ln 1 - Ln 1 of 1 lines

Usage of PFCG (Contd.)

Display role: Authorizations



Maint.: 0 Unmaint. org. levels 213 open fields, Status: Unchanged

TCS_PP_ALL TCS Production Planning

000	Maintained	Obsolete Authorization Objects
000	Maintained	Cross-application Authorization Objects
000	Standard	PLM ACOs
000	Changed	Basis: Administration
000	Maintained	Basis - Development Environment
000	Maintained	Basis - Central Functions
000	Maintained	Classification
000	Maintained	Controlling
000	Maintained	Conditions
000	Maintained	Document Management
000	Maintained	EH&S
000	Maintained	Progress Tracking
000	Maintained	Financial Accounting
000	Maintained	Human Resources
000	Standard	Real Estate
000	Maintained	Logistics Controlling
000	Maintained	Logistics Execution - Warehouse Management
000	Maintained	Logistics Execution - Transportation
000	Standard	Logistics Execution - Shipping
000	Maintained	Logistics - General
000	Maintained	Materials Management: Inventory Management/Phys.Inventory
000	Maintained	MM: Material Requirements Planning
000	Maintained	Materials Management: Purchasing
000	Maintained	Materials Management: Master Data
000	Maintained	Materials Management - Invoice Verification
000	Maintained	Materials Management: External Services
000	Standard	Materials Management - Valuation and Account Determination
000	Maintained	Plant Maintenance
000	Maintained	Production Planning
000	Maintained	Integrated Product and Process Engineering
000	Maintained	Project System

Authorizations are categorized on the basis of the SAP Functional areas. Take the example of Production Planning

Usage of PFCG (Contd.)

Display role: Authorizations

Icons: Open, Changed, Maintained, Organizational Levels..., Information

Maint.: 0 Unmaint. org. levels 213 open fields, Status: Unchanged PP

Icon	Object	Field	Value	Object
Maintained	CC Change Master - Authorization Group			C_AENR_BGR
Maintained	CC Eng. Chg. Mgmt. Enhanced Authorization Check			C_AENR_ERV
Standard	CC Engineering change mgmt - revision level for materials			C_AENR_RV1
Maintained	CC Engineering Change Mgt - revision level for documents			C_AENR_RV2
Standard	CIM: Reworking error records from autom. goods movements			C_AFFR_TWK
Maintained	CIM: Order category			C_AFKD_ATY
Maintained	CIM: Authorization for Prod Order/Order Type/Plant/Activity			C_AFKD_AWA
Maintained	CIM: Plant for order type of order			C_AFKD_AWK
Maintained	CIM: Confirmation			C_AFRU_AWK
Maintained	CIM: Confirmation			T-E158001680
	Activity	01, 02, 83, 85		ACTVT
	Order Type	*		AUFART
	Plant	*		WERKS
Maintained	CIM: Confirmation			T-E158001681
	Activity	*		ACTVT
	Order Type	*		AUFART
	Plant	*		WERKS

Authorization Field
Names

Authorization Field Values

Authorization Objects

Interpretation of Authorization Field Values

The image shows two overlapping SAP windows. The top window is titled 'Define Values' and shows the object 'C_AFRU_AWK' with the description 'CIM: Confirmation'. Below this, the field 'ACTVT' is selected with the description 'Activity'. A list of activities is shown with checkboxes: 01 Create or generate, 02 Change, 03 Display, and 05 Reverse. All are checked. The bottom window is titled 'Field values' and shows the same object 'C_AFRU_AWK' with the field 'WERKS' selected, described as 'Plant'. It shows a 'Value Intvl' table with columns 'From' and 'To'. The first row is empty, and the rest are also empty.

- In this specific example of Production Planning , the C_AFRU_AWK object has the fields activity , Order Type and Plant.
- The field values for activity shows that the full range of functions are permitted.
- Now since Order Type and Plant values are “*” , this means that the user who has been assigned the role TCS_PP_ALL will automatically be able to process all confirmations for all order types and all plants in the SAP System.
- In order to restrict the user to process confirmations for a particular plant , the BASIS administrator must specify explicitly the plant names or order types in PFCG change mode.
- Example shown below :

The image shows the 'Field values' window for object 'C_AFRU_AWK' with field 'WERKS' (Plant). The 'Value Intvl' table is populated with the following data:

From	To
1004	
1100	
1234	
1704	

Assigning Users to a Role

Change Roles

Role: TCS_PP_ALL
Description: TCS Production Planning

Tab: User

User comparison

User Assignments

User ID	User name	From	to	I...
HPAD1-135767	Demo User for HPAD	26.12.2007	31.12.9999	
HPAD2-135767	Demo User for HPAD	26.12.2007	31.12.9999	
HPAD3-135767	Demo User for HPAD	26.12.2007	31.12.9999	
HPAD4-135767	Demo User for HPAD	26.12.2007	31.12.9999	
HPADRFCUSER	RFC User For HPAD	26.12.2007	31.12.9999	
NHPCTR61	NHPCTR61	23.05.2007	31.12.9999	
NHPCTR62	NHPCTR62	23.05.2007	31.12.9999	
NHPCTR63	NHPCTR63	23.05.2007	31.12.9999	
SAPLOGON	SAPLOGON	06.06.2008	31.12.9999	
SAPPLM01	SAPPLM01	04.12.2007	31.12.9999	
SAPPLM02	SAPPLM02	30.01.2008	31.12.9999	
SOLMANSM3100	SOLMANSM3100	04.12.2007	31.12.9999	

Using the Tab "User", you can explicitly add users to a role

After adding, you must perform a user comparison, so that the user master records are updated

User Master Comparison

Change Roles

Other role

Role: TCS_PP_ALL
Description: TCS Production PLanning

Description Menu Authorizations **User** MiniApps Personalization

Compare Role User Master Record

Last comparison

User	119361
Date	21.03.2009
Time	18:19:20

Complete adjustment

User	119361
Date	21.03.2009
Time	18:19:20

Information for user master comparison

Status: User assignment has changed since the last save

Complete comparison Information

User Assignments

User ID	User name
HPAD1-135767	Demo User for HPAD
HPAD2-135767	Demo User for HPAD
HPAD3-135767	Demo User for HPAD
HPAD4-135767	Demo User for HPAD
HPADRFCUSER	RFC User For HPAD
NHPCTR01	NHPCTR01
NHPCTR02	NHPCTR02
NHPCTR03	NHPCTR03
SAPLOGON	SAPLOGON
SAPPLM01	SAPPLM01
SAPPLM02	SAPPLM02
SOLMANSM3100	SOLMANSM3100

23.05.2007 31.12.9999
06.08.2008 31.12.9999
04.12.2007 31.12.9999
30.01.2008 31.12.9999
04.12.2007 31.12.9999

☒ User comparison

The user comparison button should be in green.

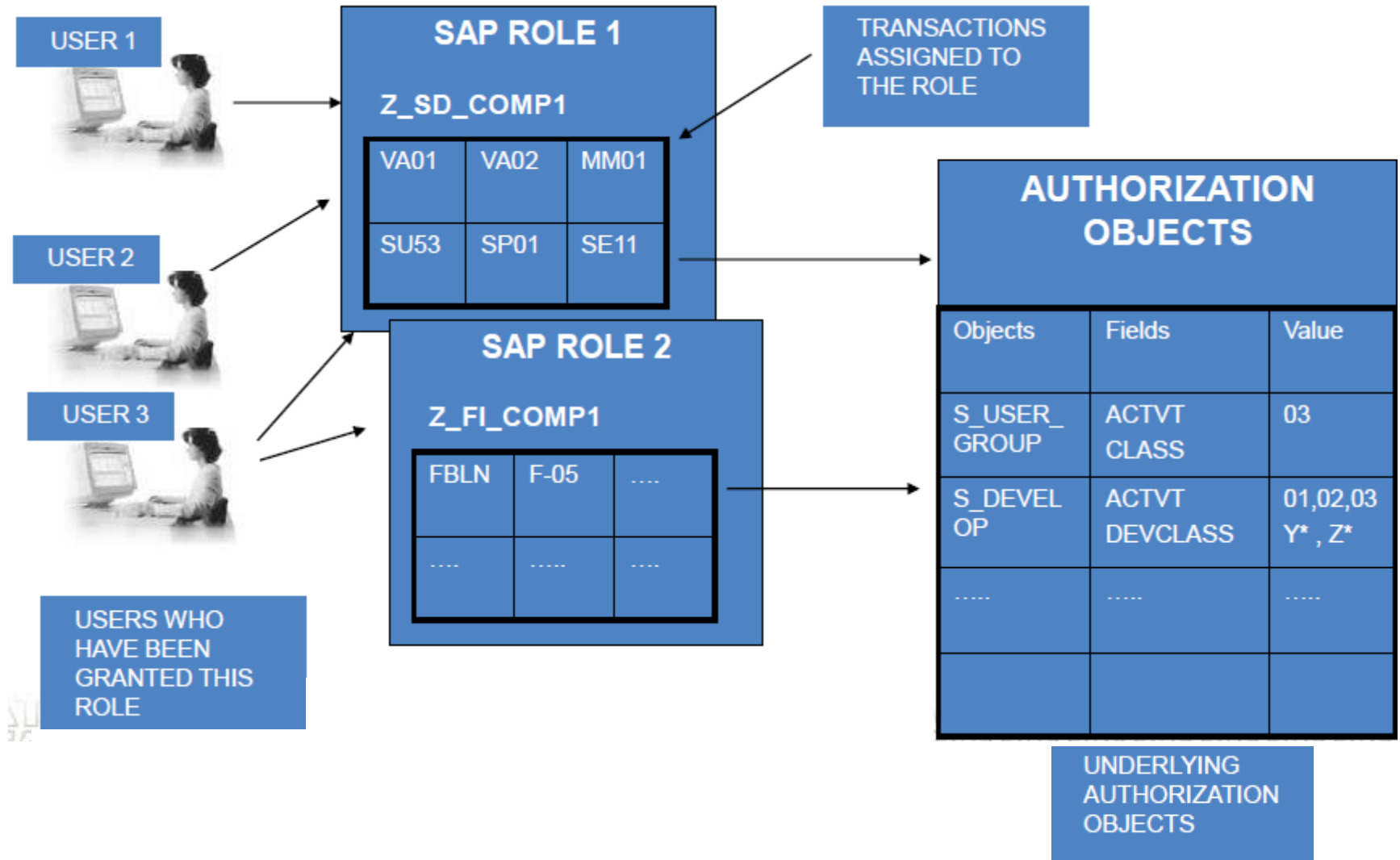
Authorization Profiles Concept

- After making changes in the role , you have to generate the profile for the role as well as the authorization profiles for the objects
- The Role and Profile are two different concepts. The role is a collection of authorization objects grouped by functional areas
- The profile is a specific compiled version of either the role as a whole or the authorization object
- In ECC 6.0 , you should not assign profiles to a user , as both SU01 and PFCG automatically determine the required profiles
- In ECC 6.0 , you must assign ONLY roles to users






The screenshot displays the SAP authorization configuration interface. It shows two roles, both named 'Maintained CIM: Confirmation'. The first role is associated with the authorization profile 'T-E158001600', and the second role is associated with 'T-E158001601'. Both roles have three authorization objects: 'Activity' (values: 01, 02, 03, 05), 'Order Type' (value: *), and 'Plant' (value: *). An 'Information About Authorization Profile' dialog is open for the profile 'T-E1580016', showing the following details:

Information About Authorization Profile	
Profile Name	T-E1580016
Profile Text	Profile for role TCS_PP_ALL
Status	Authorization profile is generated

Hierarchy of Users, Roles and Objects



Managing User Logon Parameters

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

Managing User Logon Parameters (Contd.)

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_gul_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

SAP Standard Users

- Essentially, there are two types of standard 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 ECC installation). Standard 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 standard 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 created automatically 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.

SAP Standard Users (Contd.)

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 or the password changed. This user should only be used for EarlyWatch functions (monitoring and performance).

SAP* User Special Features

- 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 standard user. Create a superuser with full authorization.
- If you now delete the user master record SAP* from the database SQL prompt, 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.

NOTE : The user master record in SAP is in the database table : USR02

Initial Passwords of Standard Users

Initial Logon Procedure in SAP Clients

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



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.

Break





User Information Management and Troubleshooting

User Information System – Transaction SUIM

- You can obtain an overview of user master records, authorizations, profiles, roles, change dates, and so on using the information system.
- You can display lists that answer very varied questions. For example:
 - Which users have been locked in the system by administrators or failed logon attempts?
 - When did a user last log on to the system?
 - What changes were made in the authorization profile of a user?
 - In which roles is a certain transaction contained?
 - Which authorization objects are assigned to roles
 - Who has made the last changes in a user's master record ?

Using SUIM

User Information System

Structure

- User Information System
 - User
 - Cross-System Information (Central User Administration)
 - Users by Address Data
 - Users by Complex Selection Criteria
 - With Unsuccessful Logons**
 - By Logon Date and Password Change
 - With Critic

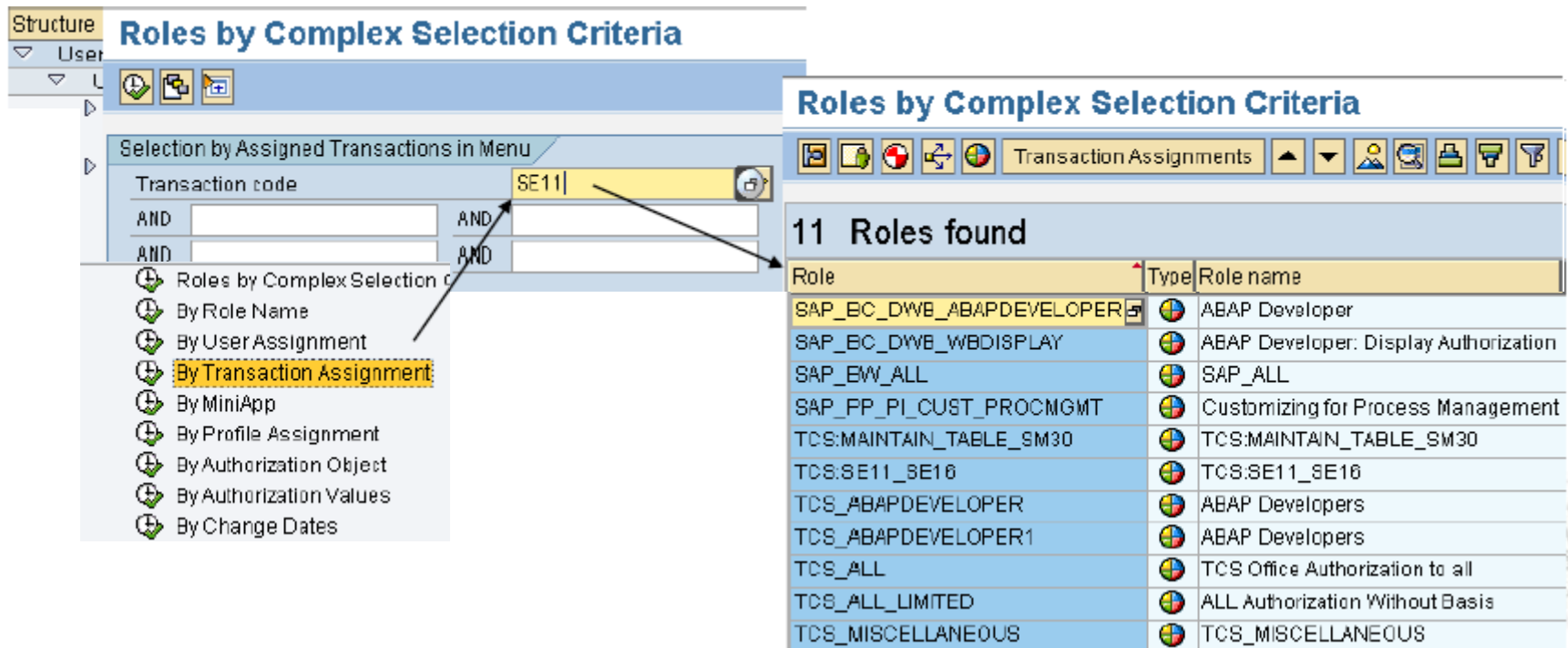
Users by Logon Date and Password Change (39 Hits)

Roles	System	ER1	Client	100	Checked by	119361	21.03.2008	19:02:34
Profiles	Profile Parameters of Instance	septs01_ER1_10						
Authorizations	loginfailed_user_auto_unlock	0						
Authorization Ob	loginfails_to_user_lock	3						
Transactions	login/disable_password_logon	0						
Comparisons	Selection Criteria:							
Where-Used Lis	Users Valid Today							
Change Docum	Users not Locked							

User	Group	User Type	Creator	Created On	Valid from	Valid through	Logon	Logon	Password	Password	Lock	Reason for User
123072	SUPER	A Dialog	TCBADM	02.11.2006			22.11.2006	10:54:58	✓	14.11.2006	Administrator	
126700		A Dialog	ABAP12	14.02.2007			30.04.2007		✗	16.04.2007	Incorrect Logon at	
137137		A Dialog	210233	20.06.2007			22.06.2007	20:28:18	✓	20.06.2007	Administrator	
145457		A Dialog	179115	31.01.2007			10.09.2007	15:43:25	✓	05.05.2007	Incorrect Logon at	
158782	SUPER	A Dialog	161185	01.02.2007			18.02.2007	18:10:27	✓	07.02.2007	Administrator	
162694		A Dialog	158606	23.02.2007			13.04.2007	13:48:50	✓	23.02.2007	Incorrect Logon at	
162704	SUPER	A Dialog	TCBADM	02.11.2006			18.01.2007	14:55:02	✓	02.11.2006	Administrator	
165236	SUPER	A Dialog	117109	18.07.2006			05.03.2007	18:43:36	✓	19.07.2006	Incorrect Logon at	
168878		A Dialog	128700	18.02.2007			18.09.2007	10:41:50	✓	18.02.2007	Incorrect logons	
178360	LGHC	A Dialog	221337	23.10.2008	30.09.2008	31.03.2009	14.03.2009		✗	02.03.2009		

Looking up all Roles for a Transaction

- For maintaining strict standards of security compliance , the SUIM transaction is extremely important
- For example , some SAP roles such as SAP_ALL and SAP_NEW should not be granted to any users
- Granting access to SE11 and SE38 in production systems can cause inadvertent changes to programs or tables
- Example of all roles for transaction SE11



The screenshot displays the SAP SUIM (Security User Interface Monitor) transaction. The left pane shows the 'Roles by Complex Selection Criteria' menu with 'By Transaction Assignment' selected. The right pane shows the results for transaction code 'SE11'.

Roles by Complex Selection Criteria

Transaction code: SE11

Selection by Assigned Transactions in Menu

AND [] AND [] AND [] AND []

Roles by Complex Selection Criteria

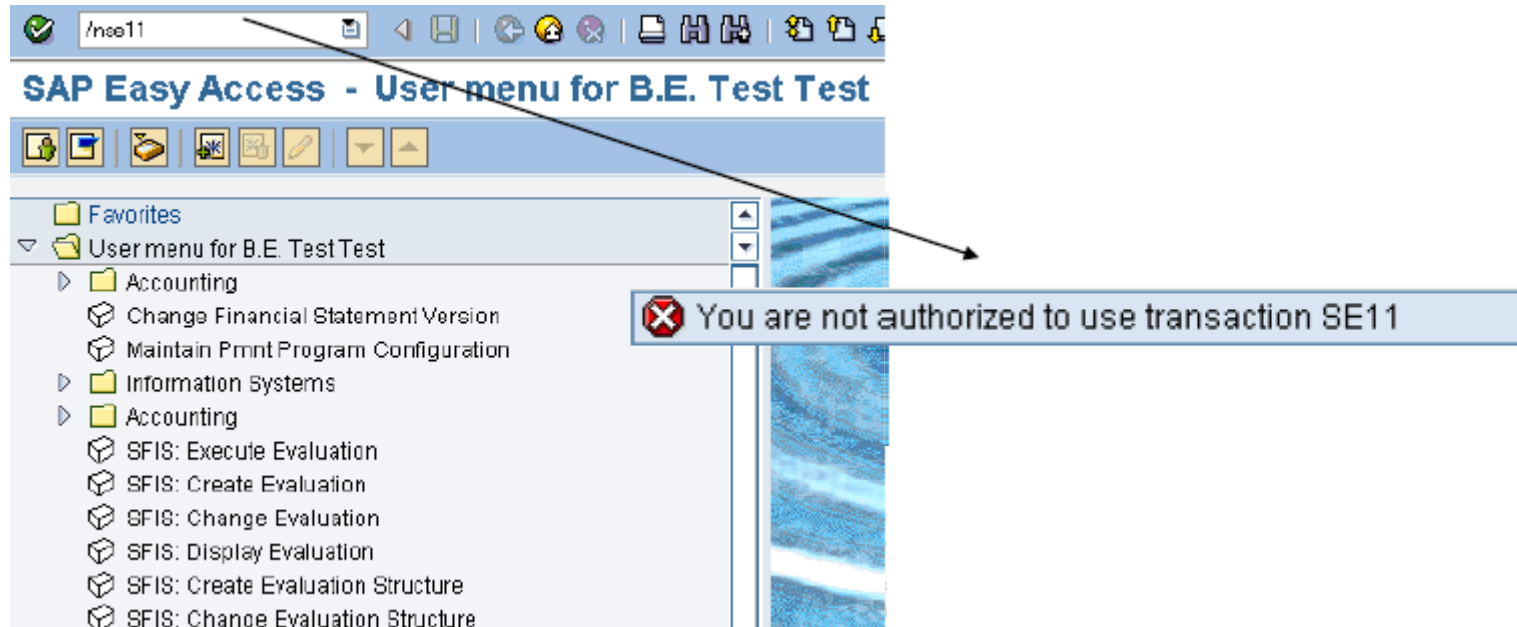
- By Role Name
- By User Assignment
- By Transaction Assignment**
- By MiniApp
- By Profile Assignment
- By Authorization Object
- By Authorization Values
- By Change Dates

11 Roles found

Role	Type	Role name
SAP_EC_DWE_ABAPDEVELOPER	ABAP Developer	ABAP Developer
SAP_EC_DWE_WBDISPLAY	ABAP Developer: Display Authorization	ABAP Developer: Display Authorization
SAP_EW_ALL	SAP_ALL	SAP_ALL
SAP_PP_PI_CUST_PROCMGMT	Customizing for Process Management	Customizing for Process Management
TCS:MAINTAIN_TABLE_SM30	TCS:MAINTAIN_TABLE_SM30	TCS:MAINTAIN_TABLE_SM30
TCS:SE11_SE16	TCS:SE11_SE16	TCS:SE11_SE16
TCS_ABAPDEVELOPER	ABAP Developers	ABAP Developers
TCS_ABAPDEVELOPER1	ABAP Developers	ABAP Developers
TCS_ALL	TCS Office Authorization to all	TCS Office Authorization to all
TCS_ALL_LIMITED	ALL Authorization Without Basis	ALL Authorization Without Basis
TCS_MISCELLANEOUS	TCS_MISCELLANEOUS	TCS_MISCELLANEOUS

Troubleshooting Authorization Issues – SU53

- The SU53 transaction is a trace transaction , which provides comprehensive information on the errors encountered during an authorization check.
- The SU53 transaction must be immediately run in the same user session following the authorization error
- Below example shows how the user encountered an authorization error , and how the information was obtained from SU53. User tried to execute SE11. In the same session , the user executes SU53 (see next slide)



SU53 Error Report

Display Authorization Data for User TEST USER

Text View			
Description			Authorizati
User Name	TEST USER	Authorization Object	S_TCODE
System	ER1	Client	100
Date	21.03.2009	Time	19:12:54
Instance	sapcs01	Profile Parameter auth/new buffering	4
Authorization check failed			
Object Class AAAAB Cross-application Authorization Objects			
Authorization Obj. S_TCODE Transaction Code Check at Transaction Start			
Authorization Field TCD Transaction Code			
			SE11
User's Authorization Data TEST USER			
Object Class AAAAB Cross-application Authorization Objects			
Authorization Object S_TCODE Transaction Code Check at Transaction Start			
‣ Authorizat. T-E158001000 Transaction Code Check at Transaction Start			
‣ Authorizat. T-E158001001 Transaction Code Check at Transaction Start			
‣ Authorizat. T-E158001002 Transaction Code Check at Transaction Start			
‣ Authorizat. T-E158001003 Transaction Code Check at Transaction Start			

- The SU53 report shows that the transaction SE11 has not been assigned to any of the roles that has been granted to the TEST USER.
- The solution would be explicitly add the authorization object , known as S_TCODE with value "SE11" in any one of the roles assigned to TEST USER.

Breakout Session



Exercise

- **Special Note : Instructions for instructor – Set Check/Maintain on all authorization objects for MM01 using SU24**
- **Login into the system with the userid/password provided by your instructor**
- **Start transaction SU01 , and create a test user TESTGRP(x).**
- **Start transaction PFCG , and open the role TCS_FI_ALL**
- **Create a copy of this role with the name TCS_FI_ALL_Group(X)**
- **Open the role , and with the help of the instructor , insert the authorization object S_TCODE. For field value , enter MM01**
- **Assign your test user to this role , and do user comparison**
- **Login with the new user and password , and run transaction MM01**
- **Try and create a new material. Check for any authorization errors.**
- **Run SU53 immediately and analyze the report**

Q&A Session



People matter, results count.



About Capgemini

With more than 125,000 people in 44 countries, Capgemini is one of the world's foremost providers of consulting, technology and outsourcing services. The Group reported 2012 global revenues of EUR 10.3 billion.

Together with its clients, Capgemini creates and delivers business and technology solutions that fit their needs and drive the results they want. A deeply multicultural organization, Capgemini has developed its own way of working, the Collaborative Business Experience™, and draws on Rightshore®, its worldwide delivery model.

Rightshore® is a trademark belonging to Capgemini



www.capgemini.com

