Authorizations Made Easy

Generating Authorization Profiles

Release 4.5A/B

SAP Labs, Inc.
Palo Alto, California

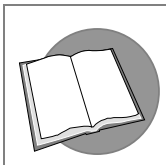
Copyright

Trademarks

R/3 Simplification Group
SAP Labs, Inc.
3475 Deer Creek Road
Palo Alto, CA 94304

www.saplabs.com/simple
simplify-r3@sap.com

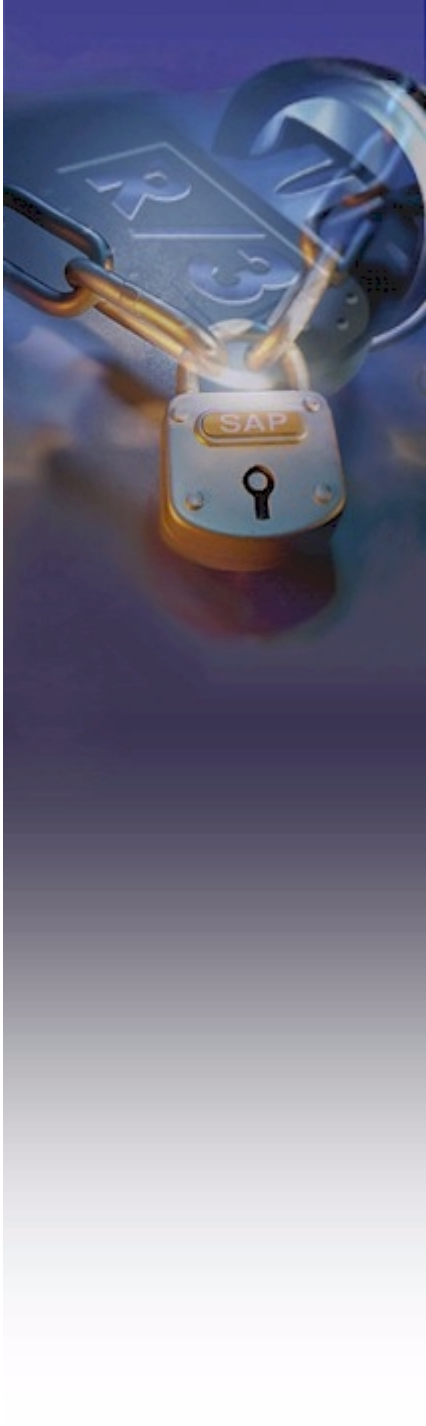
Printed in the United States of America.
ISBN 1-893570-23-1



Contents at a Glance

Detailed Table of Contents

Introduction



Contents

About this Guide

This guide is designed to help you set up the authorization environment in the customer system using the Profile Generator (PG). It explains what you need to know to perform this task and helps you use the standard tools provided with your system.

This guide refers to Release 4.5A/B of the SAP R/3 System. All screenshots are from Release 4.5A unless otherwise noted. This guide provides you with the following:

- The big picture (security and the authorization concept in R/3)
- Tasks you need to perform during and after installation of R/3 to facilitate the use of the PG
- Tasks you need to perform after an upgrade of the R/3 System
- All the essential steps for security implementation using the PG
- How to install and work with the predefined activity groups (PDAGs)
- Information on the Session Manager implementation (transaction *SESS*)
- Tasks to prepare for going live
- Appendixes with the most important Online Service System notes about using the PG and the most frequently asked questions.
- PDAGs in transport files on a CD for Releases 4.5A and 4.5B

Do You Need this Guide?

This guide was designed for the following people using the PG either in an implementation project or as an ongoing reference:

- **Basis Consultants** who install R/3 and set up the security at customer sites
- **Application Consultants** who want to start using the PG as the basis for their customer security implementation
- **Customer IT and help desk personnel**

How to Use this Guide

Depending on your general SAP and authorization concept specific knowledge, start with the following sections:

- If you have little or no knowledge concerning security and the authorization concept in R/3, start with chapter 1, *R/3 System Security and the Authorization Concept*.
- Everyone, even the experts, should read chapter 2, *Setting Up the Profile Generator*. Familiarity with this chapter ensures a complete setup before you actually start working with the PG.

- If you have already used the PG in Release 3.0F/3.1G/3.1H/4.0A/4.0B we strongly recommend that you read the chapter *What's New in 4.5* and the appropriate section in chapter 14, *Upgrades*. In this chapter, we discuss the steps to be performed before you continue working with the PG after an R/3 System upgrade. We provide information for a smooth transition to your next release.
- Read chapters 1–9 at least once for information related to the implementation of security and using the Profile Generator. After that, you can browse the chapters on performing specific tasks.
- The PDAGs and authorization profiles provide a basis to further configure your specific requirements. All of the predefinitions are easily adaptable to your needs, and standard R/3 settings are also available. Chapter 10 describes how to start with the PDAGs and adapt them to your needs.
- Before transporting activity groups, read chapter 12, *Transporting* carefully.
- Chapter 13, *Tips and Trouble-Shooting Management*, helps solve ongoing authorization problem once you go live.

Certain terminology, user information, and special icons are used throughout this guide. The following sections explain how to identify and use these helpful features.

Special Icons

Throughout this guide special icons indicate important messages. Below are brief explanations of each icon:

Exercise caution when performing this task or step. An explanation of why you should be careful is included.

This information helps you understand the topic in greater detail. It is not necessary to know this information to perform the task.

These messages provide helpful hints and shortcuts to make your work faster and easier.

This icon indicates that you will find additional software included on a CD at the end of the book or on the Simplification Group web page *http://www.saplabs.com/auth*.

Navigating the System

You may navigate the R/3 System by using either menu paths, transaction codes, or shortcut and function keys. If you use transaction codes, remember that you can enter the codes from the main *SAP R/3* screen. But if you wish to jump from one transaction to another, you must precede the transaction with either **/n** or **/o**, as follows:

/n<trans code>	(for example, **/nVA01**)	Use **/n** to exit the current transaction and start a new transaction. Your current transaction gets replaced by the new one.
/o<trans code>	(for example, **/oVA01**)	Use **/o** to open a new session (window). Your current transaction is maintained, while a new window opens with the new transaction.

Before you use **/n<transaction code>**, make sure you have saved all information. Otherwise, when you jump from one transaction to another, all unsaved information is lost.

If you wish to review transactions side-by-side, use **/o<transaction code>**.

Terminology

The following sections explain the terminology used throughout this guide.

Choose

When you see the word "choose," you will either perform certain actions by choosing particular buttons on screen (using the mouse or a shortcut key, for example) or follow given menu paths.

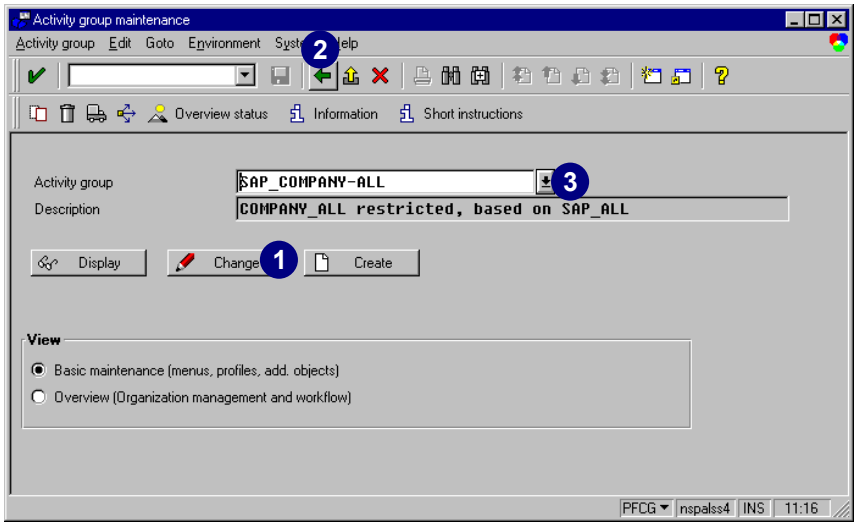
Buttons and Icons

"Choose" is always used for actions involving on-screen buttons or icons.

For example, the following phrases ask you to choose an on-screen button. You may either click with the mouse or use shortcut keys to activate the function.

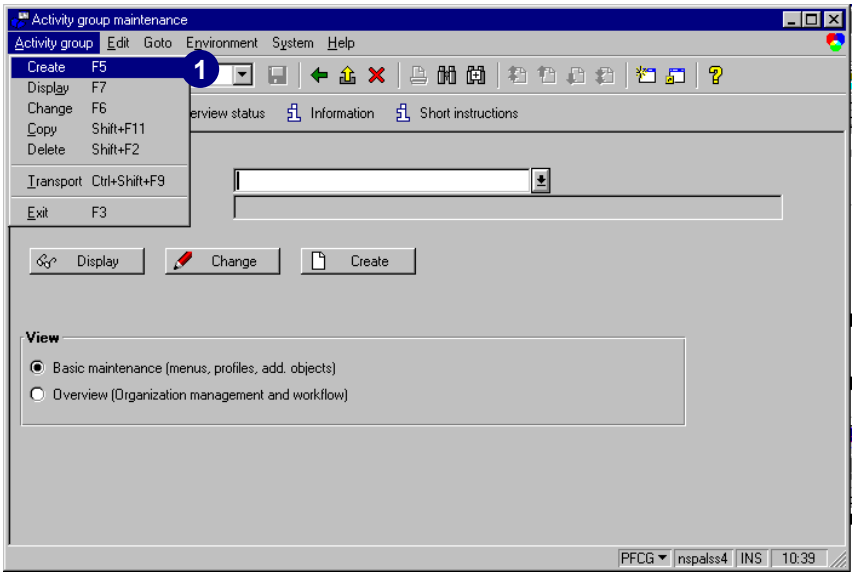
1. Choose *Change*.
2. Choose *Back*.
3. Choose *possible entries*.

Number callouts on the screenshot help clarify the activity.



Menu Paths

The word "choose" always appears with menu paths. In some cases, a menu path might lead you through several screens. Either use your mouse to select the menu item from the top of your window or use shortcut keys. In most cases, the direct transaction is also provided.



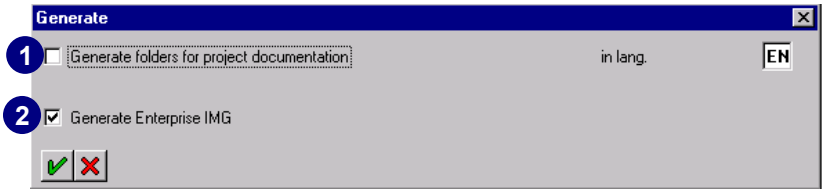
Menu paths appear as follows:

1. On the *Activity group maintenace* screen, choose *Activity group* → *Create*.
2. In the *Command* field, enter transaction **PFCG** and choose *Enter* (or choose *Tools* → *Administration* → *User maintenance* → *Activity groups*).

Select

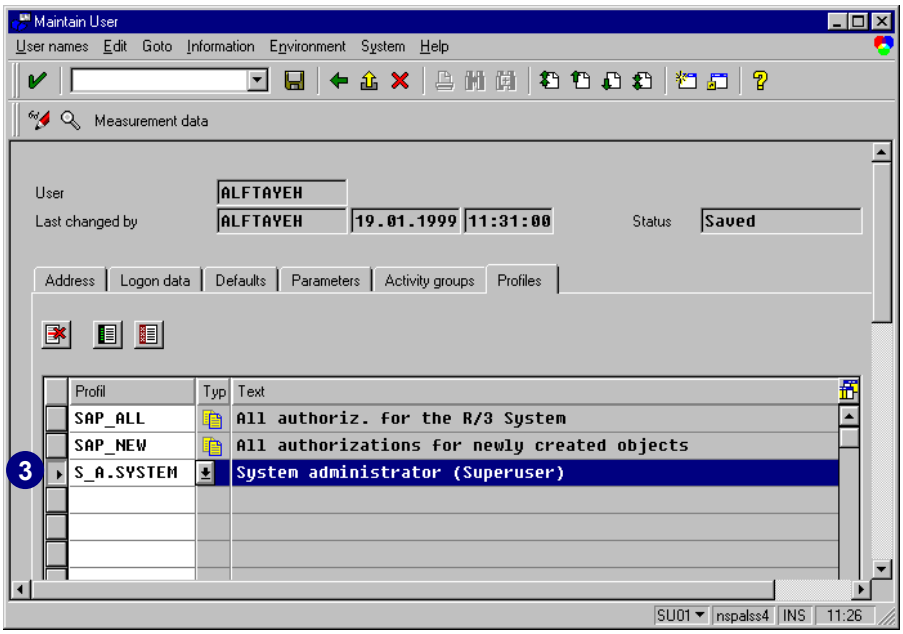
The words "select" and "deselect" always appear in instructions for checkboxes and radio buttons. For example:

1. Deselect *Generate folders for project documentation*.
2. Select *Generate Enterprise IMG*.



Sometimes “select” is used to select a particular line. For example:

3. Select the line for *S_A.System – System administrator*.



Typeface Styles

The steps that require “user input” (text to be entered into a field or after a command prompt) are indicated with **`bold, courier`** font such as:

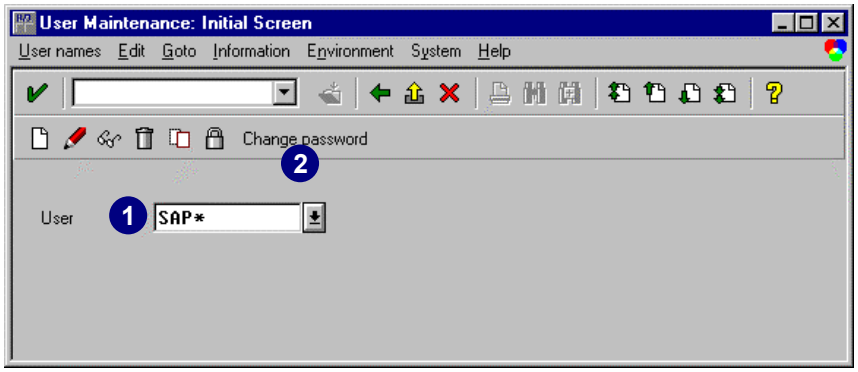
Enter **`14287`** in *Personnel number* .

Notice that “Personnel number” appears in *Object style,* which is italicized text that indicates the word is an on-screen object, such as a:

- Button
- Field
- Screen title
- Book or chapter title
- Screen text or messages

For example:

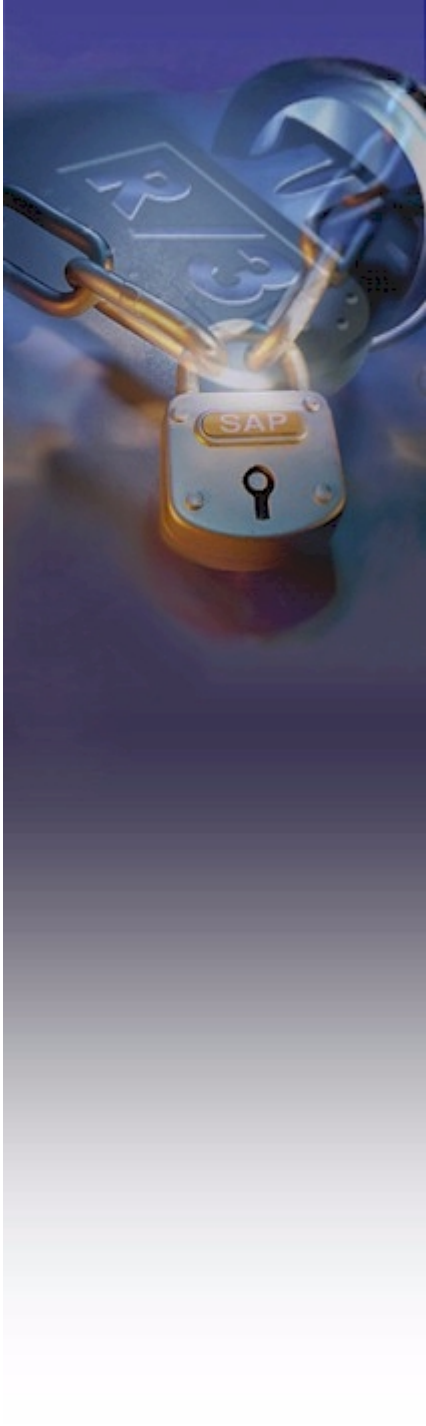
1. In the *User Maintenance* screen, enter **`SAP*`** in *User*.
2. Choose *Change password*.



With the above examples, in the first step, whenever you see text in **`courier bold`**—user input style—you know that information needs to be entered. Also in the first step, the words *User Maintenance* and *User* are italicized because they refer to a screen title and an on-screen field.

The second step indicates that an action is required. *Change password* is italicized because it is an on-screen button.

What's New in 4.5



Contents

Overview

This chapter provides a brief description of the new functionality of the Profile Generator (PG) and other related changes in the R/3 Releases 4.5 A/B.

For step-by-step procedures and detailed information on specific topics, please see the appropriate chapters, as referenced.

For the latest news, you should always check the release notes for 4.5.

Activation of the Profile Generator

If you install R/3 Release 4.5x new the Profile Generator (PG) is now already activated. If you upgrade to 4.5x from an earlier release where you did not utilize (and therefore did not activate) the PG needs to be activated.

For detailed information, see chapter 2, the section *Activating Profile Generator*.

Transporting

Transporting Activity Groups

When you transport activity groups, this action also transports the authorization profiles. Unlike previous releases, the profiles no longer have to be regenerated in the target system in transaction *SUPC*. However, you have to compare the user master records (user master reconciliation) when you import activity groups into the target system.

Transporting Activity Group User Assignments

You can decide whether you would like to transport the user assignments together with the activity groups.

You can lock the system against importing user assignment from activity groups. However this needs to be done in the Customizing table *PRGN_CUST,* using transaction *SM30*.

Transporting the user assignments should only be done if the central user administration is not being used.

For detailed information, see chapter 12, *Transporting*.

Responsibilities and Derived Activity Groups

Activity groups with responsibilities that were created in Releases 4.0A and 4.0B are migrated now to separate activity groups in 4.5x that are derived from each other. As a result of the migration, the new activity groups then receive the old activity groups' transactions. For each responsibility, a derived activity group contains the authorization data and user assignments.

With this new functionality, the old functionality is completely secured with additional possibilities. For example with the old responsibility, which is now a true activity group, you can assign users and authorization data.

For detailed information on derived activity groups, see chapter 4, the section *Copying and Deriving Activity Groups*.

Customizing Authorization

With this option you can assign projects or views of the Implementation Guide (IMG) projects to the activity group. The aim of this assignment is to generate authorizations for and assign users to specific IMG activities. When you generate profiles, this also generates the authorizations necessary to execute all activities in the assigned IMG projects/project views. It is also possible to transfer users to an activity group, if users (resources) are assigned to IMG projects in the project management.

For detailed information on how to *Assign IMG Project/Project Views to Activity Groups* and how to *Maintain/Update Customizing Authorization,* see chapter 5, the section *Customizing Authorizations*.

For detailed information on how to create user assignments with customizing authorizations, see chapter 8, the section *Transfering Users from an IMG Project to an Activity Group.*

Globally Deactivating or Activating Authorization Checks

It is now possible to switch off the check on individual authorization objects globally (using transaction code *auth_switch_objects*).

For detailed information, see chapter 2, the section *Globally Deactivating or Activating Authorization Checks.*

What's New in Specific Modules

To see what is new in a specific module, please see the release notes:

To do this, select from the menu option: *Help* → *Release Notes*

Module	Description
Treasury	Loans/Basic Data has new authorizations related to credit standing check per partner
Real Estate Management	New authorization checks for Real Estate Management
Logistics-General	Changes in authorization checks for Sales Price Calculation
Quality Management	New authorization checks and PP/QM Master Recipe authorization checks
Plant Maintenance	New authorization checks
ArchiveLink	New authorization checks
All Modules	Authorization groups for output devices (printers, fax, etc.)

Chapter 1: R/3 System Security and the Authorization Concept

Contents

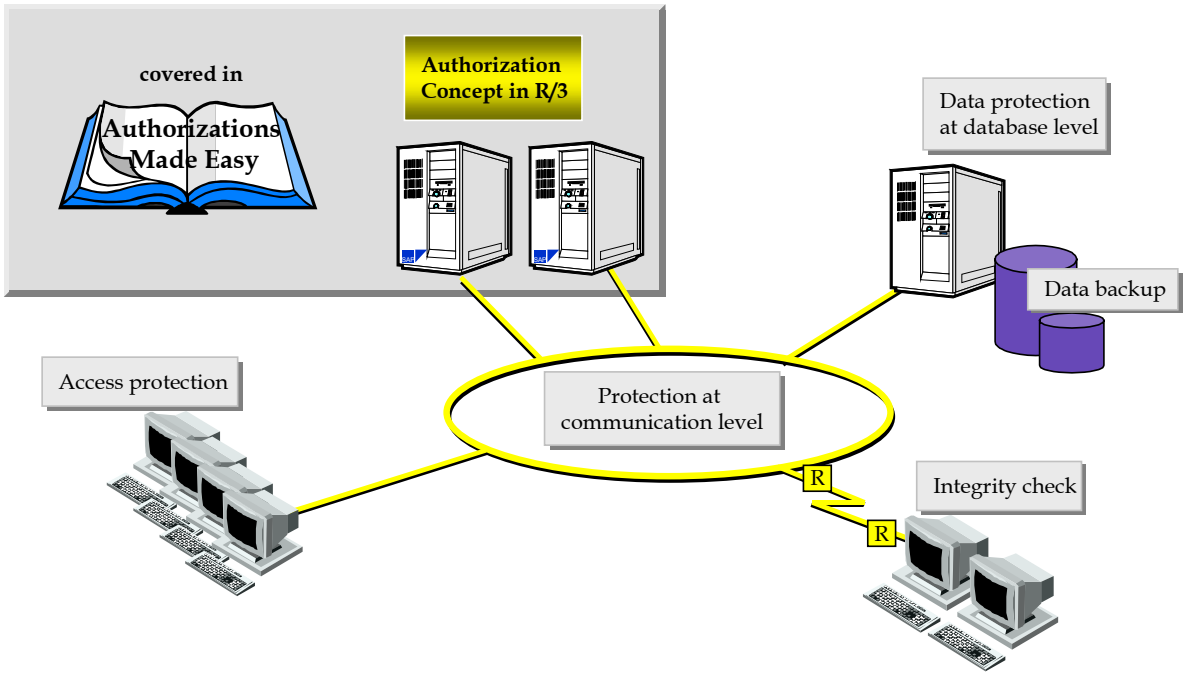
Overview

This chapter informs you about the R/3 authorization concept and an authorization design that meets requirements such as maximum security, sufficient privileges for end users to fulfill their job duties, and easy user maintenance. The authorization concept defines the functions to be carried out in various organizational units, by people in specific positions. The concept also provides a little more detail than the R/3 documentation about the authorizations and profiles required for the various enterprise areas.

Implementing a multilevel client/server environment over WANs provides great flexibility. But, in this environment, highly sensitive data and programs are at a greater risk of being lost, manipulated, and spied upon than in a conventional mainframe environment. Even with local operation, this risk applies to all three layers (Presentation, Application, and Database) and becomes even more acute than WANs.

The following graphic shows how R/3 covers the aspects of data protection and security:

R/3 Data Protection and Security



To meet the high demands of data protection and security, SAP provides the following R/3 security mechanisms:

- Access protection and authentication outside of R/3 (not discussed in this guide)
- Authorization concept (this guidebook discusses an authorization design using Profile Generator)
- Secure network communication (not discussed in this guide)
- Activity logging (not discussed in the guide)

Overview of the Authorization Concept

The concept of authorizations inside the R/3 System includes such things as:

- Profile Generator
- Locking and unlocking transactions
- Locked records
- Structural authorizations
- Data encryption
- Locking system for changes

The R/3 authorization concept permits the assignment of general and/or finely detailed user authorizations. These assignments can reach down to the transaction, field, and field value level. These authorizations are centrally administered in user master records and most allow the handling of certain R/3 components applicable to specific operations. Actions by a user may require several authorizations. For example, to change a material master record, authorizations are required for the:

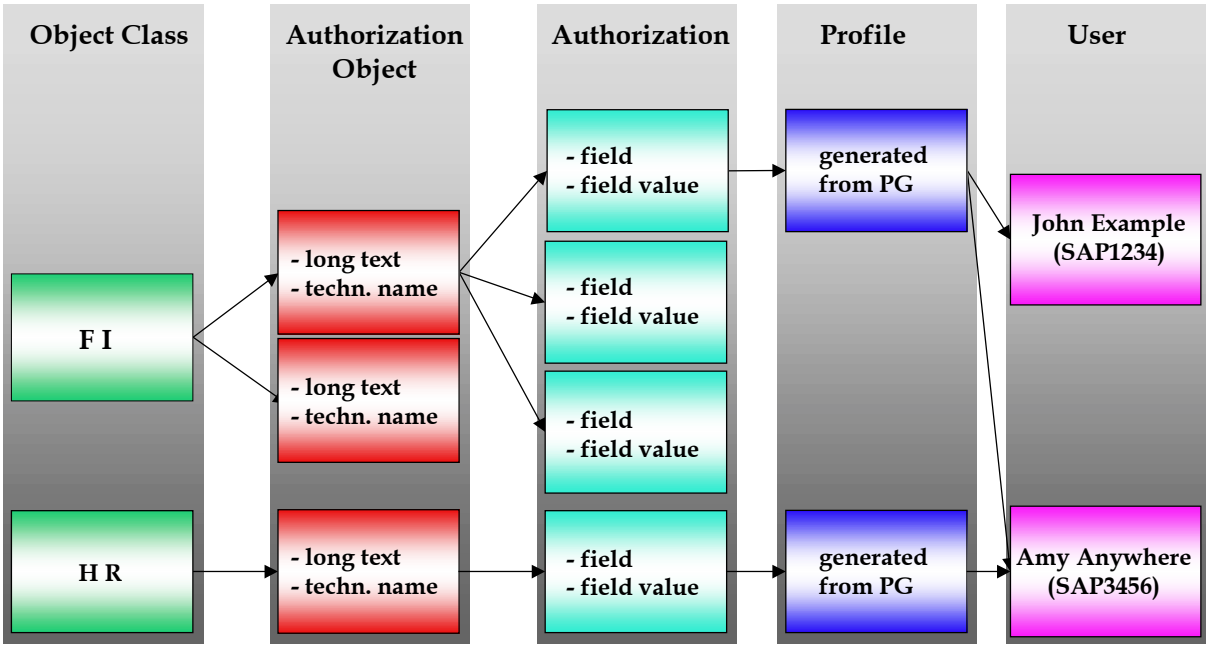
- Transaction "change"
- Specific material
- General authorization to work within the company code

The resulting relationships can become very complex. To meet these requirements, the R/3 authorization concept has been implemented as a form of pseudo-object-oriented concept with complete **authorization objects**. Each authorization object is a combination of authorization fields. An authorization always refers to an authorization object and can contain intervals for the field values. **Authorization checks** protect the functions or objects that you choose. Standard-delivered R/3 has these checks embedded in the program logic. Programmers have to decide which aspects of their programmed functionality should be checked and how the check should be conducted.

Authorization administrators create authorizations that are assigned to users in collections called **profiles**. The **Profile Generator (PG)** usually generates authorizations and authorization profiles, although authorizations can also be manually inserted into a profile.

The following graphic shows the authorization components and explains their relationship:

SAP Authorization Concept



Authorization Object

As you can see from the graphic "SAP Authorization Concept" above, objects allow complex user authorization checks. An authorization object works as a template for a to-be-defined authorization and contains a maximum of ten fields per object. Users may only conduct an activity if they satisfy the authorization check for each field in the authorization defined on a specific authorization object.

Authorization objects are grouped in an object class, such as Financial Accounting and Materials Management. Authorization objects can be created manually by choosing *Tools* → *ABAP/4 Workbench* → *Development* → *Other Tools* → *Authorization Objs.* → *Objects.* Because authorization objects are client independent objects that are defined in the ABAP Workbench, the Developers/Programmers/… are the ones that are most commonly responsible for creating new authorization objects.

Changes are necessary only if you "modify" your system and want to include AUTHORITY-CHECK calls or new authorization objects. You can only change or delete authorization objects added by your company. R/3 authorization objects may not be deleted or changed. If you wish to change an object, you must first delete all authorizations with which it is associated.

Authorization Object Fields

Authorization fields for an object can be created manually by choosing *Tools* → *ABAP/4 Development Workbench* → *Development* → *Other Tools* → *Authorization Objects* → *Fields.*

The fields in an authorization object are linked to data elements in the SAP ABAP Dictionary. The permissible values constitute an authorization. When an authorization check takes place, the system checks the values you have specified in an authorization

against those required to carry out the action. Users may only carry out the action if they satisfy the conditions for every field defined for a specific authorization object.

Using the authorization maintenance functions, define all authorization fields in the system development environment. Changes are necessary only if you "modify" your system and the new system elements are subjected to authorization checks.

Authorizations

An authorization allows you to carry out an R/3 task based on a set of field values in an authorization object. Each authorization refers to exactly one authorization object and defines the permitted value range for each authorization field of this authorization object. Authorizations are utilized in the user master record as profiles. By themselves, authorizations do not exist. They only have meaning inside a profile.

Field	Value
Customer type (CUSTTYPE)	*
Activity (ACTVT)	02

Explanation: * = all possible values; 02 = display

Authorizations are used to specify permitted values for the fields in an authorization object. There may be one or more values for each field. Authorizations allow you to determine the number of specific values or value ranges for a field. All values or empty fields can be permissible values. Changes affect all users whose authorization profile contains that authorization. The R/3 authorization administrator can maintain authorizations automatically, using the PG, or manually. Once the authorization is activated, changes affect all users which contain the profile with the activated authorization.

Once generated, authorizations and profiles created with the PG are automatically activated. If you manually create and maintain authorizations and profiles, you must also manually activate them. Generated profiles and authorizations cannot be maintained manually with the conventional maintenance transactions *SU02* and *SU03.*

Authorization Profiles

User authorizations are not directly assigned with the PG to the user master records. Instead, these authorizations are assigned as authorization profiles. The authorization administrator can create authorization profiles manually or automatically.

Single and composite profiles are possible, but, since the PG only generates single profiles, you must manually create composite profiles. By choosing, *Tools* → *Administration* → *User maintenance* → *Profiles*, the authorization administrator can manually maintain profiles or, with the PG, create profiles.

Changes affect all users to whom this profile is assigned and take effect only when the user logs on. Users who are logged on when the change takes place remain unaffected during their current session (see chapter 3 for additional information), but when they log on again, their profile will change accordingly. A user's authorizations are loaded into the user buffer only when they log on.

It is not possible to use the authorization profile maintenance transaction *SU02* to manually manipulate the PG-created authorization profiles. Although technically possible, never create a profile that contains partly manually created and partly generated authorizations or profiles.

User Master Records

Master Records enable the user to log on to the R/3 System and allow limited access to the functions and objects. The user administrator maintains user master records by choosing *Tools → Administration → User maintenance → Users.*

Authorization Checks

To conduct an authorization check, this check must be included in the transaction's source code. During the check, the system compares authorization profile values (assigned by the authorization administrator) to the values needed to carry out a program-specified action. A user may only carry out the action if the authorization check is successful for every field in the authorization object.

Authorization checks are triggered by the ABAP *AUTHORITY-CHECK* statement. The programmer specifies an authorization object and the required values for each authorization field. The *AUTHORITY-CHECK* then verifies if a user has authorization and if this authorization is from the user master record. The check is successful if an authorization is found that contains the values specified in the *AUTHORITY-CHECK*.

When R/3 transactions are conducted, since the transaction calls other work areas in the background, many authorization objects are often checked. For these checks to be successful, the user must have the appropriate authorizations. Authorization checks can be disabled by setting check indicators in transaction *SU24* or by switching off objects globally.

Activating and Deactivating Authorization Checks in Transactions

Most users receive more authorization than necessary, leading to an increased maintenance load. Authorization checks are conducted wherever they are written into a transaction's source code. Only by using the PG can check indicators be set to exclude:

- Certain authorization objects from authority checks
- Specific authorization checks in specific transactions
- An authorization object from being checked

All of these adjustments are possible without altering the program code. Prior to automatically generating the authorization profile, use the check indicators to control which objects appear in the PG and which field values are displayed. SAP delivers a default check

indicator setting with R/3. Please refer to chapter 2, the section *Reducing the Scope of Authorization Checks*.

SAP* and DDIC Users

During your R/3 installation, clients *000, 001,* and *066* are created. In clients *000* and *001,* two special users are defined, but no special user is created in client *066*. Since these users have standard names and passwords, you need to secure these users from unauthorized usage (the EarlyWatch and CPIC user are not covered in this book).

The two special R/3 users are:

- *SAP**

  Defined as the standard R/3 superuser, *SAP** does not require a user master record. Rather, it is:
  - Defined in the system code
  - Has a default password (**`PASS`**)
  - Has unlimited system access authorizations

  When you install R/3, a user master record is defined in clients *000* and *001* with the initial password **`06071992`**. *SAP** user master record deactivates *SAP**'s special properties. To prevent *SAP** misuse, change the password. We recommend, however, that you deactivate *SAP** and define your own superuser.
- *DDIC*

  This user is the maintenance user for the ABAP Dictionary and software logistics. The user master record for *DDIC* is automatically created in clients *000* and *001* and has the default password **`19920706`**. System code testing allows *DDIC* special privileges for certain operations. For example, *DDIC* is the only user that can log on during an upgrade. To prevent *DDIC* misuse, change the password.

Use report **`RSUSR003`** to check whether the standard *SAP** and *DDIC* passwords have been changed.

What Is the Profile Generator?

SAP's Profile Generator (PG) facilitates the authorization administrator's creation, generation, and assignment of authorization profiles. Released with 3.1G, this tool accelerates R/3 implementation by simplifying the task of setting up the authorization environment. The administrator needs only to configure the customer-specific settings; the PG manages other tasks, such as selecting the relevant authorization objects for consideration. The PG is fully integrated in R/3 and is available on all R/3-supported

platforms. The PG represents yet another improvement of SAP's tool-based support and a reduction in R/3 implementation time.

The PG is an approach to defining the authorization environment. The administrator no longer uses the authorization objects to define the authorizations for various user groups; instead, authorization profiles are built around the functions to be performed in R/3. Based on function selection, the PG selects the relevant authorization objects and groups them in a new authorization profile.

Using functions to define authorization profiles:

- Speeds up the process
- Defines authorization profiles
- Simplifies administrator/user communication, allowing both the administrator and users to use the same R/3 function terminology

To use the PG, you first have to set it up. Setting it up involves a three-step process that you only perform once:

- Setting the SAP R/3 system parameter correctly
- Using *SU25* to initialize the tables *USOBT_C* and *USOBX_C* (and then customizing them if desired)
- Creating and generating the company menu

For detailed information please read chapter 2.

Once the PG is set up, then you can work with it. However, before starting, it is good to understand its components.

The Components of the Profile Generator

The PG utilizes the following components:

Activity Groups

An activity group is a collection of R/3 transactions, authorizations, and additional objects. You can assign an activity group to as many users as you want. You can create, display, change, copy, and transport activity groups.

Derived Activity Groups

You can use an existing activity group as a reference when creating a new one. The system transfers the transactions in one activity group to a new activity group—one that remains dependent on the first. You can display the hierarchy of the activity groups that inherit transactions from each other by choosing *Activity group* → *Where-use list*.

With an activity group derived from a different activity group, you cannot enter transactions directly. You cannot reset the definition of the initial activity group from which the derived activity group inherited its transactions. Passing on transactions only refers to the menu selection and not to the authorizations. You must maintain authorizations separately in each activity group, these are not passed on. It is also possible to transfer the authorization data of the previous activity group to the derived activity group as a copy.

Company Menu

The company menu displays the menu options that exist in the activity group.

User Assignment

The users that you assign to an activity group may execute the transactions in the activity group with the corresponding authorizations.

In order to successfully create an activity group and assign it to a user, the following steps are involved:

1. Create an activity group and give it a name.
2. Select from the company menu which transaction codes this activity group is to have access to (this is not a required step). Alternative transaction codes can also be entered manually, without using the company menu.
3. Review, complete, or add the field values needed to the authorizations included in the activity group.
4. Assign the activity group to an appropriate user.

Generating the Profiles

Authorization profile definitions are based on the company menu, which is generated during the R/3 implementation and is intended to show only the R/3 functions (transaction codes) that are actually used by the customer. Each customer is responsible for generating its own company menu. From this menu, the administrator chooses the specific menu paths and functions for each user group. This selection describes the R/3 activities that users in each user group are authorized to perform. These initial configuration steps are also used in the Session Manager (please read chapter 4 for detailed information) to generate the user-specific menu.

Using the selected transaction codes, the PG determines the effected authorization objects. To simplify the creation of subsequent individual authorization profiles, R/3 contains default values for many authorization fields in specific authorization objects. For example, one possible access restriction might be the default value *Display*, limiting the user to display mode on certain transactions.

Additionally, the PG identifies the organizational levels that play a role in the extracted authorization objects and clearly displays these levels for the administrator. The authorization administrator may have to intervene and manually define the levels to which the users need access (for example, the company code).

The PG then places the specified levels in the authorization objects. At this point, a lot of authorization object fields for the new authorization profile have been filled, however there are still fields that need to be maintained. The authorization objects are displayed hierarchically in a special maintenance transaction. The administrator may fine-tune the remaining values, such as material type, order type, etc.

Within this maintenance transaction, the administrator can easily navigate from the overview screen to the lowest display level (the authorizations and their fields) and directly

assign the values. Generally, permissible values can also be assigned at higher levels. The following utilities to specify the values are available at every level of the hierarchical display:

- Value selection from lists
- Checkboxes for simple activity selection
- Delete and copy functions

If administrators determine that no further authorization restrictions are necessary on a certain level, by choosing a button, the PG fills in the remaining values.

Finally, another menu item in the system assigns the users to the R/3 functions. In this process, the PG automatically copies all the corresponding authorization profiles to the user master record. Of course, users can be assigned multiple selections, which means that certain general authorizations need to be maintained only once and are available for assignment to all system users.

Integrating the PG in R/3 also enables the administrator to access the documentation on every authorization object directly from the PG. Furthermore, the PG can list all R/3 functions that check a specific authorization.

Requirements and Availability

The PG runs on all supported platforms and has been available since Release 3.1G for general customer use. With Release 4.5 it is already activated for use.

What Is an Activity Group?

The process of security implementation with the new PG is based on the creation of activity groups or a collection of linked or associated activities, such as tasks, reports, and transactions. An activity group is a data container for the PG to generate authorization profiles and usually represents a job role in your company. (However, customers throughout the world often define activity groups somewhat differently. As such, there is no one concrete definition of an activity group, other than it is a data container for authorizations.)

For example, to implement security for a buyer:

1. Create the activity group, *Buyer.*
2. Include all of the business transactions *Buyer* can access.
3. Generate the appropriate authorization profile for *Buyer* by selecting the transactions a buyer would perform and by providing the authorizations that the transactions utilize with the appropriate values.
4. Assign *Buyer* to a new user or a position in your system.
5. Update the user master record for the user.

   The new user now has all the necessary access rights needed to work as a buyer in your company.

Activity groups are defined by the customer performing the implementation and allow systematic organization and efficient maintenance of system activities.

The SAP Session Manager, SAP Business Workflow, and Personnel Planning and Development are intricately linked with the PG. The SAP Session Manager uses the PG's company menu (which is the same menu used when an activity group's transactions are selected from a menu structure). SAP Business Workflow includes something called workflow tasks that can be linked to an activity group. Users assigned to have access to a particular activity group really come from the HR-Personnel Planning and Development Functionality. Furthermore, the plan version that is used in HR-Personnel Planning and Development is the same plan version used by the PG and Workflow.

Using an activity group as an information database reduces data entry time. Select the criteria, such as access rights, and divide the activities into appropriate groups. For example, you could decide to group activities by subject matter, such as personnel, payroll, or budgeting. Or, you could group activities by job classes, such as translation activities, computer programmer activities, or secretarial activities. You could also set up a combination of subject matter and job-oriented activity groups. Activity groups are created and maintained in the activity group maintenance transaction *PFCG* (the transaction for calling the PG). After setting up activity groups, you may assign them to various R/3 objects.

What Happened to Responsibilities?

If you have worked with the R/3 System in Release 4.0x or have read the 4.0B *Authorizations Made Easy* guidebook, then you may have wondered what happened to the functionality called "responsibilities." In Release 4.5, responsibilities were replaced by a concept called "derived activity groups" and these derived activity groups function a bit different from the 4.0 responsibilities. If you used responsibilities in 4.0 and upgrade to 4.5, your responsibilities are converted automatically into derived activity groups.

For detailed information on derived activity groups please see the corresponding section earlier this chapter and chapter 4.

Activity Group Assignments

An activity group can be assigned to many users. One user can also be assigned to many activity groups.

An activity group can be assigned to the following types of users:

- R/3 login user IDs

  An R/3 user is an individual who is recognized by the R/3 System and is allowed to log on. For the system to recognize users, their names must be entered in the user master record of the Basis component.

- Jobs

  A job represents a general classification of work duties, such as secretary, computer programmer, instructor, etc. Many employees in your company may hold the same job classification. (For example, there might be 20 people whose job is secretary.) Positions are usually based on jobs. Anyone who holds a job automatically inherits the infotype settings, attributes, and properties of that job. Unless the activity groups grants general access rights such as the rights needed to work with SAPoffice, be careful when assigning activity groups to jobs.

- Positions

  A position represents an employee's unique, individual assignment within a company (for example, marketing secretary, sales manager, etc.) Positions should not be confused with jobs. You can handle authorization management in an almost completely position-oriented fashion. All the access rights are then linked to the position, so it does not matter who fills this position. Once a user changes positions after the user master record is updated, the authorization profile automatically changes.

- Organizational units

  Organizational units represent any organizational entity that performs a specified set of functions within a company. For example, organizational units represent subsidiaries, divisions, departments, groups, special project teams, etc. Identify the organizational structure at your firm by creating organizational units and identifying the relationships among the units. Anyone who is assigned to an organizational unit automatically inherits the infotype settings, attributes, and properties of this organizational unit.

  Examples of units include:
  - Subsidiaries
  - Divisions
  - Departments
  - Groups
  - Special project teams

  Unless the activity groups grants general access rights, such as printing, be careful when assigning activity groups to organizational units. For example, if authority profiles tend to be fairly standard for all workers in an organizational unit, it may be most effective to assign activity groups and its profiles to organizational units. When exceptions occur for jobs or positions, create additional activity groups for them. If, however, authorities vary by job or position, it may be best to assign activity groups to the jobs or positions concerned. By creating organizational units and identifying the relationships between the units, you identify your company's organizational structure.

Purpose of Assigning Activity Groups to Objects

Depending on which part of the system you are working in, assigning activity groups to objects serves different purposes:

- Session Manager

  Activity assignments determine the system areas that users see when they log on.
- Business Workflow

  Activity assignments determine the tasks that users perform in the system. (For workflow users it is mandatory to include tasks in activity groups.)
- Human Resources (HR)

  Activity assignments serve as highly detailed object descriptions, such as job and position descriptions.

You can assign the same activity group to many different objects. Conversely, a single object can be associated with many different activity groups. The different activity groups assigned to an object are referred to as the object's **activity profile**.

The Big Picture: Successful and Secure R/3 Implementation

1: Schedule Everything

Make security an integral part of the R/3 project plan from the very beginning of the implementation by:

- Scheduling time to interview each application area
- Identifying requirements
- Documenting roles to help determine what an activity group will mean for your company's implementation of authorization components of the R/3 System.
- Constructing the authorization profile
- Testing
- Fixing discrepancies
- Implementing the system
- Transporting

Schedule time for post-upgrade activities, such as assessing security differences and upgrade profiles. R/3 security used to be one of the most underestimated tasks and was frequently addressed as a post-live activity.

2: Plan Ahead

Consider the following questions:

- What is your organization's security philosophy?
- What level of security does your data require?
- How much risk are you willing to assume in each application area?

The less risk your company assumes, the greater the resources needed to successfully implement R/3 security. These guidelines need to be established before the security implementation.

3: Organize a Security Team and Establish Business Liaisons

A team effort between the application areas (data owners) and the authorization administrator is the key to a successful implementation. Since the PG sets up the authorization environment, the HR department needs to be involved. If a user moves to a new position, this user needs to be assigned to a different activity group. With new employees or an employee leaving the company, the HR department knows when to inform the appropriate department and implement the corresponding security changes.

To build the appropriate activity groups and authorization profiles, authorization administrators need to know which R/3 menu paths and transactions each application area uses. If you plan to let end users log on to R/3 through the Session Manager, documenting those menu paths and transactions becomes even more important. Since the R/3 authorization concept is created from your enterprise-wide data hierarchy, authorization administrators need to know the corporate hierarchy.

For each transaction, the administrators must know which data users can work with and what access rights users have with regard to that data. By using the PG to set up security, activity groups can build the framework for R/3 access rights. The definition of the activity groups can then be shifted into the application areas where data owners are responsible for their job roles.

4: Communicate your Security Implementation Concept

Conduct a workshop with the authorization administrators and application areas (data owners) to review the R/3 authorization concept and its impact on data owners. The implementation framework should be explained, and later, staff from each application area should be interviewed.

5: Document Access Paths or Access Rights for Each Role

Each application area will have to supply roles or R/3 job descriptions to define activity groups. A role can be one, or a combination of many, tasks and activities.

For each application area, document the following:

- Different roles in a job role matrix
- Menu paths and transactions that end users will access

- Default values for organizational values
- Access restrictions to specific organizational levels
- Restrictions for access rights for each job role

End user training documents can be a part of this process. All necessary authorizations should be based on activity selection and the appropriate activity groups. Authorization profiles should be based on the supplied roles. The activity group, therefore, represents the corresponding job role as specifically as possible. Nevertheless, activities, such as printing rights, need to be in a separate activity group so that a user can have more than one assigned activity group at a time.

Two different approaches for documenting the job role matrix are the:

- Business process orientation
- Component orientation

See the following diagrams.

A Business Process Orientation

			Enterprise Job Role		BUYER		A/P CLERK
			Activity Group - Name - Long text	**Auth. Profile names**	**Z:Buyer01** **Buyer01** **Buyer01**	**Z:Buyerall** **Buyerall** **Buyer All**	**...**
Process ID	**Business Process**	**Procedure**	**Trans action**	**Default Org. Levels** **Menu path**	Division: 01 Sales Organization 0001 Distribution Channel: 01	Division: * Sales Organization * Distribution Channel: *	
1761	Material Determination		VB11	Logistics → SD → Master Data → Products → Matl Determination → Create	Only in Purchasing	Only in Purchasing	
		Create Master Record for Material Determination	VB11	Logistics → SD → Master Data → Products → Matl Determination → Create	Only in Purchasing	Only in Purchasing	
		Change/Delete Master Record for Material Determination	VB12	Logistics → SD → Master Data → Products → Matl Determination → Change	Change also for Sales Org. 0002 and Distrib. Ch. 02		
		Display Master Record for Material Determination	VB13	Logistics → SD → Master Data → Products → Matl Determination → Display	See all (*)		
1763	Condition Processing		V-41	Logistics → SD → Master Data → Pricing → Prices → Material Price → Create			
		Create Price Condition Record	VK11	Logistics → SD → Master Data → Pricing → Prices → Others → Create			
...							

A Component Orientation

			Enterprise Job Role		A/P Clerk		A/P Supervisor
			Activity Group – Name - Long text / Auth. Profile names		Activity Group A/PClerk01 Accounts Payable Clerk 01 / Auth. Profile Z:APCl01	Activity Group A/Pclerk02 Accounts Payable Clerk 02 / Auth. Profile Z:APCl02	...
Module	Area	Function	Trans action	Default Org. Levels / Menu path	Company Code: 0001 Business Area 0001 Account type: A,D	Division: 0001 Sales Organization 0002 Distribution Channel: A,D	
FI-A/P	Bank Accounts	Create	FI01	Accounting → Financial Accounting → Accounts Payable → Master records → Banks → Create	Only in Financial Accounting	Only in Financial Accounting	
FI-A/P	Bank Accounts	Change	FI02	Accounting → Financial Accounting → Accounts Payable → Master records → Banks → Change	Only in Financial Accounting	Only in Financial Accounting	
FI-A/P	Bank Accounts	Display	FI03/ FI04	Accounting → Financial Accounting → Accounts Payable → Master records → Banks → Display Accounting → Financial Accounting → Accounts Payable → Master records → Banks → Display changes	Only in Financial Accounting	Only in Financial Accounting	
FI-A/P	Bank Accounts	Delete	FI06	Accounting → Financial Accounting → Accounts Payable → Master records → Banks → Mark for deletion	Only in Financial Accounting	Only in Financial Accounting	
FI-A/P	Invoice Entry	Input and Post	FB10	Accounting → Financial Accounting → Accounts Payable → Master records → Iv/cr. mem. Fast entry		All Account types	
FI-A/P	Invoice Entry	Input and Post	F-43	Accounting → Financial Accounting → Accounts Payable → Document Entry → Invoice		All Account types	
...							

6: Review

Review the enterprise-wide job-role matrix before you build the activity groups. Determine the security options by creating a sample activity group for each job role and generating its authorization profile. Discuss the security options with the data owners in each application area. Application data owners need to be aware of the potential risks (such as excessive accesses) that result from their decisions.

7: Build Activity Groups and Generate Authorization Profiles

Remember your data hierarchy while postmaintaining open authorization fields. The R/3 authorization concept is based on your enterprise organizational structure. During the process of postmaintaining authorization profiles, ask whether you want to:

- See all data, change all data?
- See all data, change some data?
- See all data, change no data?

8: Assign Activity Groups to Users or PD Objects

Before testing the generated authorization profiles, you must first create test users. The new security approach requires that you assign each activity group a test user or, for example, position and manually update the user master. This way, the automatically generated authorization profiles is transferred into the corresponding user master record. If necessary, assign multiple activity groups.

9: Test

With the help of application area representatives, perform security unit testing for each created test user. The job role matrix can be used as the foundation for this test plan. Each role should be thoroughly tested before your go-live date. Be careful when testing roles in end-user training, because if a user's authorizations are missing, your entire training schedule may be delayed.

10: Use the R/3 Authorization Tools to Quickly Implement Security

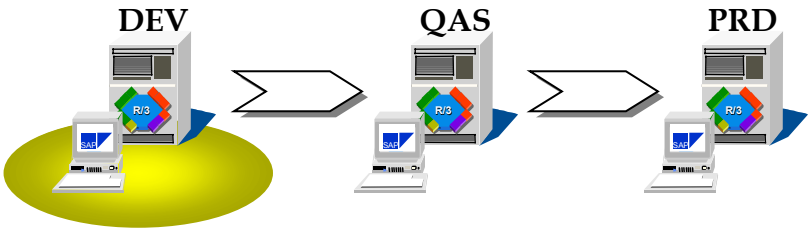
Many resources exist, in addition to this guidebook, from which you can obtain valuable information about security-related topics. We encourage you to review these other resources and use them with this guidebook.

The following table lists information sources concerning security implementation.

Information Source	Location
Overview of the most important *Online Service System notes*	Appendix A
FAQ (frequently asked questions)	Appendix B
Overview of system profile parameters	Appendix C
Library/Online Documentation	Choose *Help* → *R/3 library* → *Basis* → *Computer Center Management System* → *Users and Authorizations*
Release Information	Choose *Help* → *Release notes.*
R/3 Security Guide	Online Service System Note 39267
Report Documentation	Report documentation can be accessed from the selection screen by either choosing *Help* → *Extended Help* or *System* → *Services* → *Reporting*, entering the report name, and then selecting *Goto* → *Documentation.*
Glossary	Choose *Help* → *R/3 library* → *Glossary* for the entire glossary or choose *Help* → *Glossary* for a context-sensitive glossary.
Context-Sensitive Help	Move the cursor to a field or to a system message and press *F1.*
Knowledge Products	Online Service System note 61675
ABAP/4 Workbench Docuset	Online Service System note 60382
SAP*Net*	*SAPNet* is an internet service that brings new information and communication channels between SAP and its customers. Log on by entering *http://www.sap.com/* on an internet browser and click the *Partner Customer* button. Click *Frequent users* and enter your Online Service System password.
SAP Labs/ Simplification Group	Simplification Groups web page *http://www.saplabs.com/auth* for updates, beta releases of new guidebooks, additional information, predefined activity groups, guidebooks for previous releases, etc.
*Accelerated*SAP Roadmap (ASAP)	The ASAP Implementation Roadmap recommends using the PG in its authorization design proposal. You can also find links to this guidebook from different locations in the roadmap structure. Inside ASAP, choose *Implementation Roadmap* → *Phase 3: Realization* → *Establish Authorization Concept*.

Case Study: Security Strategy in a Three-System Environment

The Development System (DEV)



When the development system (DEV) is first installed, project members including configurators, developers, system administrators, and recent trainees comprise the bulk of R/3 users. We recommend the use of predefined activity groups (see chapter 10), which can be found on the attached CD or the Authorizations page of the Simplification Group *http://www.saplabs.com/auth*. As the R/3 project progresses, the need to limit user access increases. In general, DEV system users have more access than quality assurance (QAS) or production (PRD) system users.

As configuration is done in DEV you can now use the new functionality of customizing activity groups to ensure that people are configuring only their own part of the system. (Please read chapter 5 for detailed information on customizing authorizations.)

Treat superuser accounts like "root" in UNIX. The <*YourCompany*>*_ALL* profile limits risk on the DEV system. System malfunctions due to excessive access can also cause project development delays.

You now control who creates and maintains:

- Users
- Profiles
- Authorizations

You also eliminate attempts to:

- Lock transactions
- Delete user sessions
- Stop work processes

This control maintains the system's integrity and its stability. Using the PG, the authorization administrator develops end user profiles and authorizations in the DEV system. These profiles and authorizations will be transported to the QAS system for final testing before moving to PRD. The end user master records are usually created in PRD closer to the go-live date. The activity groups, together with the transported authorization data, are assigned to the end users as required in PRD. When you transport activity groups, this also transports the authorization profiles. These profiles do not need to be regenerated in the target system. However, you should compare the user master records when you import activity groups into the target system if users are already assigned. Please see chapter 12 for more information about transporting.

Maintaining documentation is also important because it:

- Helps future project rollouts proceed smoothly
- Is essential to pass security administrative functions to other project members
- Is required by auditors

The authorization administrator should work closely with the client copy administrators. When new clients are created, activity groups are not automatically copied. Since users, activity groups, authorization profiles, and authorizations are all client-dependent, the client copy administrator also needs to know which user master records to copy. Please see chapter 12 for more information about transporting.

The authorization administrator should also work closely with the change management administrators. Both administrators are important project control points. The system landscape, client landscape, and client roles should be clearly defined and presented to the project team. Development classes and authorization groups should be established for all new development. All administrators should complete SAP's training course *BC325 Software Logistics* (We recommend that you attend this workshop immediately after the initial installation of your R/3 System).

Next, these administrators should conduct a project-specific workshop to both review the system and client landscape and discuss the following control points:

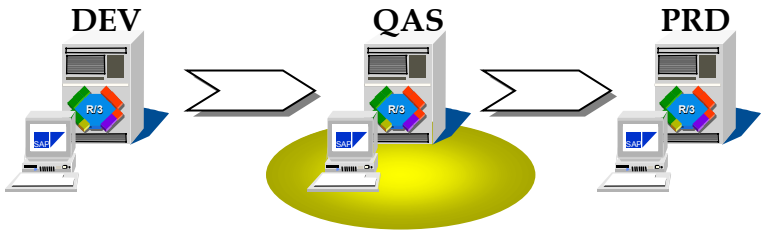
- When development requests will move
- To which clients these requests will move
- Whose signatures will be required along the way

The authorization administrator should work closely with the developers to enforce security standards for new ABAP programs and transactions, which can be enforced through Change Management. All new customer-written codes should be assigned to an authorization group, with transaction *SE38,* the ABAP editor attributes screen. Unprotected customer-written programs and transactions in PRD always present problems.

The authorization administrator should involve the corporate auditors at this juncture.

We recommend involving the corporate auditors up front so their requirements are incorporated in the development efforts. It is always unpleasant to audit post-live projects. In the worst case scenario, projects should be **halted** until auditor requirements are met, and at a minimum, all of the original development work may have to be revised.

The Quality Assurance System (QAS)



When the QAS system and client are created, the authorization administrator can start transporting the activity groups from the DEV system to the QAS system. Authorization profiles for imported activity groups no longer need to be regenerated, since the system can do this automatically now. Before moving the activity groups and authorization data to PRD, a final testing plan should be produced.

For example, an FI project team member may use a sample accounts payable user ID to:

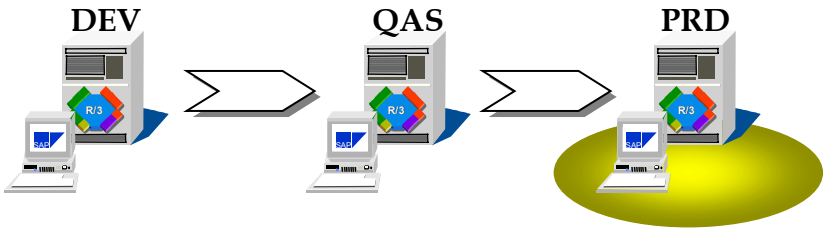
- Confirm that the user has access to the specific transactions governed by each activity group to which the user is assigned.
- Ensure that these transactions match the company-defined role for accounts payable.
- Verify that the sample user ID does not have access to unauthorized transactions.

Some sites conduct a day-in-the-life test as part of their go-live plan, where end users log on to a preproduction environment and simulate real production. This process is an excellent way of testing the generated authorization profiles.

The Training Client System (TRG)

While many customers do not put their training environment on another system entirely, many do. You need to set up the appropriate authorizations for the training system as well. The appropriate authorization setup cannot be determined without first knowing from where the data that appears in the training system comes from (or how the system and training client were created.) For example, if the training system is a copy of the production environment or a copy of the client where conversions and interfaces were initially tested, it may be possible that the training system contains sensitive information such as social security numbers, converted payroll information, addresses, etc.

The Production System (PRD)



Once the activity groups and authorization profiles have been fully tested in QAS, and end-user and project-team approval has been provided, these activity groups are moved to PRD. Actual end-user IDs can be created. A form that includes all of the pertinent information for user-ID creation, along with the proper signatures, is developed and distributed to the departments.

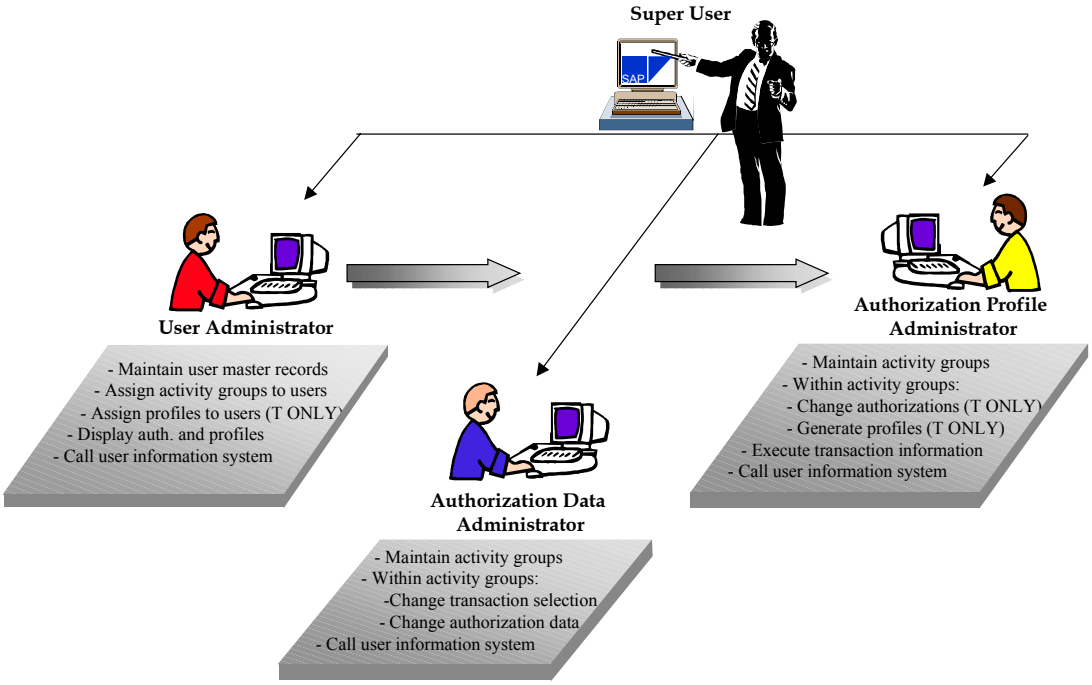
The authorization administrator should be a part of the go-live plan. The first days of going-live are hectic, and there should be a procedure to report access problems in production. The help desk is a good focal point. When users have access problems (for example, when users see the message: *No authorization for transaction XXXX*), they should execute transaction *SU53* to obtain the authorization required for this transaction. (Remember, since 3.1H, transaction *SU53* is also protected by object *S_TCODE*. See chapter 6, *Special cases*, for more details). A screen print should be sent to the help desk and the authorization administrator for evaluation. Once the application area owner approves the additional access, it is assigned to the user. Additional access means that the activity groups might be changed or that a missing authorization object may need to be manually inserted in the authorization profiles.

The authorization administrator should start planning for the other project phases. This may include other rollouts to different locations, different plants, different modules, or R/3 upgrades. All of these rollouts should involve the authorization administrator.

Authorization Administration Using the Profile Generator

If you are using the PG, you can divide the system administration tasks as shown in the graphic below to ensure greater system security. For larger companies or companies that have several people devoted to the authorizations component of R/3, this division makes sense. For smaller companies, dividing up such tasks complicates the process of creating and maintaining the authorizations component.

Organizing User and Authorization Maintenance Using the Profile Generator



You should also decide whether maintenance of users, activity groups, authorization profile, and authorizations should be centralized or decentralized. We recommend centralizing maintenance until your go-live date and first rollout. Centralized administrators have a better understanding of what is involved in a rollout, and centralizing the administrative tasks establishes naming standards. By the first rollout, all administrative functions should be documented and can then be decentralized.

Conversely, when the administrative functions are decentralized up front, administrators use different naming standards for their activity groups, authorization profiles, and authorizations, and different approaches to implementing security. If each administrator creates his or her own standards, everything has to be renamed once the authorization implementation is standardized.

The superuser sets up user master records, profiles, and authorizations for administrators in a department, a cost center, and other organizational units. Within an area, administrative tasks are divided between the user administrator, authorization data administrator, and authorization profile administrator. The following is a list of each administrator's tasks and responsibilities:

- User Administrator
  - Creating and changing users
  - Assigning users to activity groups
  - Assigning profiles beginning with *T* to users (or following your own naming convention)
  - Displaying authorizations and profiles
  - Working with the user information system (transaction *SUIM*)

  Displaying or changing activity group data and changing or generating profiles should **not** be permitted for user administrators.
- Authorization Data Administrator
  - Creating and changing activity groups
  - Changing the transaction selection and authorization data in activity groups
  - Working with the user information system (transaction *SUIM*)

  Changing users and generating profiles should **not** be permitted for authorization data administrators.
- Authorization Profile Administrator
  - Displaying activity groups and their data
  - Generating authorizations and authorization profiles beginning with *T* based on existing activity groups (or respectively following your own naming convention)
  - Working with the user information system (transaction *SUIM*)

  The following tasks should **not** be permitted for authorization profile administrators:
  - Changing users
  - Changing activity group data
  - Generating authorization profiles containing authorization objects beginning with S_USER

Setting Up Security Administrators

We have predefined the user, authorization data, and authorization profile administrators (chapter 10 describes how to import the PDAGs). After importing the appropriate activity groups for the administrators, follow the directions below. Since Release 3.1G, SAP has delivered three different templates for administrators to include in a profile (chapter 6 describes how to work with templates).

After importing the PDAGs, you should see the following activity groups in the activity group maintenance transaction *PFCG*:

Activity Group	Administration
S_Admin_Auth_Data	Authorization data administrator
S_Admin_Profile	Authorization profile administrator
S_Admin_User	User administrator

(Chapter 8 provides more information on assigning activity groups to users or PD objects. Log on to R/3 with these users.)

If you want to distribute the user maintenance tasks between several user administrators, you must assign the user to a user group. Only the administrator with authorization for that user group may change the master record. User administrators may change any user master record not assigned to a user group.

How the Three Administrators Work Together

The authorization data administrator:

- Creates an activity group
- Chooses transactions
- Maintains authorization data

Without the appropriate authorization to generate the profile, the authorization data administrator saves the profile and accepts the default profile name *T,* or a name that follows your naming convention.

The authorization profile administrator:

- Calls transaction **`PFCG`**
- Selects the *Display mode* to check the data
- Generates the authorization profiles

Finally, the user administrator assigns the activity group to a user or a PD object, such as a position, and updates the user master record. The authorization profile is then added to the user master record.

The profiles that are assigned to these administrators do **not** start with a *T*, and they themselves are only allowed to generate profiles that begin with a *T*. This is to ensure that they cannot assign themselves more authorizations than they are allowed to have. Also see Online Service System note *93769*.

Policies and Procedures

User Administration

Policies

- Superusers *SAP** and *DDIC*
  - There is no user *SAP** and *DDIC* in any client without a password.
  - The *SAP** user has no authorizations.
- User naming convention

  All users are assigned names identical to their employee ID numbers.
- User maintenance
  - The system administration department has to receive the *User Modification Request Form*, with e-mail, signed by the user's application department manager.
  - All profiles that the user requires must be specifically listed on the request form. The form must indicate whether the user is temporary or permanent.
  - For temporary employees, an account expiration date must be included.
- User leaving the company
  1. The *User Modification Request Form* must be filled out and signed by the application department manager.
  2. A copy of this form must be sent to HR department.
  3. The HR department manager must sign the request for deletion.
  4. This manager sends the signed copy back to the system administration department.
  5. All employee master record information, including internal post office, must be deleted.

Procedures

- Superusers *SAP** and *DDIC*
  - *SAP** is used only for client copies.
  - Pseudo superusers are created in each client with the *SAP_ALL* profile.
  - The password is changed every month.

    This can be determined with the following system profile parameters: *login/password_expiration_time* (see Appendix C for the list of system profile parameters).
  - Use report *RSUSR003* to check whether the standard passwords for *SAP** and *DDIC* have been changed from the defaults.
- User naming convention

  The application manager must contact the HR department and receive the new employee ID number. This ID number is entered into the *User Modification Request Form* where indicated.

- User maintenance

  The *User Modification Request Form* must be completed and mailed to the system administration department.

- User leaving the company

  The *User Modification Request Form* must be completed and sent to the system administration department and to the HR department manager. The HR department manager must sign the form and return the signed copy to the system administration department.

Roles and Responsibilities

Task	Role
Maintaining superusers	System administrator
Maintaining naming conventions	Application department manager/HR department
Maintaining users	Application department manager/system administrator
Maintaining users leaving company	Application department manager/system administrator/HR department

System Security

Policies

- IT Manager

  The IT Manager, who is responsible for all aspects of system security, must review the security strategy every two months.

- Superusers

  For revision and security purposes, the superuser *SAP** will not be used for system maintenance. All maintenance has to be performed with newly defined superusers.

- System passwords

  System passwords (DB user *sapr3*, O.S. user <*SID*>*ADM, DDIC*) must be changed every four weeks. In case of an emergency, password access must be ensured.

- User passwords

  To protect the system from unauthorized access, make users change their password every four weeks. A minimum password length of six characters is required. After three unsuccessful logon attempts the account will be locked.

- SAP connection

  The connection to SAP is opened only for a service session. These connections are *Online Service System, Early Watch,* and *Remote Consulting*. Connection to SAP can only be

opened from the customer site. Connections have to be monitored with an appropriate tool.

- SAProuter

  SAProuter, a SAP-supplied tool for securing R/3 access, is necessary for connecting to SAP systems.

- Remote connections

  For external connections (mobile end users), fixed IP addresses are assigned. One explicit entry per external connection is maintained in the permission list for SAProuter.

Procedures

- IT manager

  Every two months, the IT manager and the system administrator should review system security.

- Superusers

  The *SAP_ALL* profile is removed from the user *SAP**, and the *SAP** user is locked. All maintenance tasks are performed using accounts with the *SAP_ALL* profile.

- System passwords

  The system administrator changes the system passwords every four weeks. The system administrator must write down the current passwords and place them in a sealed envelope, which must be stored in the data safe and be accessible in case of emergency. Use report *RSUSR003* to check if system passwords have been changed.

- User passwords

  Users must change their passwords every four weeks by setting the appropriate parameters in the *DEFAULT* profile. This step ensures that the settings are valid in the entire system. The minimum number of characters for a password is six, and the intruder-lockout count is set to three.

- SAP connection

  A connection between SAP and the customer is established by starting SAProuter in the customer network and starting, for example, SAPgui for an Online Service System connection.

- SAProuter

  SAProuter is started and stopped once a day to ensure there are no open connections.

- Remote connections

  For remote users, dedicated IP addresses are maintained. These addresses must also be maintained in the *SAPROUTTAB* to make sure that unauthorized users do not log on to R/3.

Roles and Responsibilities

Task	Role
Defining and maintaining *SAPROUTTAB*	System administrator
Monitoring open connections	Operator
Shutdown/restart SAProuter daily	Operator
Review security strategy	IT manager
Changing system passwords	System administrator

Auditing Requirements

In R/3 there are several areas related to auditing:

- Process controls
- Change management
- Authorization implementation
- UNIX
- Database

Your site may have additional auditing requirements. Numerous companies have implemented excellent auditing procedures based on standard SAP tools and customer-built tools. Americas' SAP Users' Group (ASUG) Internal Controls and Audits offers the best information on how other companies have handled auditing in R/3. For more information, on ASUG see *http://www.asug.com/*. With ASUG's input, SAP has developed the Audit Information System.

Naming Convention for Authorization Profiles

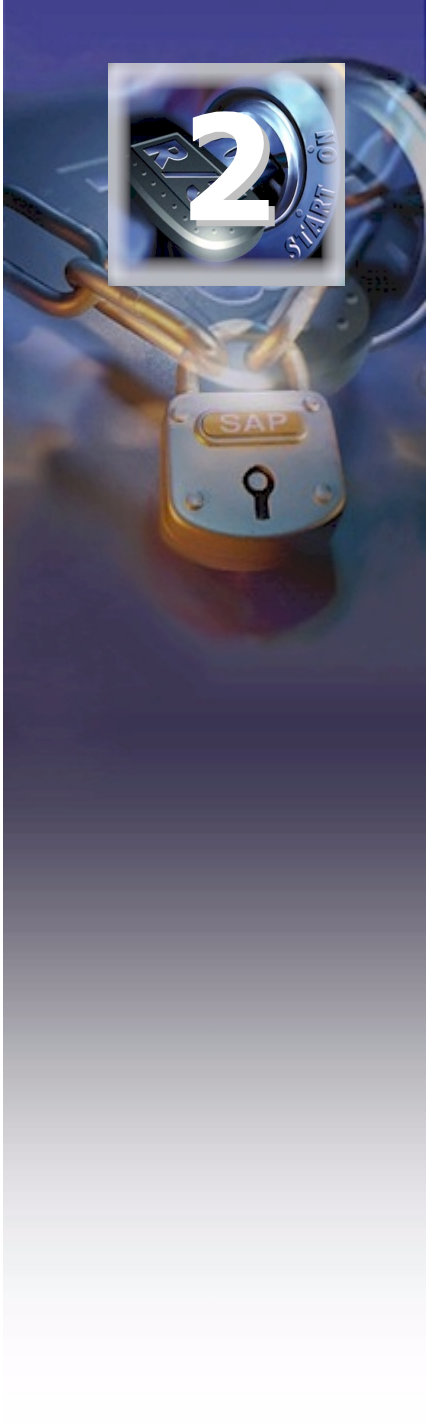
To name an authorization profile, use profile names that do not begin with *T*. Authorization profiles beginning with a *T* may contain critical (*S_USER**) authorization objects. Also, use the PG to exclude further authorization objects (for example, HR data) from the profile.

Note: We are talking about authorization profiles **not** activity groups.

When you first save the authorization profiles, you are prompted to enter a profile name. The system proposes a name for the profile; however, only the first 10 characters (the profile torso) can be freely assigned. The number of profiles generated depends on the number of authorizations in each activity group. A maximum of 150 authorizations fit into a profile. If there are more than 150 authorizations, an additional profile is generated. It has the same 10-character torso as the profile name, and the last two digits (positions 11 and 12) are used as a counter.

To avoid conflicts between customer-defined profiles and those profiles supplied by SAP, you should not use any name that has an underscore in the second position. SAP places no other restrictions on the naming of authorization profiles (refer to Online Service System note 16466). Therefore, if your company has its own naming conventions, you are allowed to overwrite the proposed name. We recommend that you use the proposed T-profile name.

The names of the authorizations are also derived from the profile torso. When more than one authorization is required for an object, the last two places are used as a counter. Based on the name for the authorization profile, the technical names for the authorizations to be created start with a *T* and comprise the internal number of the activity group and two end digits in the range 00–99. (*T-5000031800* is a sample authorization name.)



Chapter 2: Setting Up the Profile Generator

Contents

Overview

Using the Profile Generator (PG) in Releases 4.5A and 4.5B makes sense for both new customers who are just starting their R/3 project and for current customers who have already created authorization profiles with an earlier R/3 release. Maintenance transactions *SU02* and *SU03* are no longer required, and customers who have previously been using this method, should familiarize themselves with the PG. If you have already created authorization profiles without the PG, SAP offers you a way to migrate these profiles to the PG.

Regardless of which R/3 release you use, SAP would appreciate your feedback on the PG. Please fill out the evaluation form that came with this guidebook.

For information on upgrades, see chapter 14.

When to Use the Profile Generator

PG users must work with R/3 Release 3.1G or higher because SAP fully supports its use in these releases. Furthermore, SAP recommends the use of PG in these releases.

Activating the Profile Generator

In R/3 Release 4.5A and 4.5B, the Profile Generator is already activated. You do not have to set the system parameter in the R/3 instance profile. The default value is *auth/no_check_in_some_cases* = *Y*.

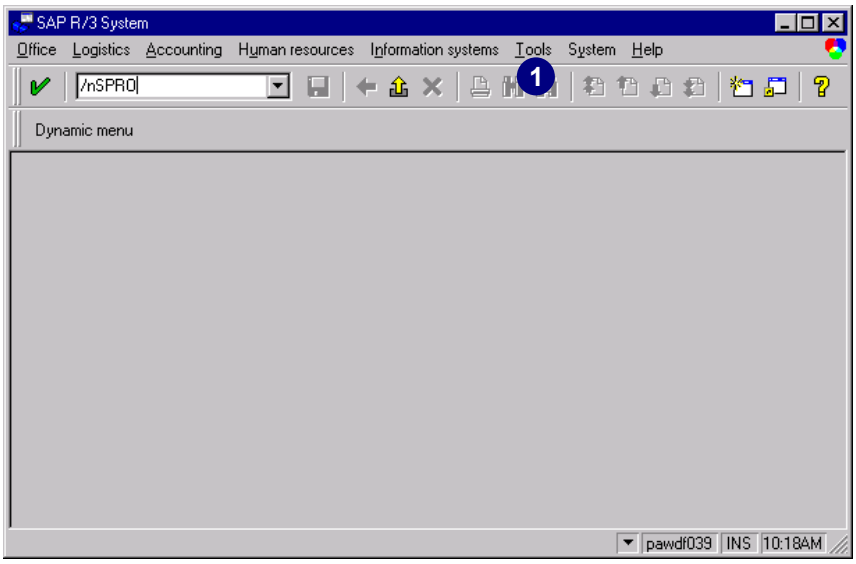
If this parameter is not present in your profile, you may have to continue with the following procedure.

The SAP standard menu and the company menu must first be generated, before you can work with either the activity group maintenance transaction *PFCG* (PG transaction) or the Session Manager.

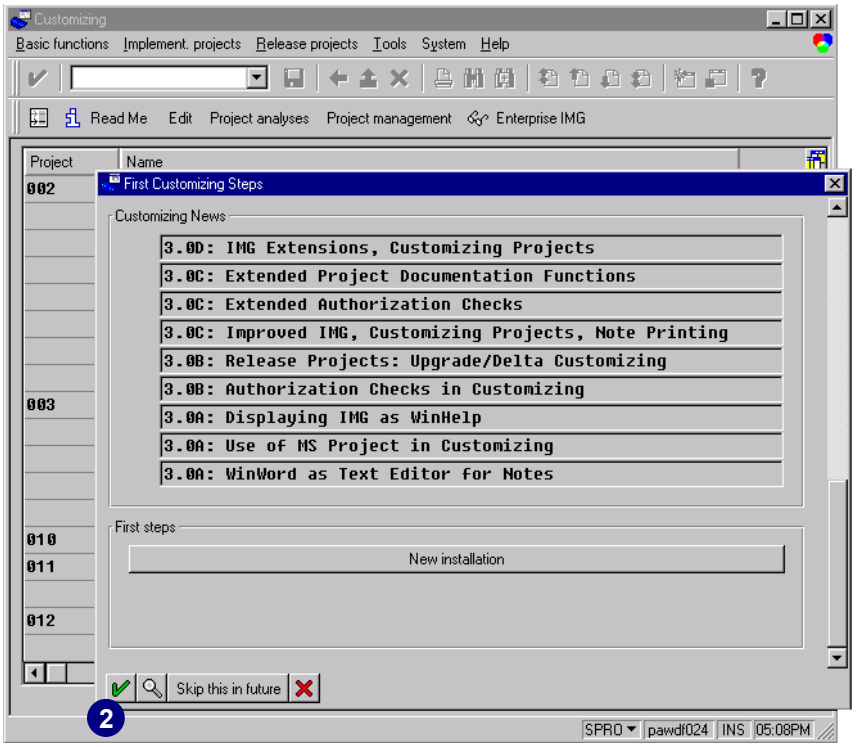
The Enterprise IMG must be generated during customizing **before** the first generation of the company menu, because this menu is based on the application components chosen in the Enterprise IMG.

Displaying the Enterprise IMG

1. In the *Command* field, enter transaction **SPRO** and choose *Enter* (or choose *Tools* → *Business Engineer* → *Customizing*).

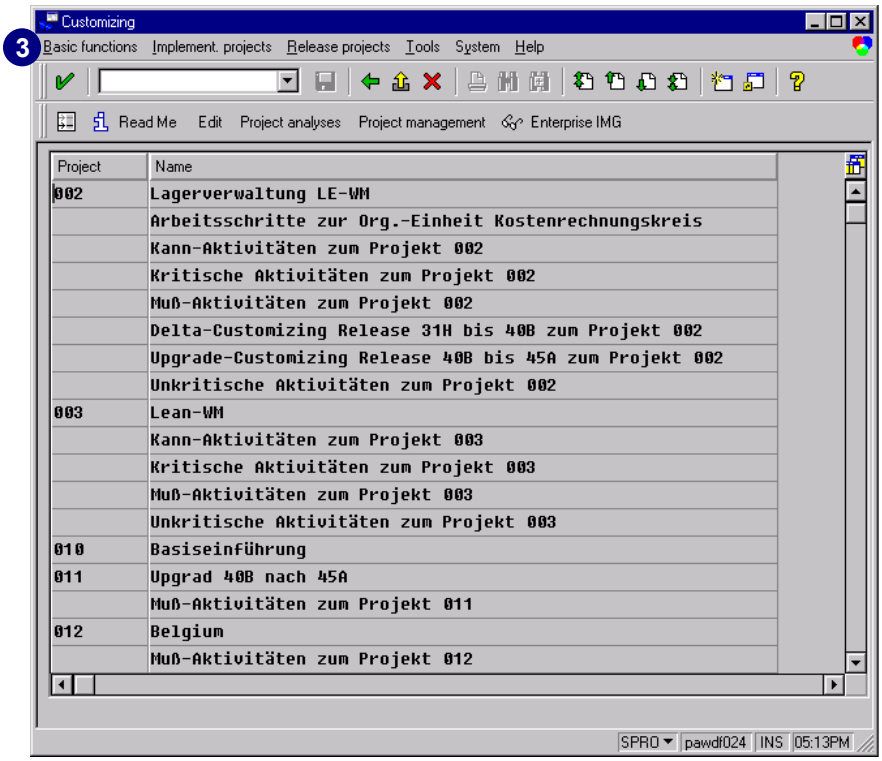


2. Choose *Enter*.

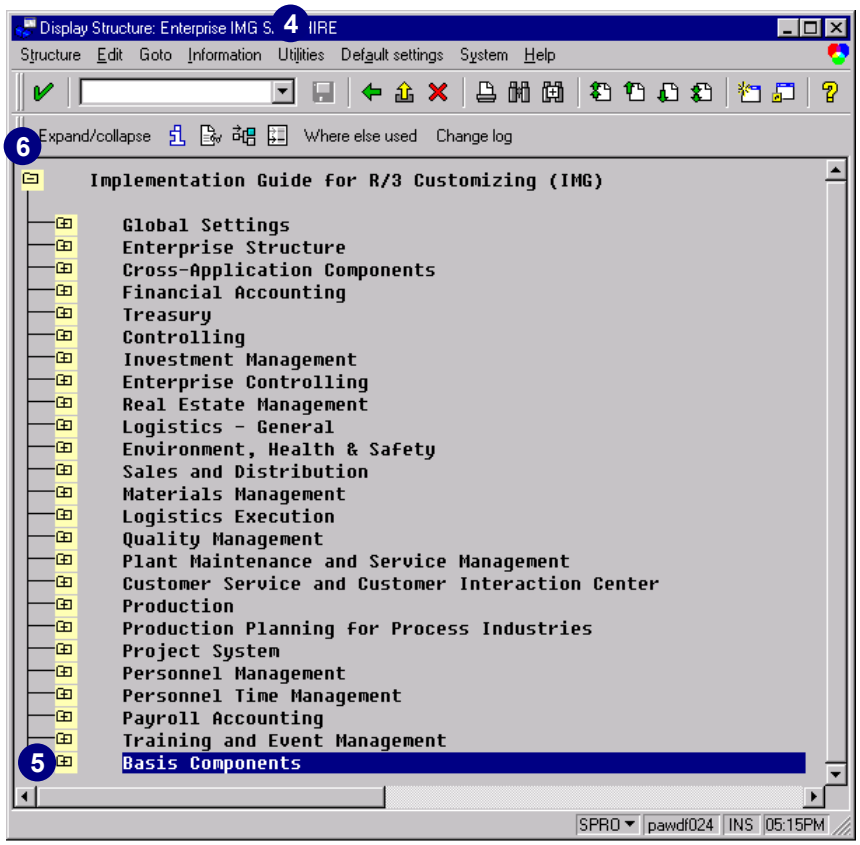


Before you proceed, generate the Enterprise IMG if you have not already done so.

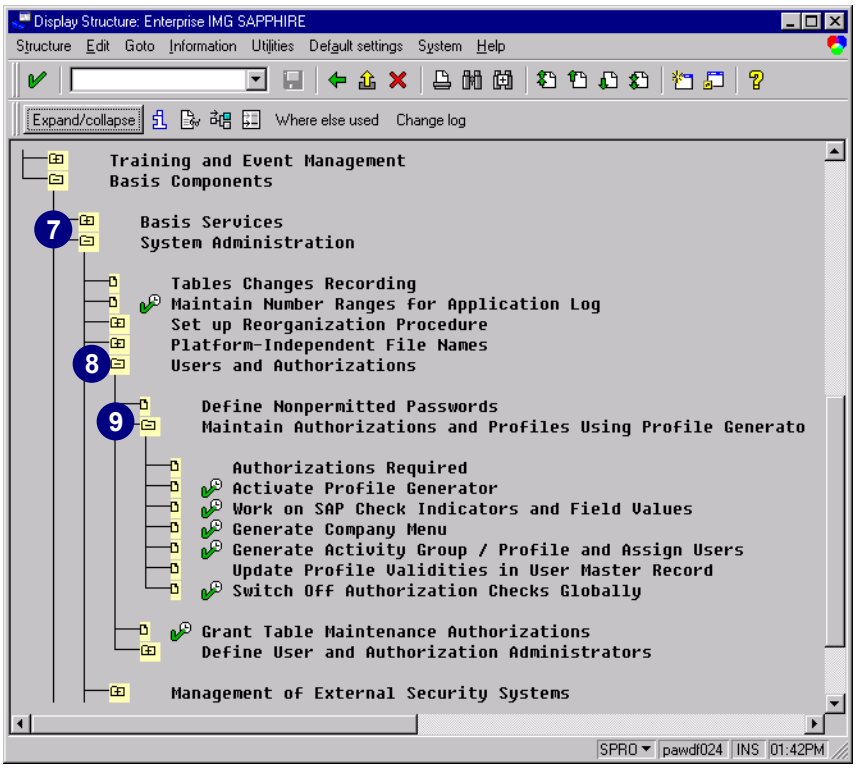
3. From this screen, choose *Basis functions* → *Enterprise IMG* → *Display*.



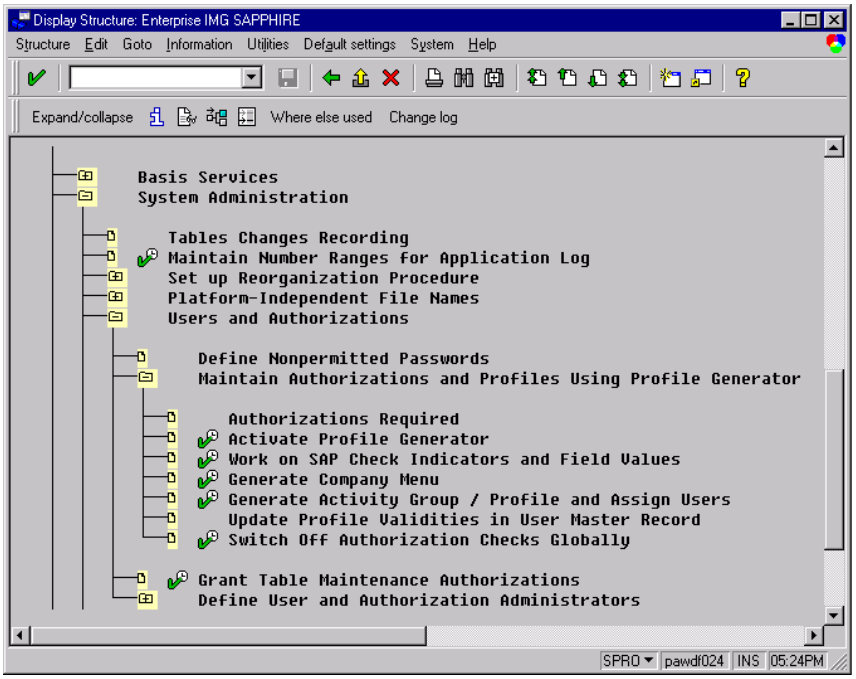
4. This sample Enterprise IMG may differ from your Enterprise IMG.
5. Position the cursor on *Basis Components*.
6. Choose *Expand/collapse,* or double-click the node for *Basis Components*.



7. Expand *System Administration*.
8. Expand *Users and Authorizations*.
9. Expand *Maintain Authorizations and Profiles Using Profile Generator*.



This screen will be our starting point for further activities in this chapter.



Setting the Required Instance Profile Parameter

First, activate the PG and permit the SAP-specified authorization checks to be switched off. To do this, you need to set the following system parameter in the R/3 instance profile:

`auth/no_check_in_some_cases` = **`Y`** (default value).

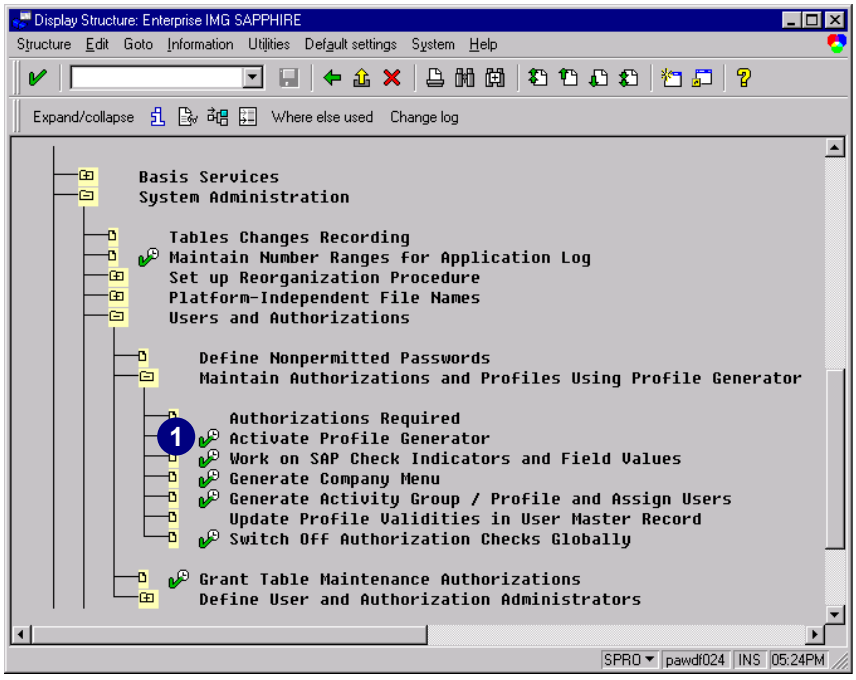
When a transaction is called, the system checks to see if that transaction's authorization checks should be suppressed. If the PG is activated, the *Change authorization data* button in the activity group maintenance transaction *PFCG* is displayed. When you use transaction *RZ10* to modify profile parameters, the changes do not immediately take effect in the associated R/3 instance because the characteristics of an instance cannot be changed during active operation. You must stop and restart the respective R/3 instance(s) for the profile change to become effective. We recommend that your R/3 system administrator handle this task for you.

If you have installed R/3 Release 4.5 as a new system, you do not have to set up the profile parameter, since it is already configured. You can continue with *Running the RSPARAM Report and Checking the Instance Profile Parameter* on page 2–13.

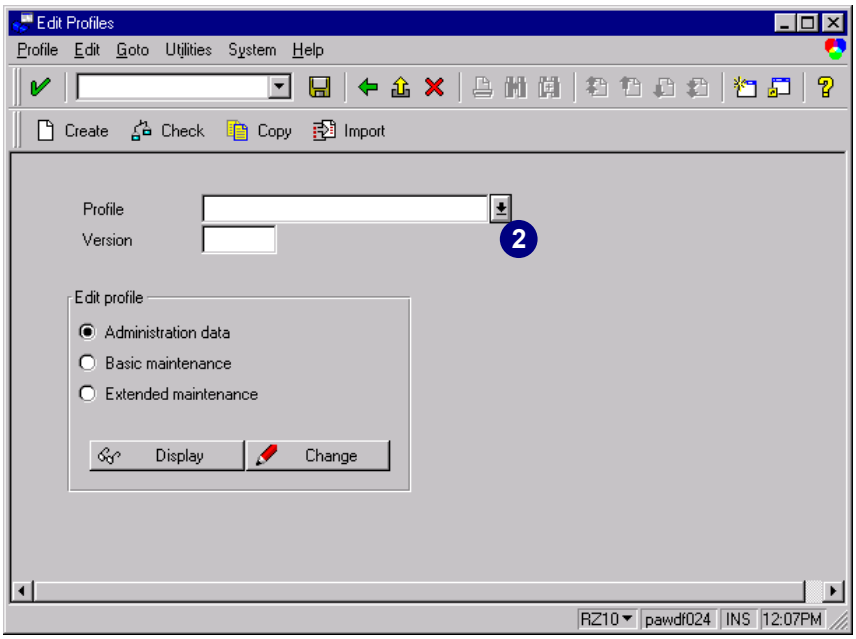
If you upgrade to 4.5 from an older R/3 version you need to proceed with the following procedure to set up the profile parameter.

To create the required profile parameter with transaction **`RZ10`**:

1. In the *Command* field, enter **`RZ10`** and choose *Enter* (or choose *Execute* next to *Activate Profile Generator*).



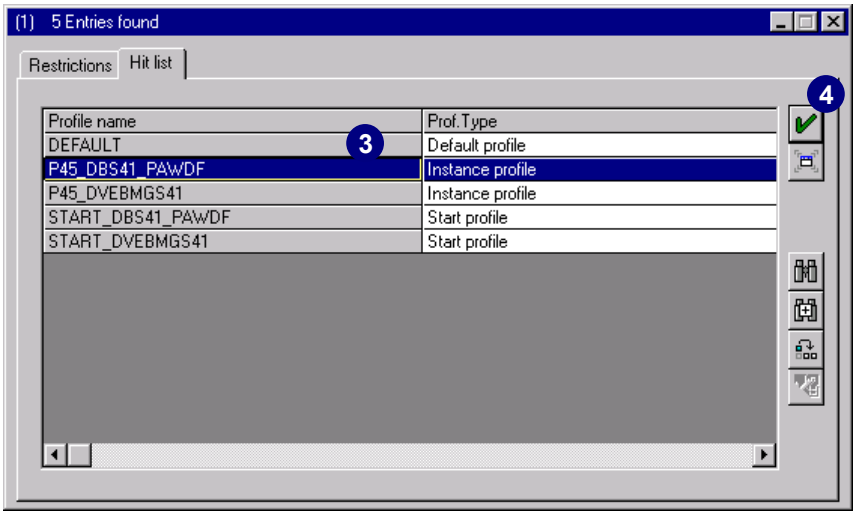
2. Choose *possible entries* for *Profile*.



3. Position the cursor on the correct profile name. The corresponding profile type (*Prof. Type*) must be *Instance profile*.

   The parameter will not work with the *Default profile* or the *Start profile*.

4. Choose *Enter*.



If no instance profiles are listed, these instance profiles are automatically generated or updated at the operating system level when you:

- First install R/3
- Upgrade to a new R/3 release
- Add a new application server

Unfortunately, the installation program cannot save these profiles directly to the database. Before the profiles can be edited, you must use the profile maintenance transaction *RZ10* to import the R/3 instance profiles file.

Two Ways to Import the R/3 Instance Profile File

- When importing R/3 profiles from all active application servers (mass import):

  1. Import the R/3 profiles after installing your R/3 System or a new R/3 release.
  2. Make sure all application servers (instances) are active.
  3. In the basic profile maintenance screen, choose *Utilities* → *Import profiles* → *Of active servers*.

  The default profile and all start and instance profiles used by the SAP instances are imported. The profiles are then checked, and a log is displayed. The names of the profiles in the database are taken from the corresponding filenames on the operating system.

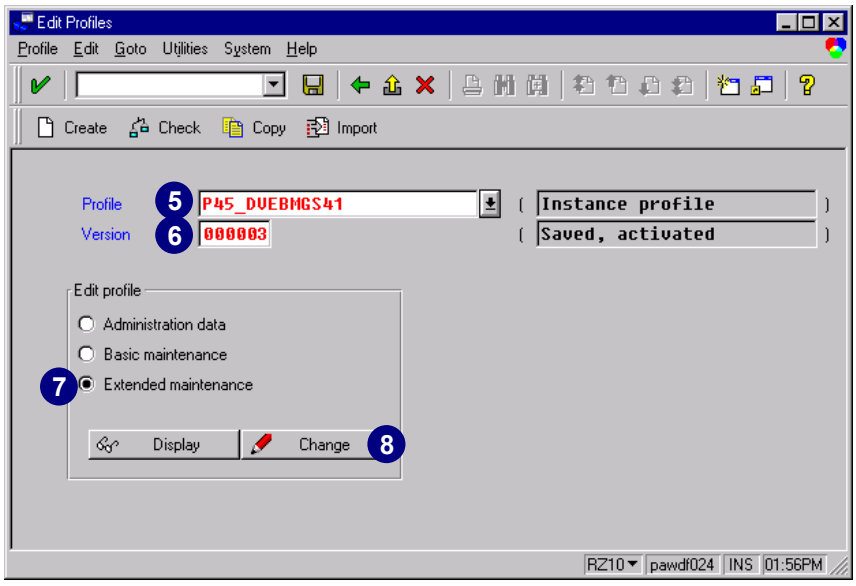
- Importing individual profiles

  This function should be used if a new application server has been installed or a profile was modified at the operating system level.

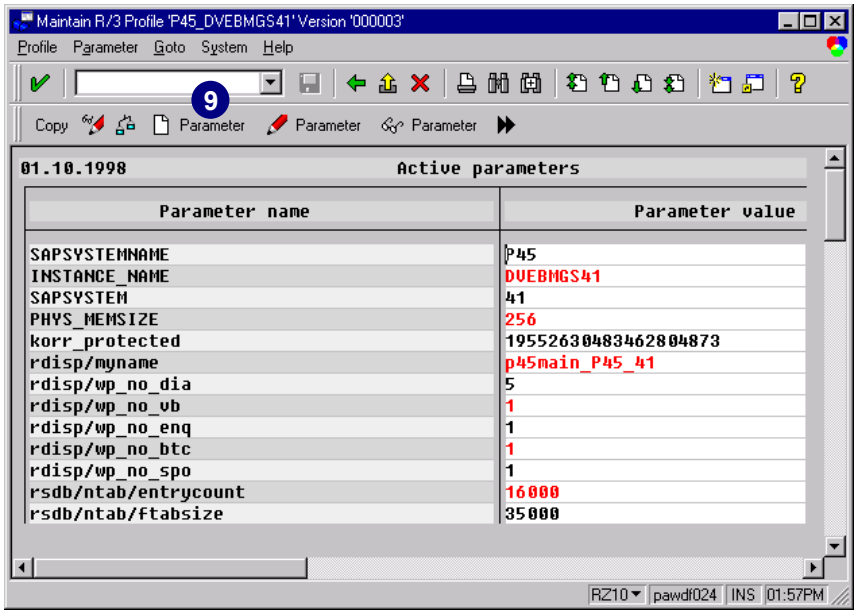
  1. You must first create a new profile using the profile maintenance function.
  2. Enter the profile name (the version number is generated automatically). The profile type and status appear on the screen for your information.
  3. Choose *Profile* → *Create*.
  4. To maintain the administration data, enter data in *Short description* and enter the file name where the profile will be activated (in *Activation in operating system file*). You must specify a reference server and profile type.
  5. Once the administration data has been transferred, choose the function *Profile* → *Import* in the *Basic maintenance* transaction screen.
  6. In the subsequent dialog box, specify into which operating system file the profile should be imported. You can display all the profile files from the global profile directory by pressing *F4*.

  The imported profile is checked for any errors. You may now edit or import the profile into the database. After the import process has been completed, you may activate the profile.

5. The profile name automatically appears in the *Profile* field.
6. The system automatically chooses the latest saved and activated version.
7. Select *Extended maintenance*.
8. Choose *Change*.



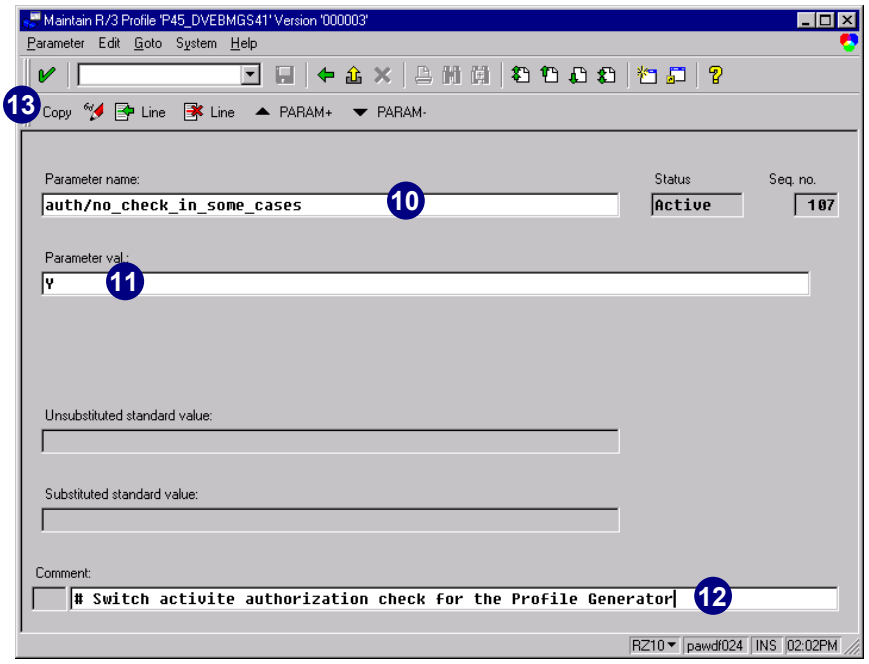
9. Choose *Create Parameter*.

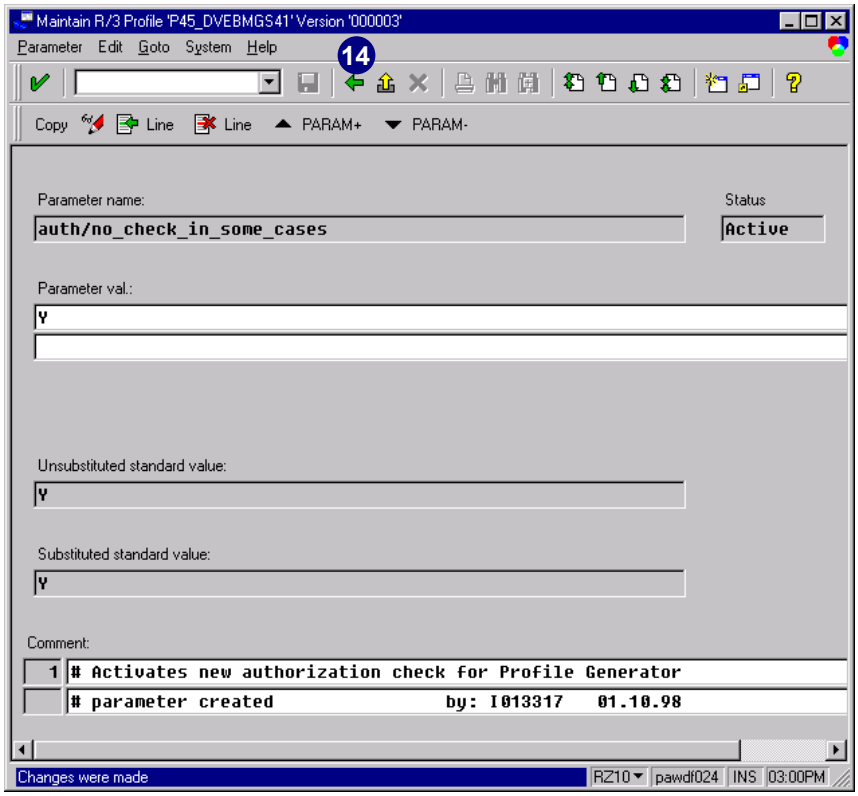


10. Enter in *Parameter name* **`auth/no_check_in_some_cases`**.
11. Enter the parameter value **`Y`** in *Parameter val.*

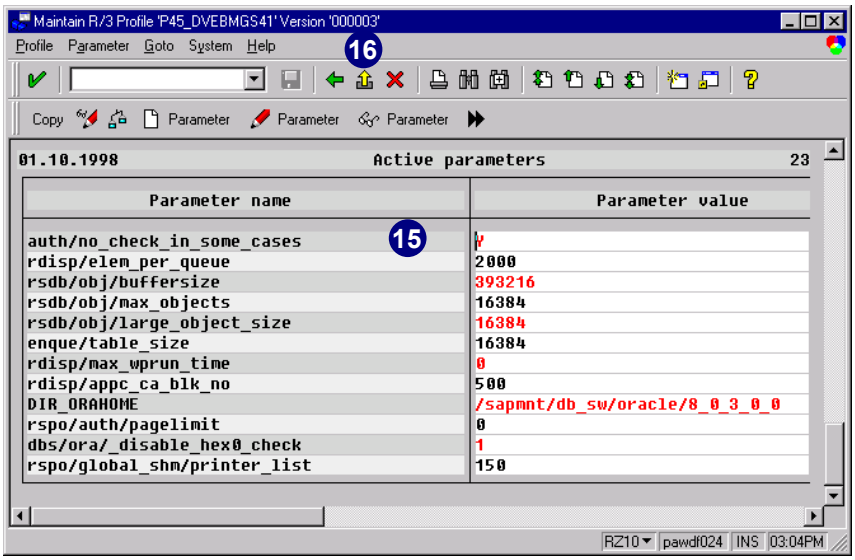
Since the *Parameter val.* field is case-sensitive, make sure you enter a capital **`Y`**.

12. Enter your comment in *Comment*. Your text must be preceded by the number sign (#).
13. Choose *Copy* twice.
14. Changes have now been made, so choose *Back*.

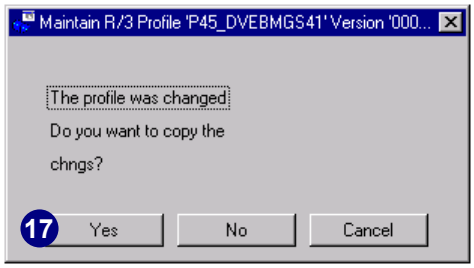




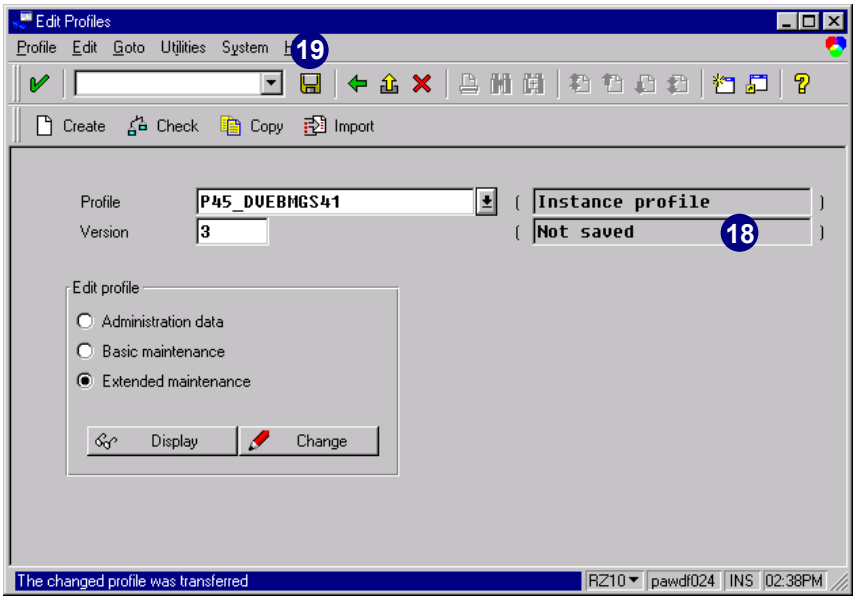
15. You can now see the new profile parameter in the list.
16. Choose *Back*.



17. Choose *Yes*.

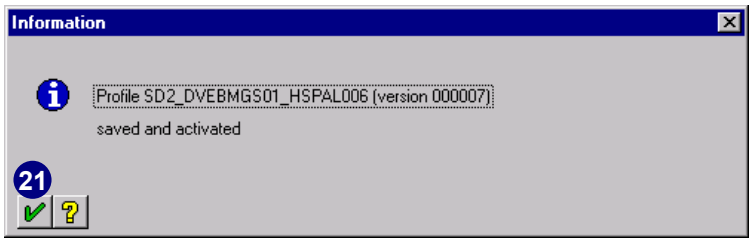


18. Notice that the changed instance profile has not yet been saved.
19. Choose *Save*.



20. Choose *Yes*.

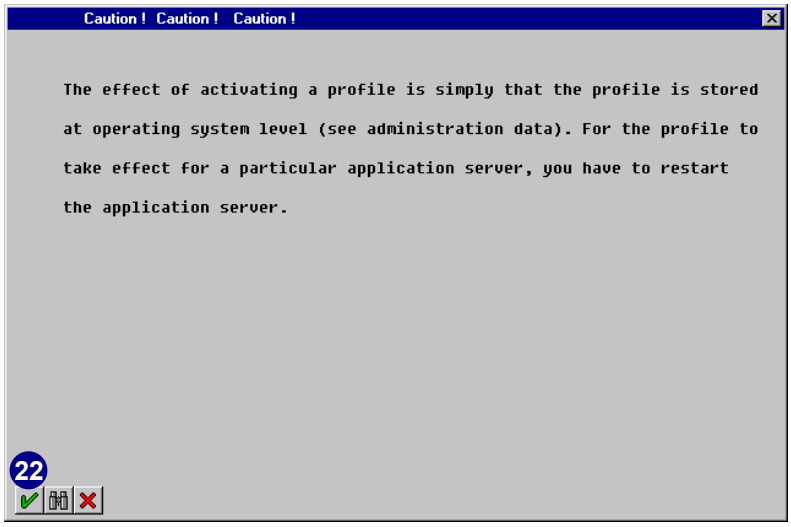
The *Information* dialog box tells you that the chosen instance profile has been saved and activated. The new version number is automatically generated.



21. Choose *Enter*.

When you modify profile parameters using transaction *RZ10*, the changes do not immediately take effect in the associated R/3 instance.

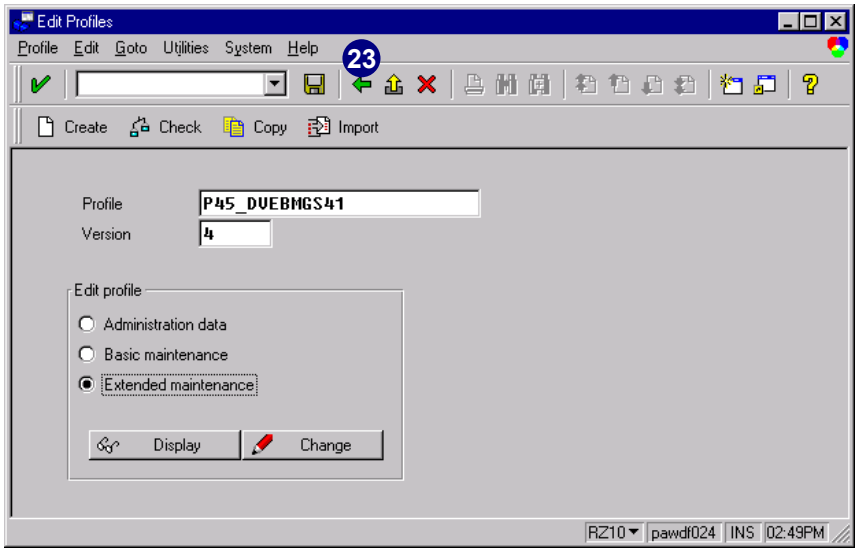
The characteristics of an R/3 instance cannot be changed during active operation. This caution dialog box tells you to restart the R/3 instance for the change to take effect.



22. Choose *Enter*.

23. Choose *Back*.

You may continue with the next section.

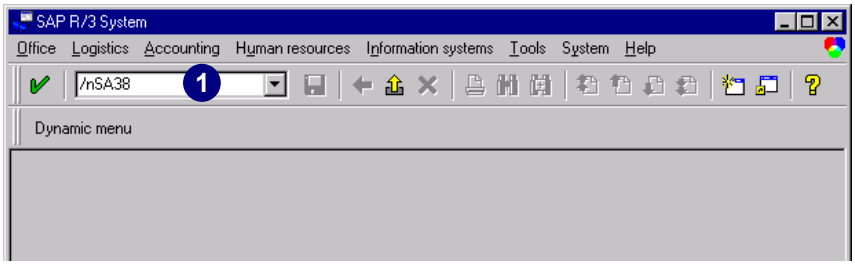


Stop and restart the designated R/3 instance(s) now. An existing active profile is automatically backed up. A backup file is created with the extension *.bak*. Even if R/3 is unavailable, you can copy and display this backup file.

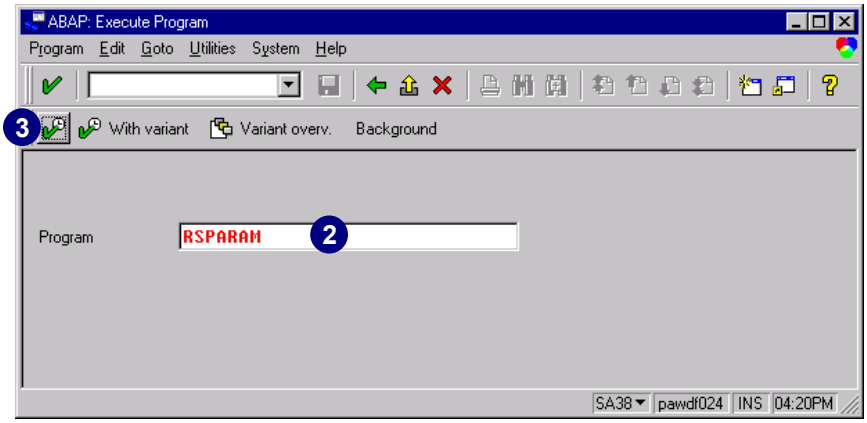
Running the RSPARAM Report and Checking the Instance Profile Parameter

Before you can continue with the rest of the general preparations for the PG, you must verify whether the instance profile parameter you set is currently active. Use the ABAP program *RSPARAM* to find out which parameters are active for a particular SAP instance:

1. In the *Command* field, enter **`SA38`** and choose *Enter* (or choose *System* → *Services* → *Reporting*).

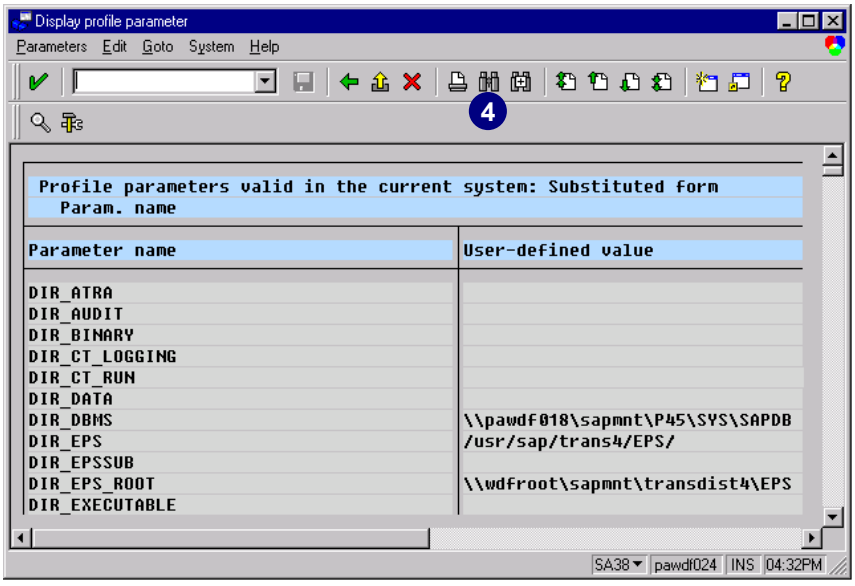


2. Enter **`RSPARAM`** in the *Program* field.
3. Choose *Execute*.

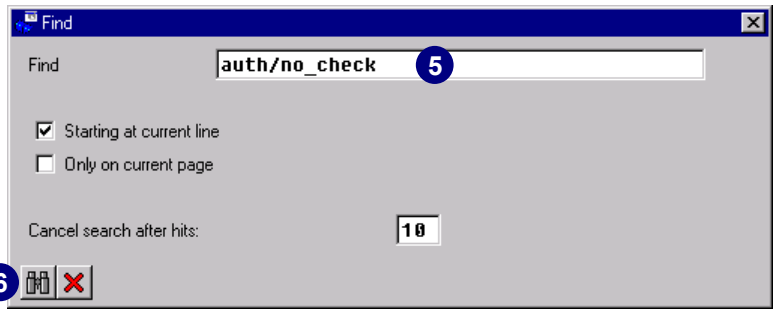


A list of parameter names appears with corresponding user-defined values. The parameter names are provided in variable form. At run-time, these variables were replaced with actual values. User-defined values are the actual values of the individual parameters.

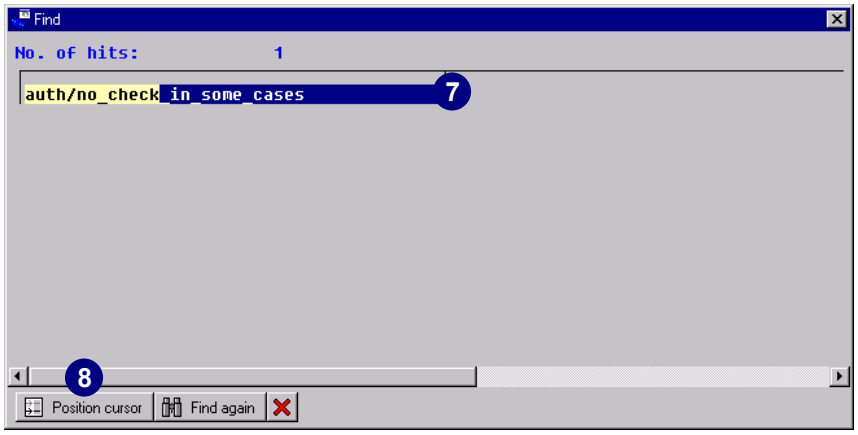
4. Choose *Find*.



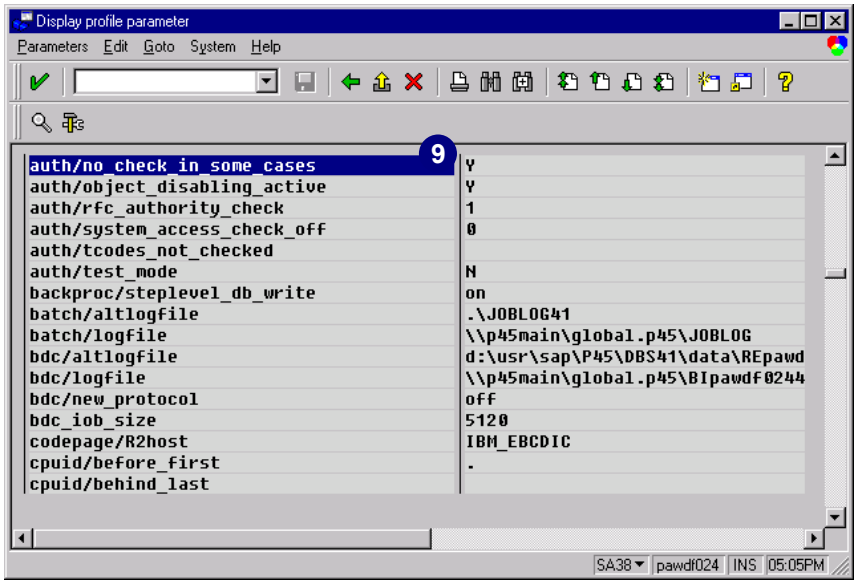
5. In the dialog box, enter the first letters of **`auth/no_check_in_some_cases`** (for example, **`auth/no_check`**) to find the profile parameter.
6. Choose *Find*.



7. Select the searched field.
8. Choose *Position cursor*.



9. If active, the profile parameter for the PG *auth/no_check_in_some_cases* is displayed as a *Y* in the second column.



If the second column does not display the value *Y* for the instance profile parameter *auth/no_check_in_some_cases*, you must first change the instance profile and then reboot the R/3 instance.

Working on SAP Check Indicator Defaults and Field Values

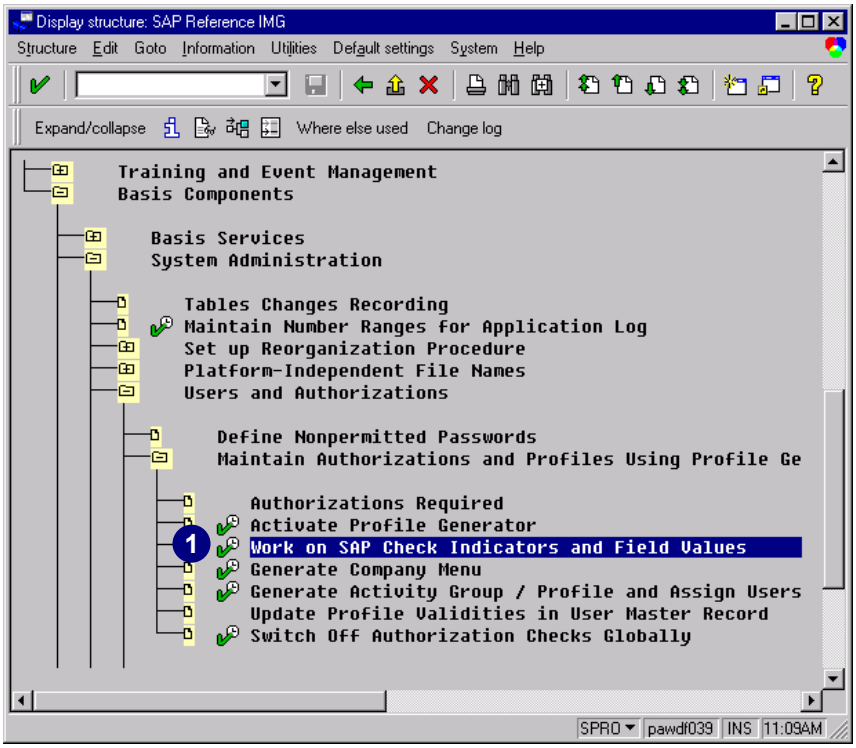
Initial Copying of SAP Defaults into the Customer Tables (SU25)

When you carry out R/3 transactions, a large number of authorization objects are checked that arise through other work areas called in the background. For authorization checks to be successful, the user must have the appropriate authorizations. For this reason, most users receive more authorizations than necessary, which leads to an increased maintenance load.

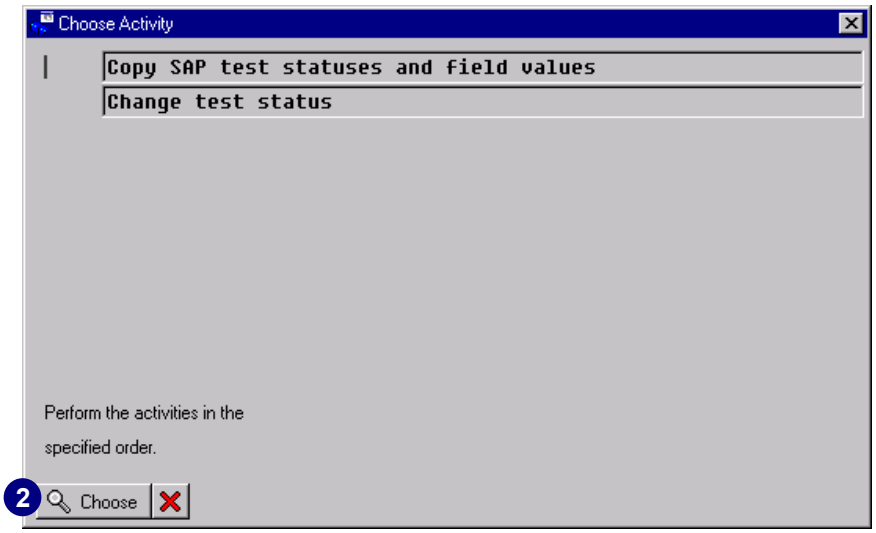
Authorization checks are carried out wherever they are specifically written into the source code of a transaction. However, using transaction *SU24*, you can set check indicators to exclude certain authorization objects from authorization checks. Authorization checks can be excluded in specific transactions, and authorization objects can be excluded globally from being checked. All of these checks are possible without changing the program code. You also use check indicators to control which objects appear in the PG and which field values are displayed for editing before the authorization profiles automatically generate.

Using transaction *SU25* (*Copy initial defaults*), copy the supplied SAP defaults, tables *USOBX* and *USOBT*. This step imports the SAP check indicator defaults for the authorization objects within a transaction and the authorization field values for the PG into customer tables *USOBX_C* and *USOBT_C*. You can edit these values later in transaction *SU24*.

1. Choose *Execute* next to *Work on SAP check indicators and field values* (or enter transaction **`/nSU25`** and continue with step 3).



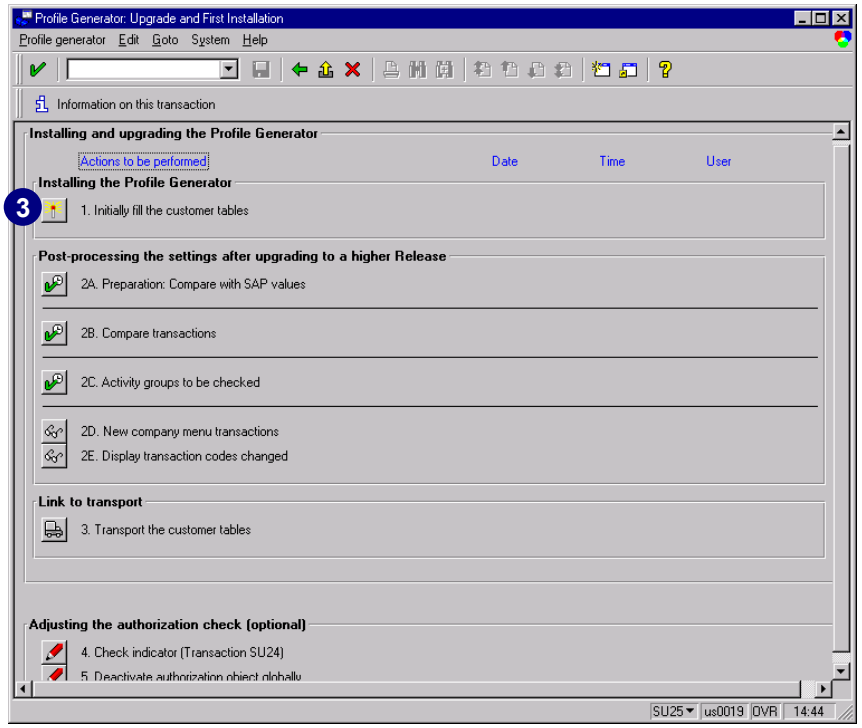
2. Place the cursor in *Copy SAP test statuses and field values* (this translation is incorrect; the text should read *Copy SAP check indicators and field values*) and choose *Choose*.



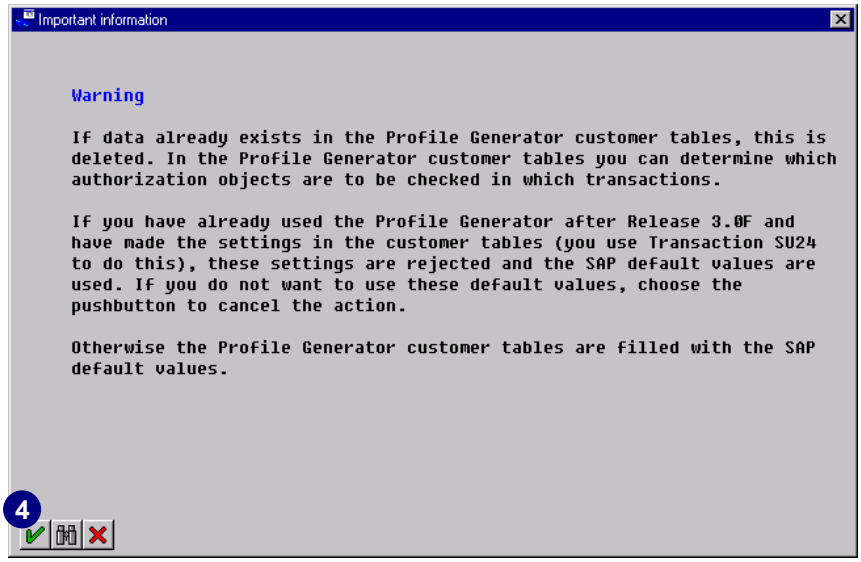
If you have not previously worked with the PG or you want to retransfer all SAP default values, please use the *Initially fill the customer tables* function in the *Installing the Profile Generator* group.

If you have already worked with the PG and want to compare your data with the SAP default values, please refer to chapter 14, *Upgrades*.

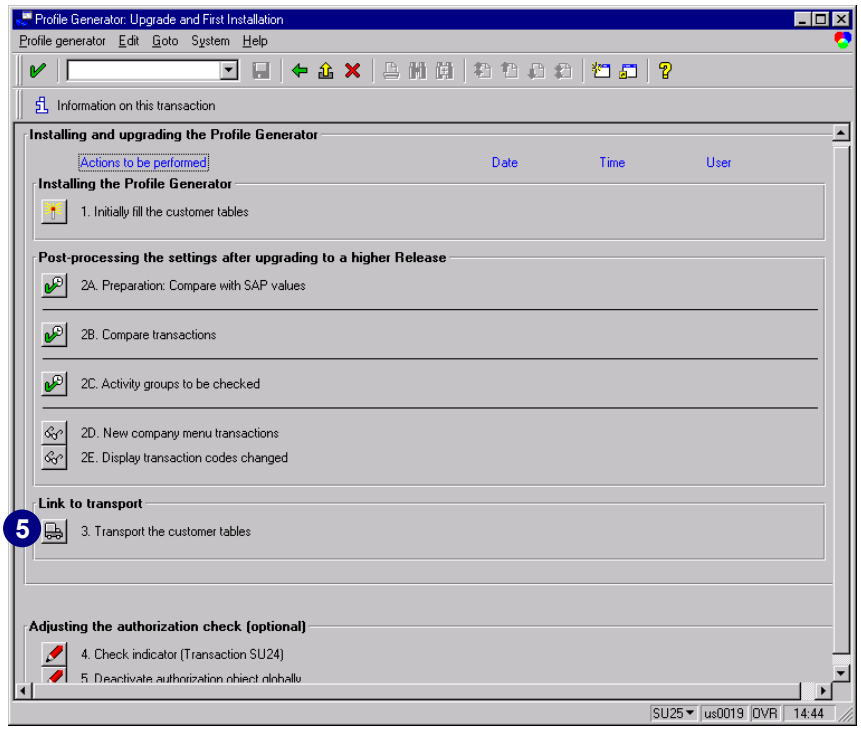
3. Choose the icon next to *1. Initially fill the customer tables*, if you have not previously worked with the PG or if you want to retransfer all SAP default values. This step takes several minutes.



4. Choose *Continue*.



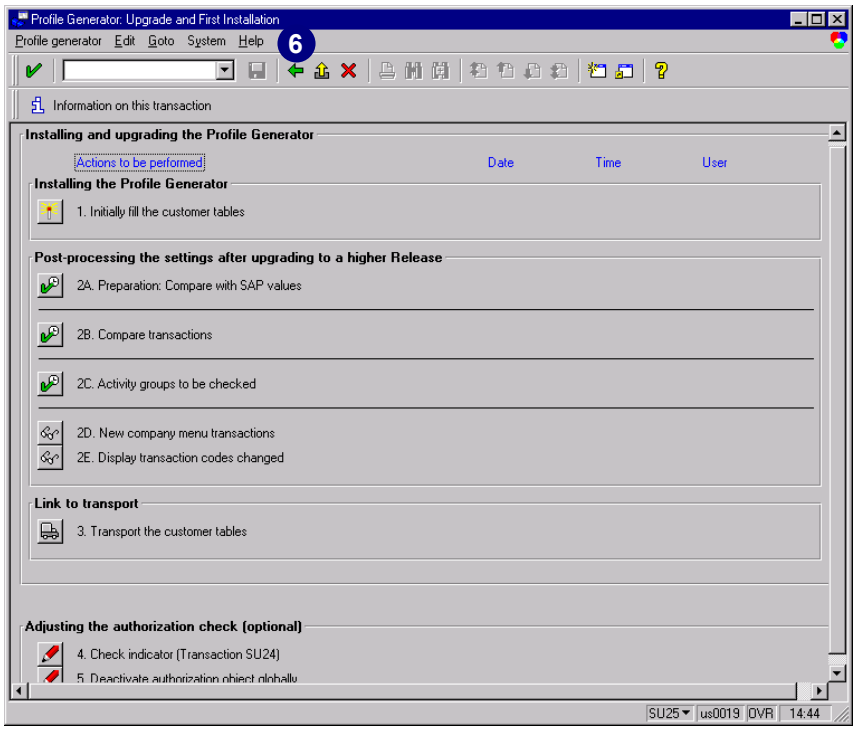
5. Choose the icon next to *3. Transport the customer tables* to transport the PG customer tables (*USOBX_C* and *USOBT_C*). This step writes all the changes that you made in steps *1*, *2A*, and *2B* and all changes to check indicators in transaction *SU24* to a transport request.



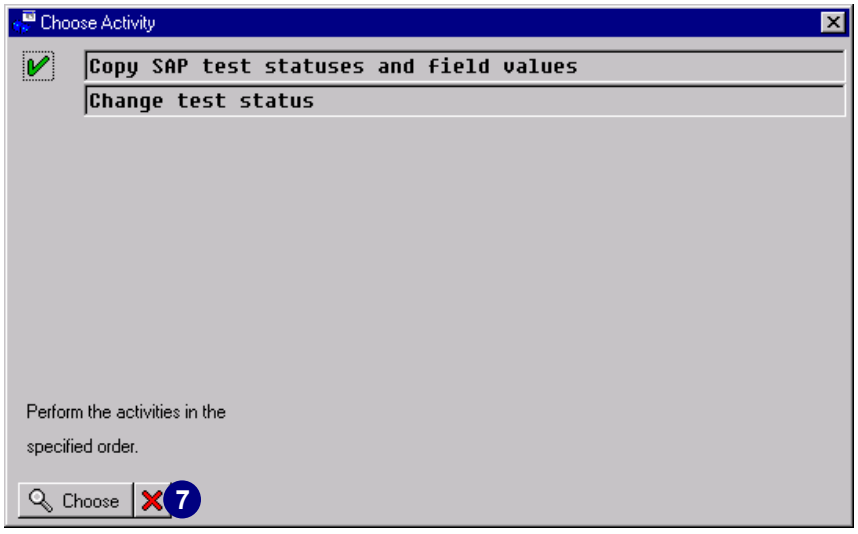
Note that the customer tables (*USOBX_C* and *USOBT_C*) are completely transported. All changes to authorization checks that were made in this transaction or in *SU24* are also transported into the target system. This step replaces all the field value and check indicator settings in the target system.

No activity groups or authorization profiles are transported in this step. To transport newly generated activity groups, use the activity group transport connection.

6. Choose *Back* after the report is finished.



7. Choose *Cancel* and continue with the next section.



Reducing the Scope of Authorization Checks in R/3 (SU24)

The following is optional. Normally you do not have to make any changes in SU24.

In the PG, you have the option to deactivate and activate authorization checks against different authorization objects.

Deactivating Authorization Checks

Whenever you perform R/3 transactions, many authorization objects are checked that arise through other work areas called in the background. For the authorization checks to be successful, the user must have the appropriate authorizations. For this reason, most users receive more authorizations than necessary, which leads to an increased maintenance load. But the core transaction is always protected by object *S_TCODE*, and authorization checks that belong to pure background functions are deactivated. (This has nothing to do with background processing).

In R/3, many authorization objects go unused by most customers. You can deactivate the authorization check against the objects using transaction *SU24*. This deactivation results in clear authorization profiles and better performance.

You can deactivate authorization checks for any of the following reasons:

- Not all authorization objects are used (for instance: F_LFA1_BEK)
- Authorization fields are usually maintained with an asterisk (*)
- Large authorization profiles
- Each transaction is checked by *S_TCODE*
- Needless authorization checks reduce the transaction performance

The following examples illustrate when to use *SU24*:

- If a warehouse worker removes goods from the warehouse, and the remaining stock falls short of a critical limit, the system triggers either a purchasing order, a production order, or both. These operations are carried out because of the system settings and therefore require no further actions by warehouse workers. Accordingly, these workers should not have authorizations for purchase or production orders, so the check against this object should be deactivated.
- Authorization object *F_LFA1_BEK* (Vendor: Account authorization) protects the vendor master records at account level. That is, with this object, it is possible to divide the vendors into groups and only assign the accounting clerk the maintenance authorization for vendors from a certain group. If you do not want to make any authorizations at this level and allow all accounting clerks to maintain all vendors, it is best to deactivate this object.

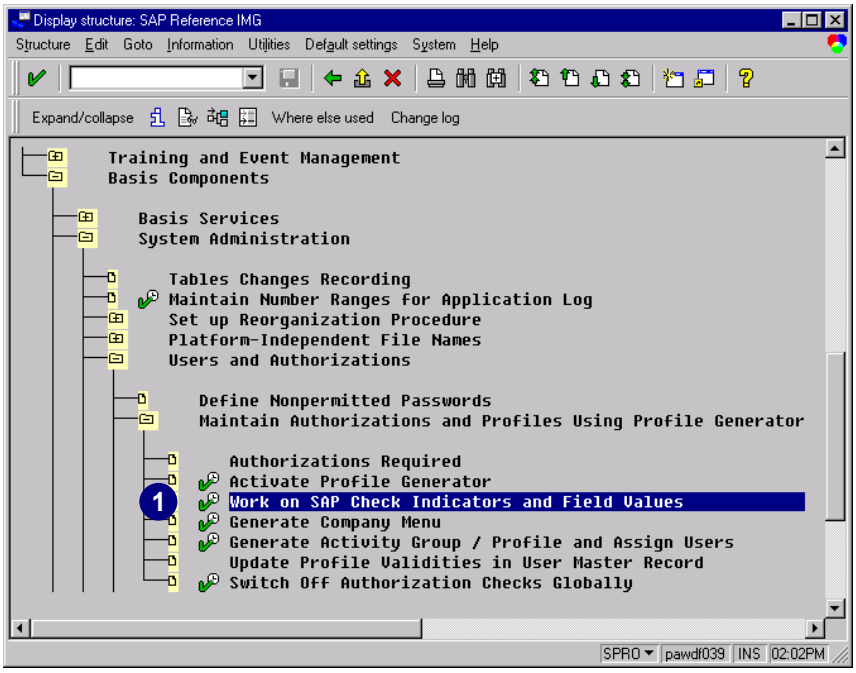
  Only if you have set the check indicator to *CM* (*Check/Maintain*), the authorization and predefined authorization field values are displayed for changing.

How to Reduce the Scope of Authorization Checks

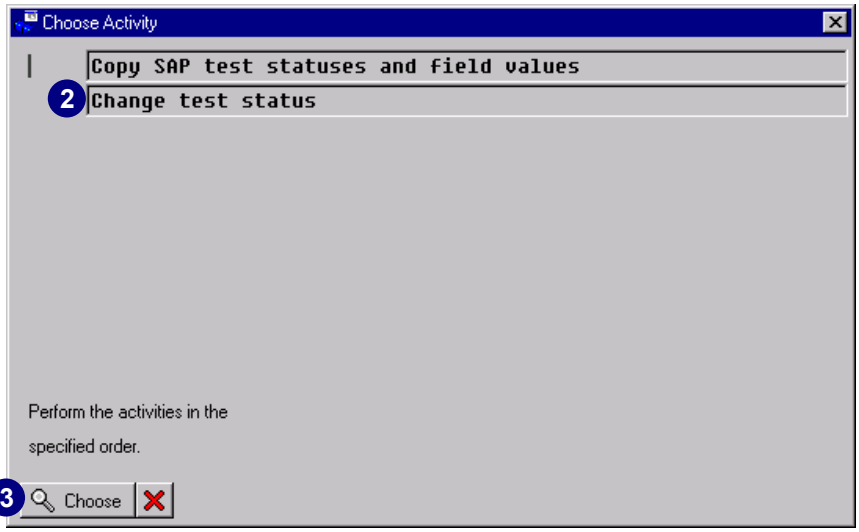
Authorization checks are carried out wherever they are specifically written into the source code of a transaction. However, with transaction *SU24* you can set check indicators to exclude certain authorization objects from authorization checks. You can exclude particular authorization checks either in specific transactions or R/3 System-wide, without changing the program code.

Before the authorization profile is automatically generated, use check indicators to control which objects will appear in the PG and which field values will be displayed. To use transaction *SU24*, you must work with the PG. Before running *SU24* you need to have at least set and activated the system parameter *auth/no_check_in_some_cases* = *Y* (default value), and run *SU25* which copies the SAP check indicator defaults and field values from table *USOBT* and *USOBX* into the customer tables.

1. Choose *Execute* next to *Work on SAP Check Indicators and Field Values* (or enter transaction **SU24** and continue with step 4).



2. Select *Change test status* (this translation is incorrect; the text should read *Change check indicator*).
3. Choose *Choose*.

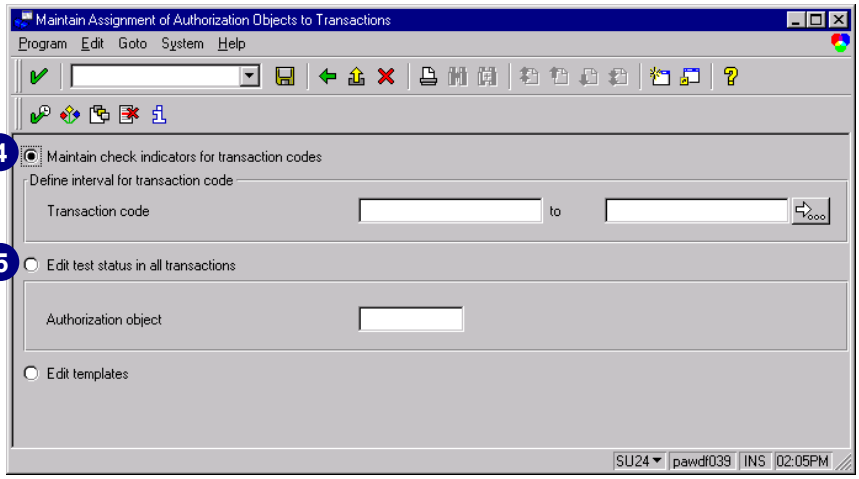


If you upgraded to Release 4.5B from Release 3.0F, 3.1G, 3.1H, 3.1I, 4.0A, 4.0B or 4.5A (assuming that you worked with the PG in these prior releases) and if you want to activate or deactivate authorization checks in *SU24*, please refer to chapter 14, *Upgrades*, before continuing. Changes to the SAP check indicator defaults and field values must be compared after the upgrade.

If Release 4.5B was recently installed, and not upgraded, you may continue with this chapter.

From the initial screen in transaction *SU24*, you may either select one of following options:

4. *Maintain check indicators for transaction codes*
5. *Edit test status in all transactions* (The translation is not correct, it should be *Edit check indicators in all transactions*).

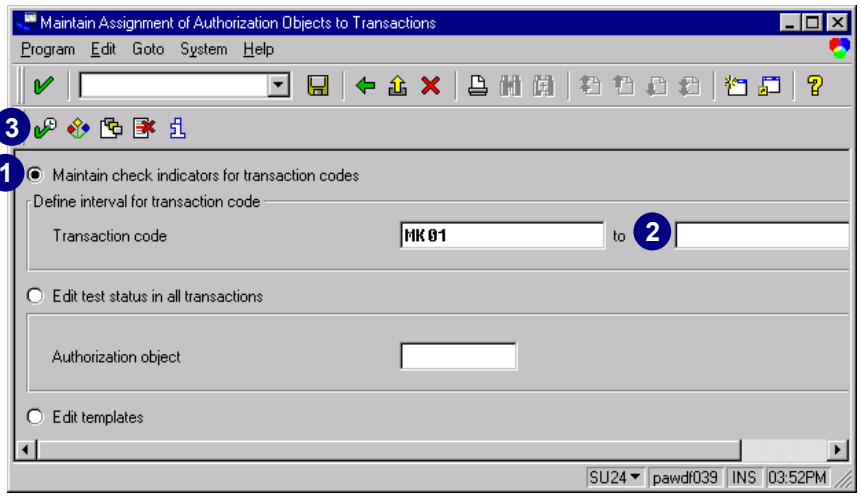


Maintain Check Indicators for Transaction Codes

Use *SU24* to display each transaction's associated authorization objects. You can deactivate or activate each of these authorization objects from the authorization check.

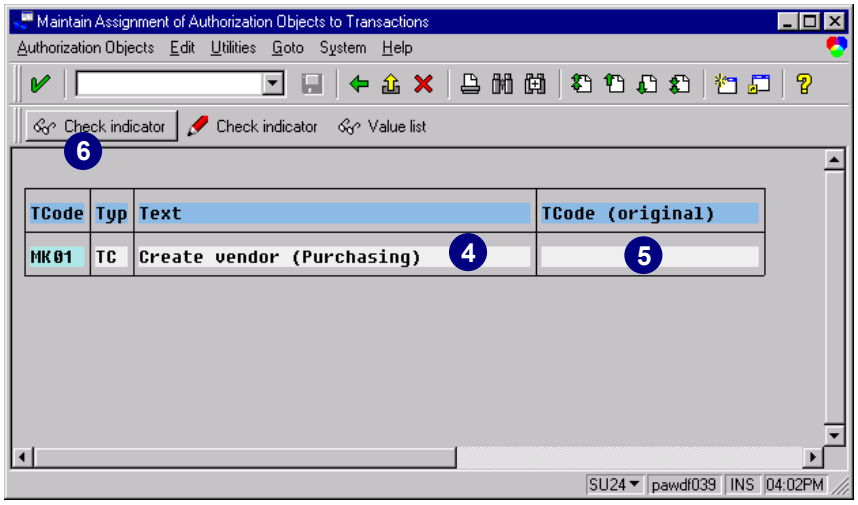
In transaction *SU24*,

1. Choose *Maintain check indicators for transaction codes*.
2. Enter either a single transaction code (for example, **MK01**) or a range of codes for which you want to list the check indicators.
3. Choose *Execute*.

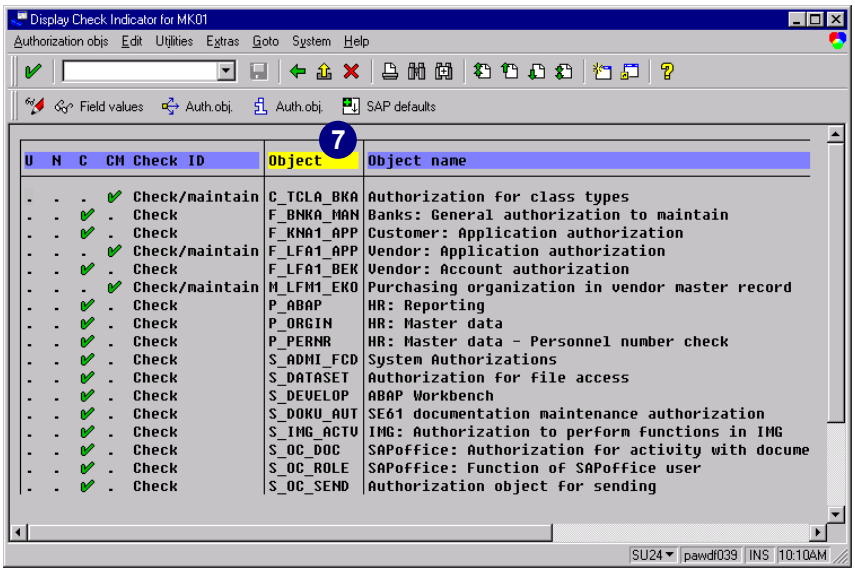


For more information, see *What Is Special with Parameter Transactions* on page 2–35.

4. Select the appropriate transaction.
5. If you are dealing with a parameter transaction, the core transaction appears in *TCode* column on the right-hand-side.
6. Choose *Display Check indicator* to display the current active check indicators for authorization objects in the selected transaction.



7. A list of authorization objects appears in the *Object* column for the selected transaction involved with their check.



What the Different Check Indicators Mean

CM = Check/Maintain

- An authorization check is carried out against this object
- The PG creates an authorization for this object and field values are displayed for changing
- Default values for this authorization can be maintained

C = Check

- An authorization check is carried out against this object
- The PG does not create an authorization for this object, so field values are not displayed
- No default values can be maintained for this authorization

N = No check

- The authorization check against this object is disabled
- The PG does not create an authorization for this object, so field values are not displayed
- No default values can be maintained for this authorization

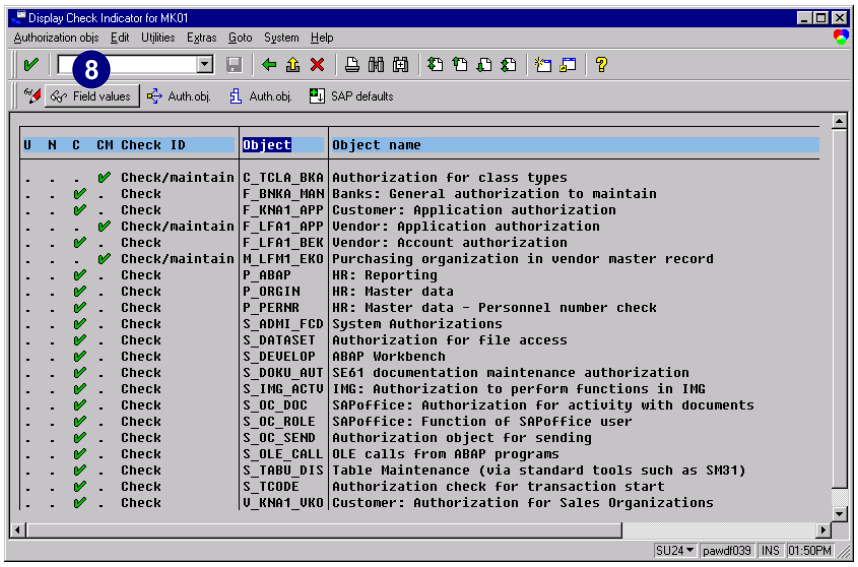
U = Unmaintained

- No check indicator is set
- An authorization check is always carried out against this object
- The PG does not create an authorization for this object, therefore field values are not displayed

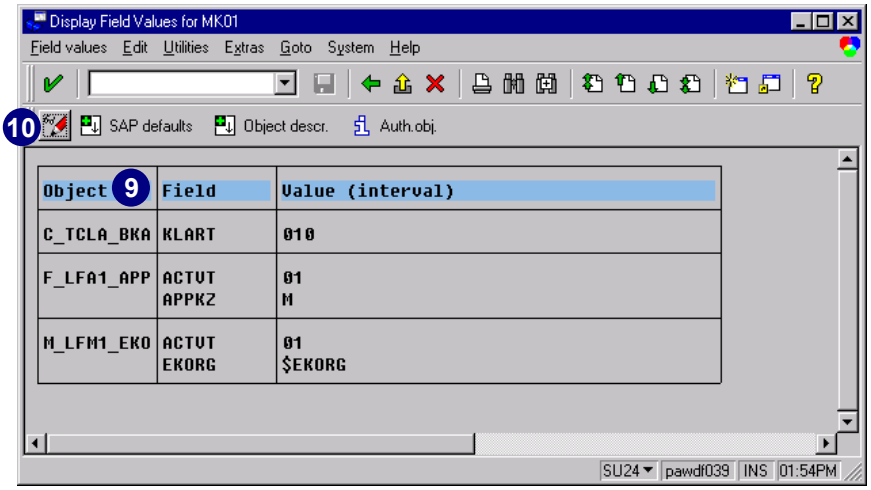
The check indicator of an authorization object is important for the PG. The PG only creates an authorization for an authorization object if the check indicator is set to *Check/Maintain (CM)*. Predefined values for this authorization are already maintained in the authorization overview. You can only predefine authorization values for an object if the check indicator is set to *Check/Maintain (CM)*.

8. Choose *Display Field values*.

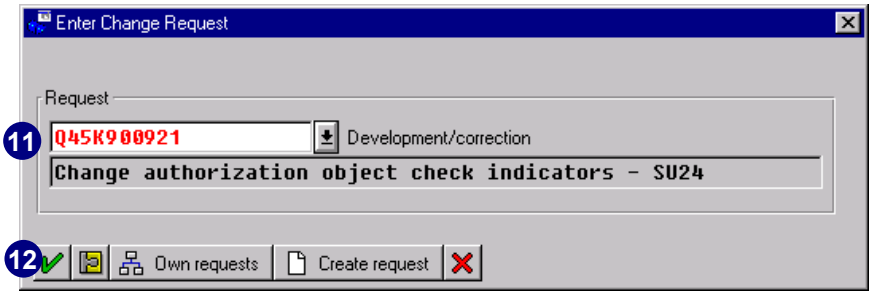
   Using the push buttons, you can display predefined authorization field values for individual objects and the SAP defaults for the check indicators.



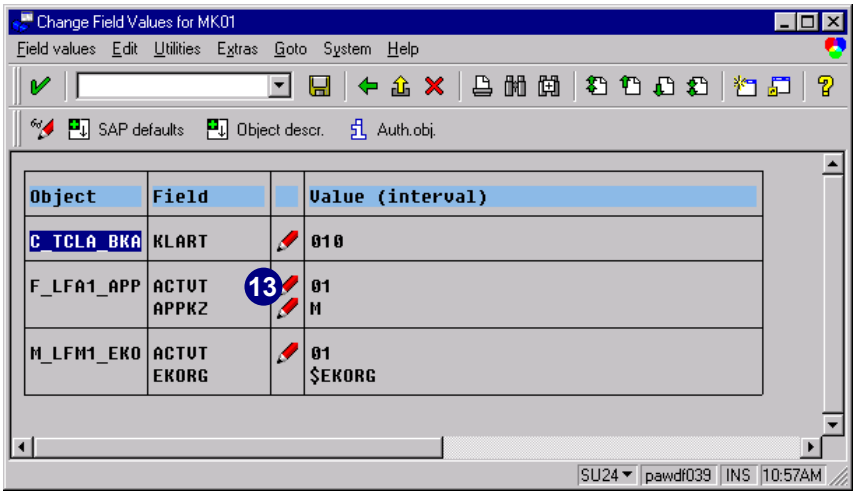
9. In our example, only three objects have the check indicators set to *Check/maintain*. Therefore three objects get displayed with predefined value sets.
10. Choose *Display* <-> *Change*.



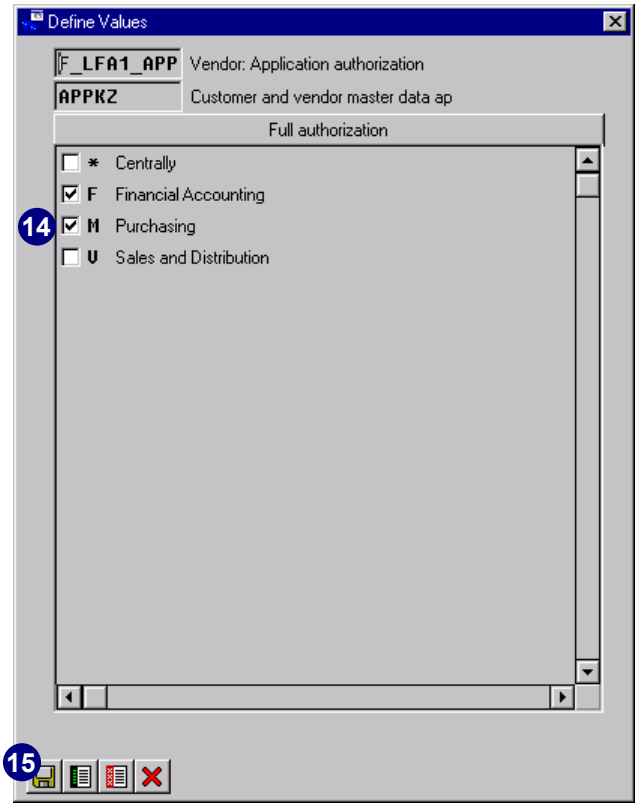
11. In the *Enter Change Request* dialog box, make sure you choose the correct change *Request* number.
12. Choose *Enter*.



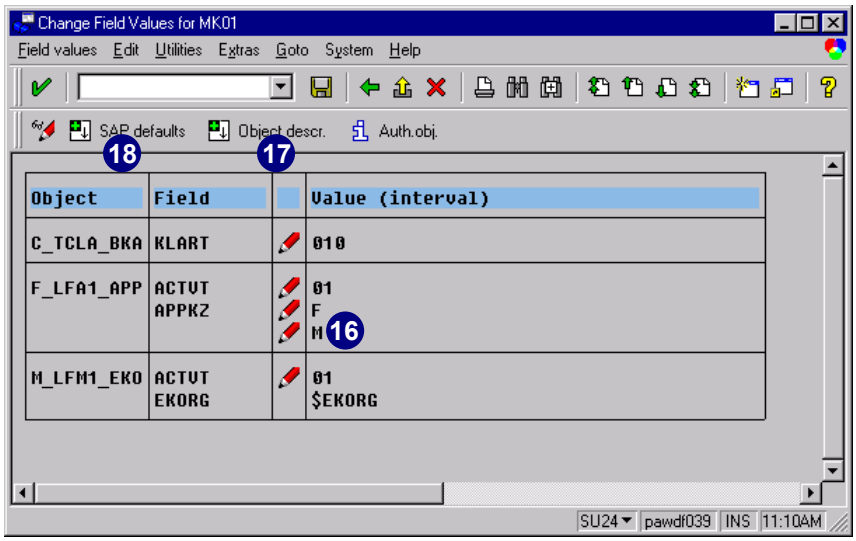
13. To change the authorization field values for one of the objects, choose *Change* next to the object's fieldname.



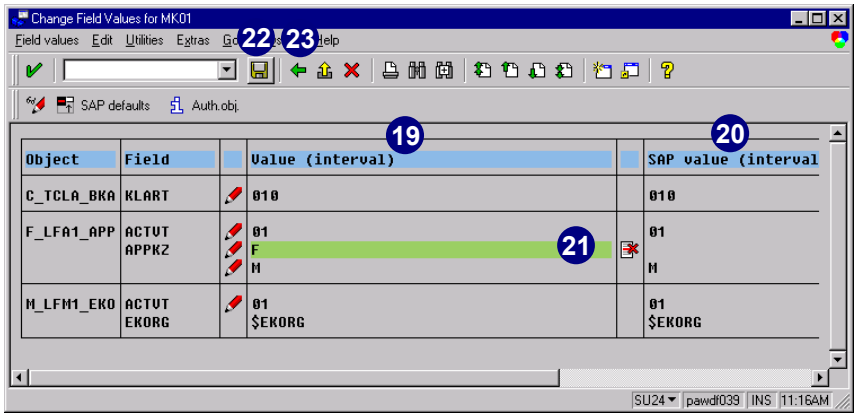
14. Select the new value.
15. Choose *Transfer*.



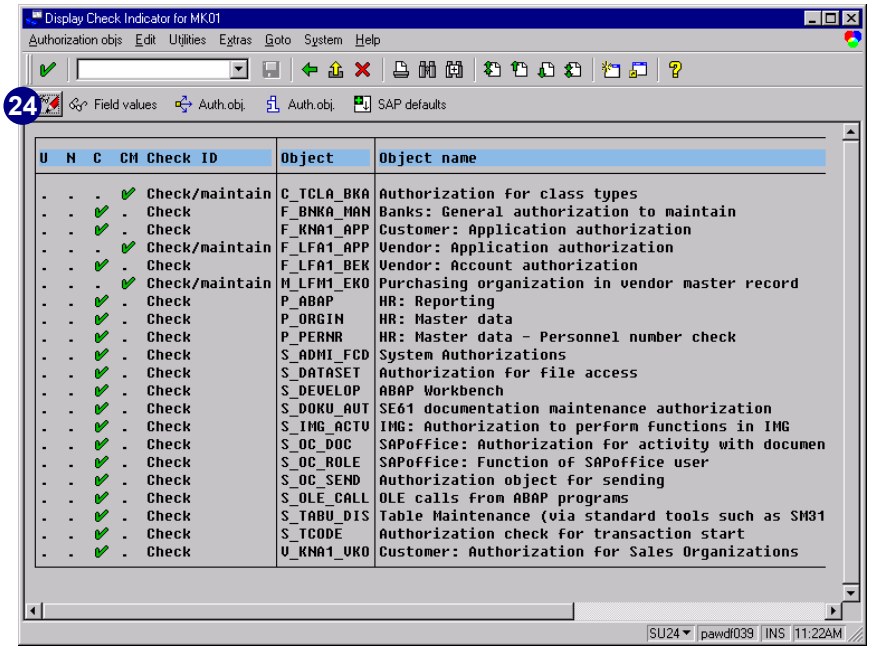
16. The value was added.
17. (optional) Choose *Show Object descr.* to display the long text for the authorization object.
18. Choose *Show SAP defaults* to display the SAP defaults to compare any changes you might have made.



19. In the *Value (interval)* column, notice your changes (this is table *USOBT_C*, which represents customer settings).
20. In the *SAP value (interval)* column, notice the originally delivered SAP default values (this is table *USOBT*, which represents SAP defaults). Values that have changed from the SAP defaults are in color.
21. To skip your changes, choose the *delete line* icon for the appropriate value you changed.
22. Choose *Save*.
23. Choose *Back* or *Hide SAP defaults*.

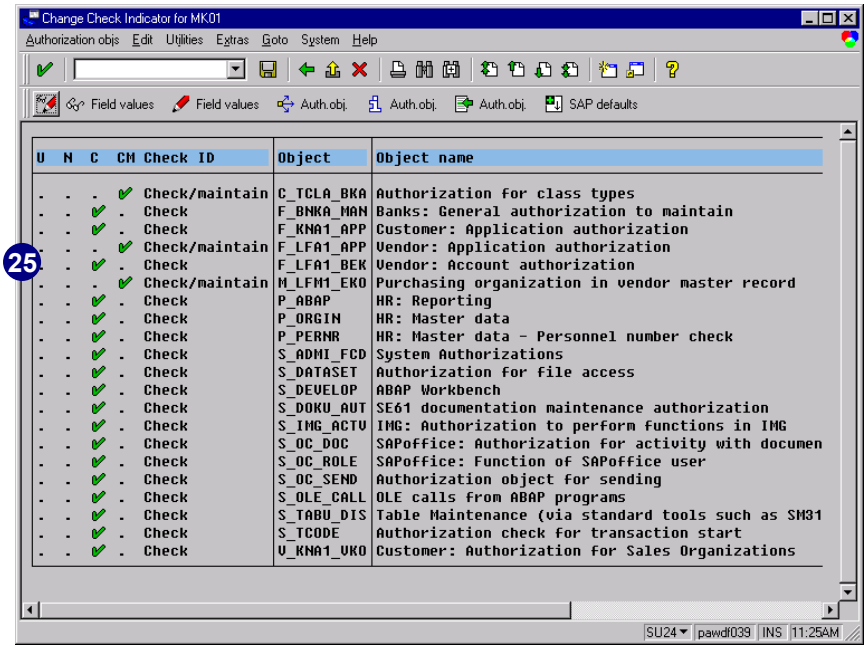


24. Choose *Display* <-> *Change* to switch to change mode for the check indicators.

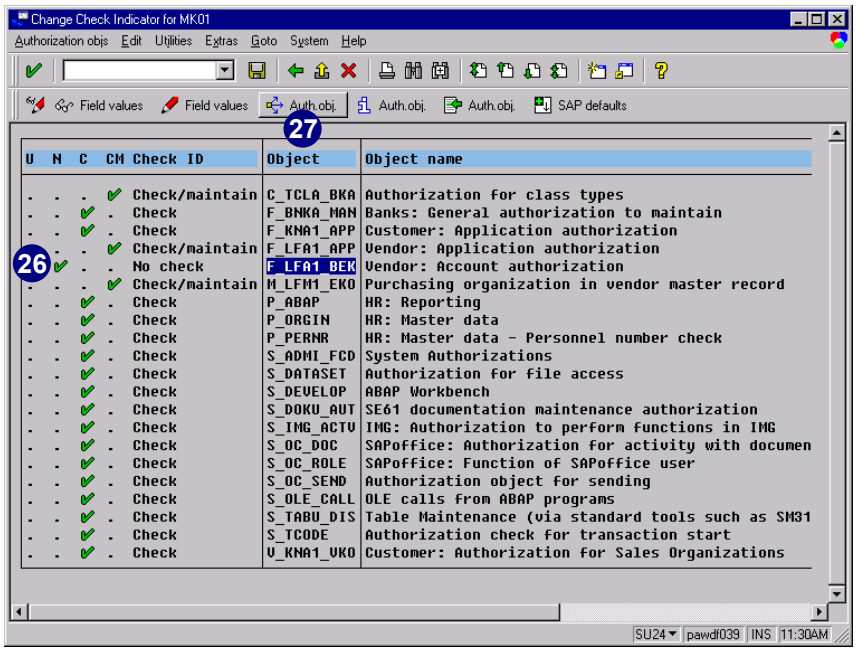


25. To change a check indicator for an object, click in the appropiate column. Notice how the cursor changes to an iconized hand as you move over the check indicators.

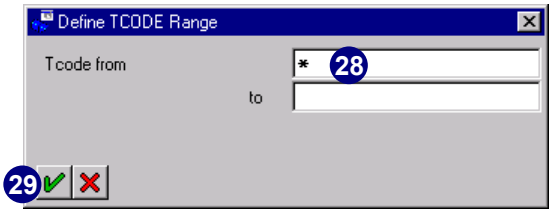
    In this example, set the check indicator for object *F_LFA1_BEK* to *No check*.



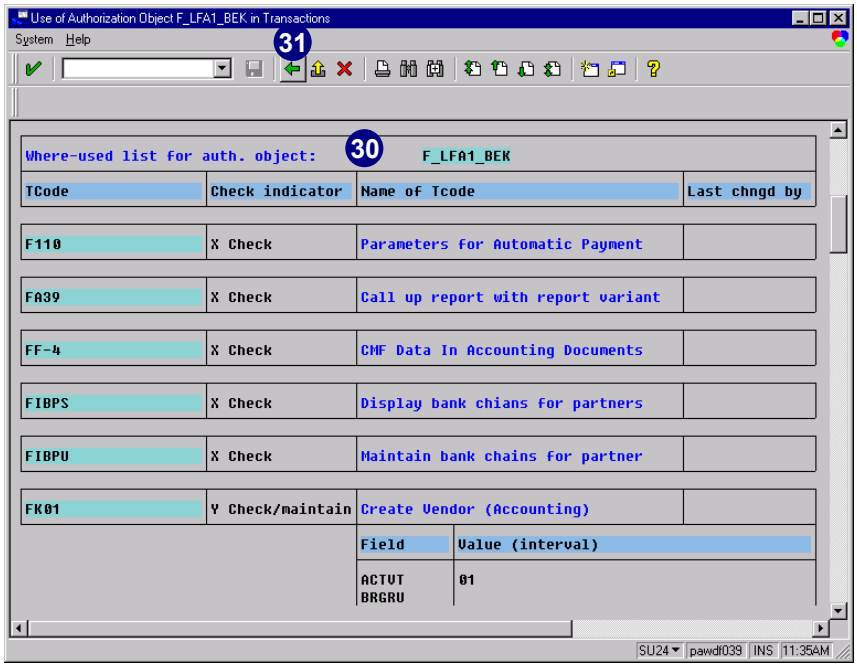
26. The check indicator has successfully been changed. *F_LFA1_BEK* will no longer be checked in transaction *MK01*.
27. Select an object and choose the *Where-used-list* icon for any authorization object.



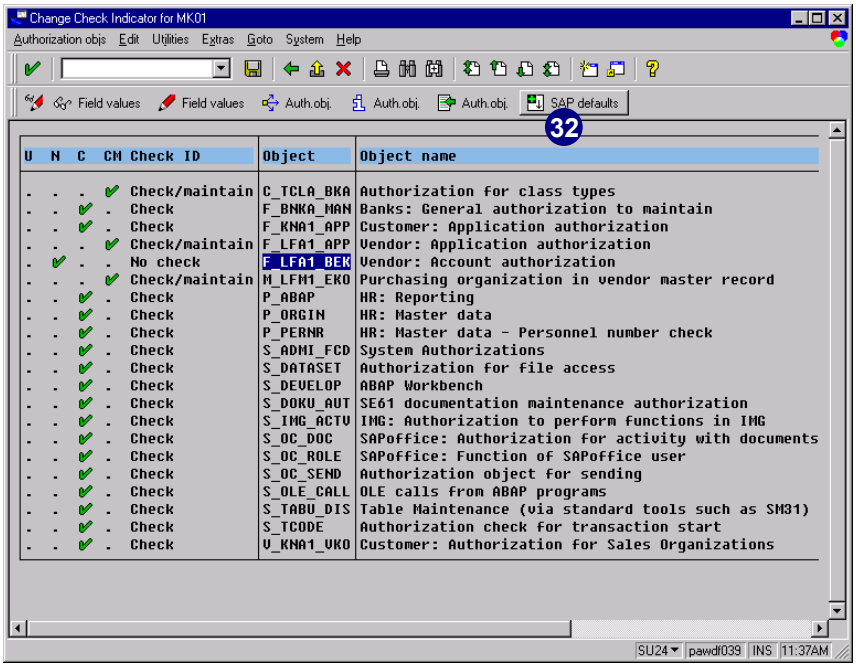
28. You have to determine a specific transaction code range. To search through all existing transaction codes, enter an asterisk (*).
29. Choose *Continue*.



30. The generated list shows all transactions according to your selection where the selected authorization object is used.
31. Choose *Back*.



32. Choose *Show SAP defaults* to display the SAP check indicator defaults in the same list.



Both table entries in tables *USOBX* and *USOBX_C* now appear for the selected transaction (in this example, *MK01*).

33. In the *Check ID* column, notice the current active check indicators for this transaction (entries in table *USOBX_C*).

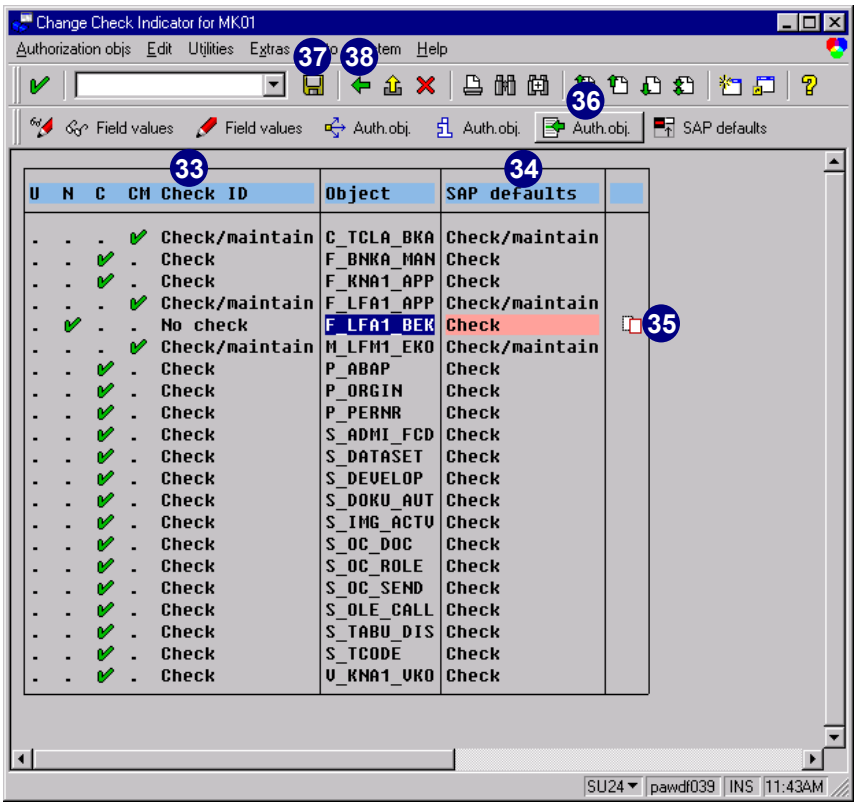
34. In the *SAP defaults column*, notice the SAP check indicator default values displayed (entries in table *USOBX*).

35. To skip your changes, choose the *Copy SAP defaults* icon to reset to the SAP check indicator default value for this authorization object. Settings that differ from SAP defaults appear in color.

36. Choose *Insert Auth. obj.* to add a new object that should be checked. There must also be an *AUTHORITY_CHECK* call in this program for the new object.

37. Choose *Save*.

38. Choose *Back*.



Exceptions
Authorization objects from the Basis (S*) and Human Resources Management applications (P_*, PLOG) cannot be excluded from being checked. The field values for these objects must always be checked.

Important Information Concerning Profile Matchup After Changes in *SU24*

If you have generated authorization profiles with the PG, after making changes to check indicators in transactions, a profile matchup is required (even if the PG does not indicate this need for the appropriate authorization profiles).

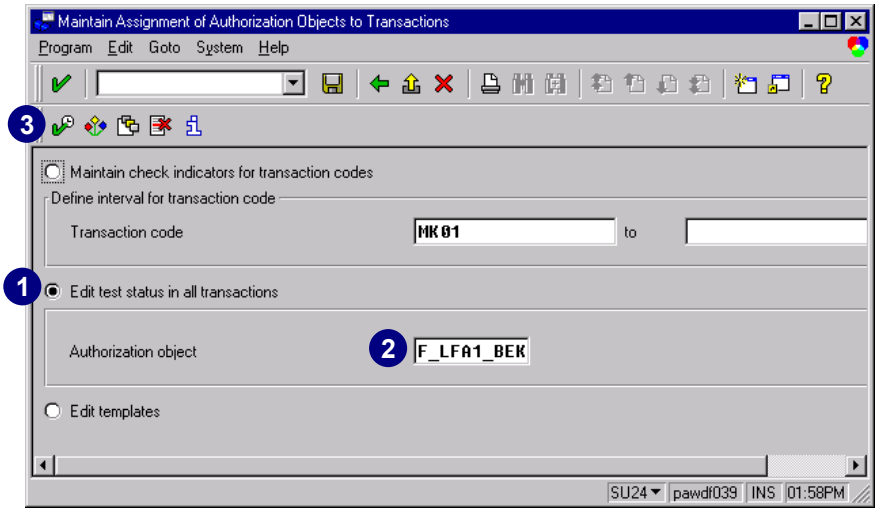
1. After making changes to check indicators with *SU24*, remember the transactions that are affected by the change.
2. Find out in which activity groups these transactions have been selected. To help identify the appropriate activity groups, access the user *Repository Information System*, transaction *SUIM*, or choose *Tools* → *Administration* → *User maintenance* → *Repository Infosys*.
3. In transaction *PFCG*, select the activity group to be regenerated. You cannot select more than one activity group at a time. When maintaining the authorization data, be sure to select *Expert Mode for profile generation* and then *Read old status and merge with new data*.
4. Regenerate the profile.
5. No user master comparison is required. Remember that changes become active with the next system logon.

Globally Changing Authorization Checks in the R/3 System

You can also globally change authorization checks for an authorization object in transactions where the authorization object occurs. You can also specifically exclude individual transactions from the global change.

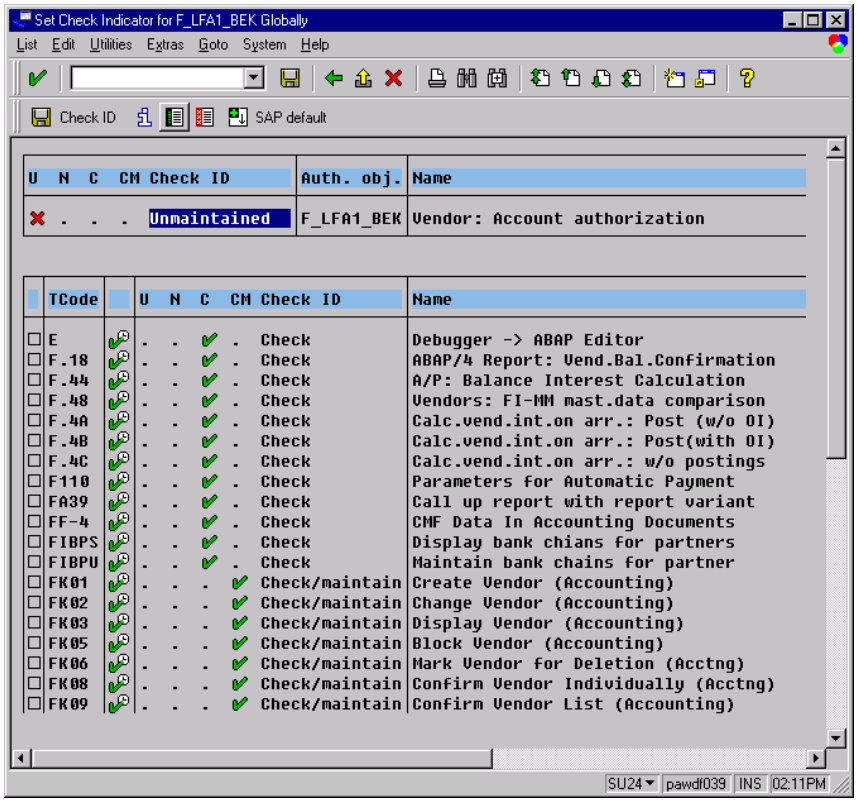
In transaction *SU24:*

1. Choose *Edit test status in all transactions* (the translation is not correct; it should read *Edit check indicators in all transactions*).
2. Enter the desired authorization object (for example **`F_LFA1_BEK`**).
3. Choose *Execute*.



For more information, see *What Is Special with Parameter Transactions* on page 2–35.

You will see a list of transactions where the entered authorization object appears with the appropriate check indicator per transaction.



The check indicator of an authorization object is important for the PG, which creates authorizations for authorization objects only if the check indicator is set to *Check/Maintain (CM)*. Predefined values for this authorization are then maintained in the authorization overview. You can only predefine authorization values for an object if the check indicator is set to *Check/Maintain (CM)*.

What the Different Check Indicators Mean

CM = Check/Maintain

- An authorization check is carried out against this object
- The PG creates an authorization for this object and field values are displayed for changing
- Default values for this authorization can be maintained

C = Check

- An authorization check is carried out against this object
- The PG does not create an authorization for this object, so field values are not displayed
- No default values can be maintained for this authorization

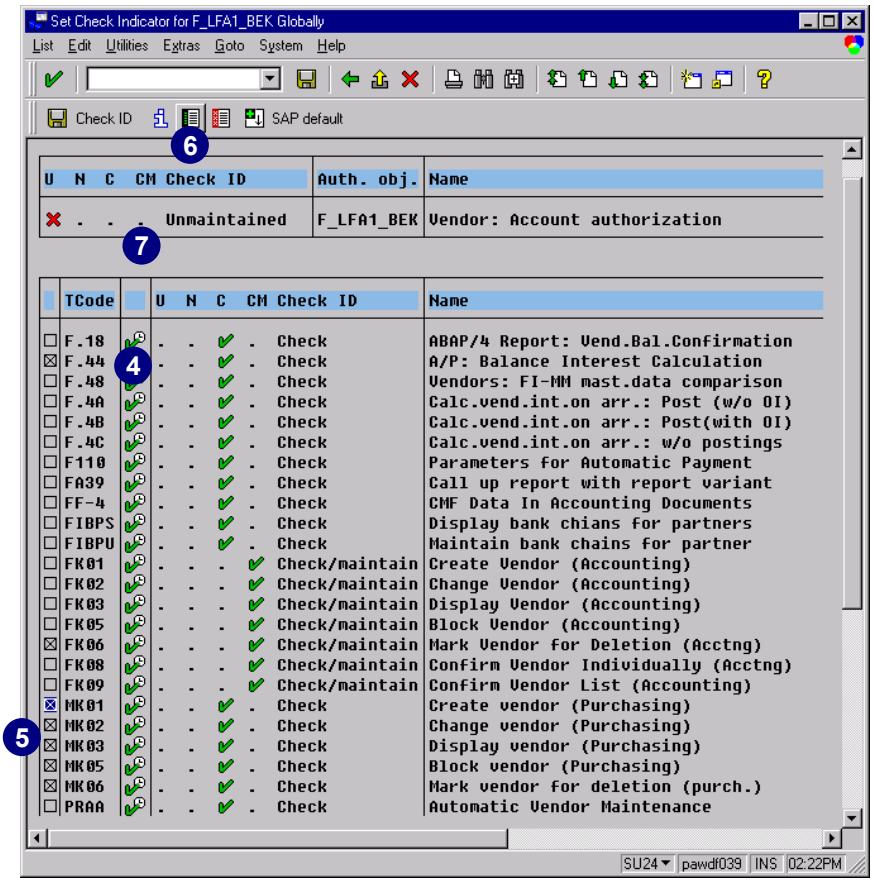
N = No check

- The authorization check against this object is disabled
- The PG does not create an authorization for this object, so field values are not displayed
- No default values can be maintained for this authorization

U = Unmaintained

- No check indicator is set
- An authorization check is always carried out against this object
- The PG does not create an authorization for this object, so field values are not displayed
- No default values can be maintained for this authorization

4. Choose *Execute* next to the *Tcode* column to call the transaction and check its function.



To alter the check indicator either for selected transactions or globally choose one of the following options:

5. Select the transactions for which you wish to change the check indicator.
6. Choose *Select all* to select all transactions first and then deselect individual transactions as necessary.

To ensure that the PG actually creates an authorization, we need to change the check indicator for the appropriate authorization object from *C (Check)* to *CM (Check/Maintain)*.

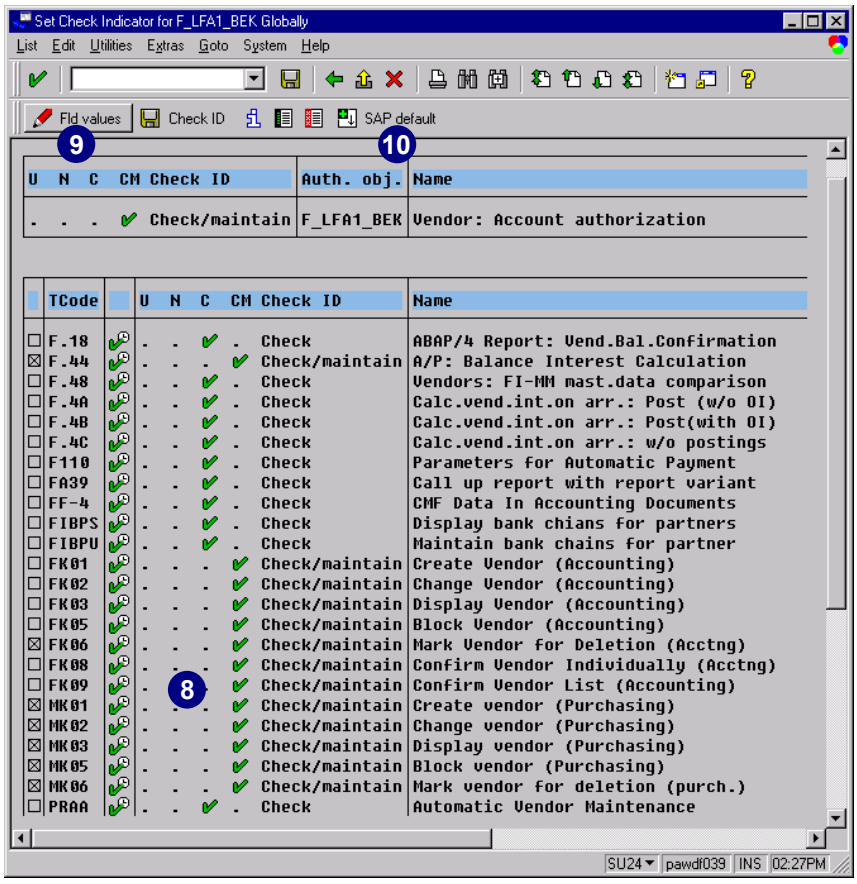
7. To simultaneously change the check indicators for the selected transactions, change the check indicator in the first line, which contains the name of the authorization object, by clicking on the gap for the new check indicator.

8. Only the check indicator for the transactions you selected have changed.

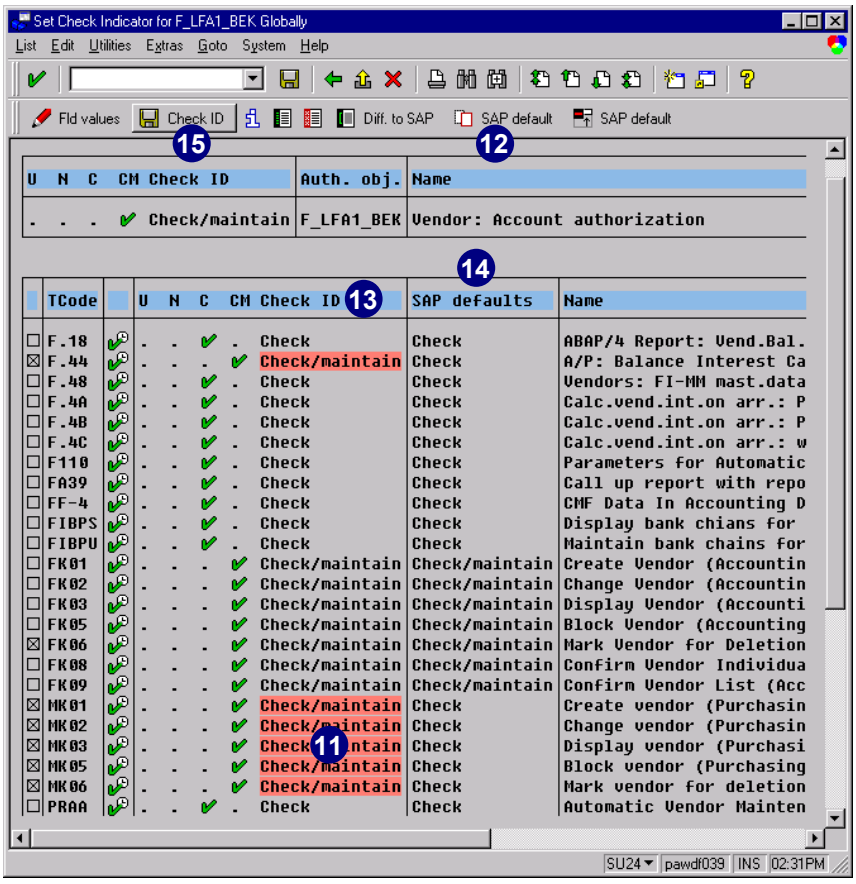
   You can also change the check indicator for individual transactions. Alter the indicator in the appropriate lines by double-clicking on the new check indicator.

9. Once a check indicator in the list is set to *CM* (*Check/Maintain*), a clickable button, *Change Fld. values*, appears. By clicking this button, you can maintain the authorization field values of the selected authorization object for all transactions whose check indicator has been set to *CM*.

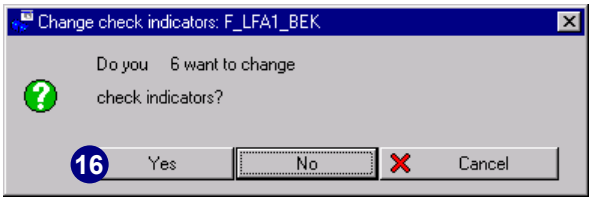
10. Choose *Display SAP defaults* to compare the current settings with the SAP defaults.



11. The changes made are shown in red. To highlight all changed transactions in yellow, choose *Edit* → *Changes* → *Display in color*.
12. Choose *Copy SAP default* if you want to restore the selected transactions to their original delivery status set by SAP. During installation, this step restores the check indicators and field values to the setting in the R/3 System.
13. In the *Check ID* column, notice the changes you made (entries in table *USOBX_C*).
14. In the *SAP defaults* column, notice the SAP check indicator default values (entries in table *USOBX*).
15. Choose *Save Check-ID*.



16. Choose *Yes*.



Exceptions
Authorization objects from the Basis (S*) and Human Resources Management applications (P_*, PLOG) cannot be excluded from being checked, because the field values for these objects always get checked. Transactions whose check indicator cannot be changed because of a local lock (ENQUEUE) or a lock in the correction and transport system (for object catalog entry *R3TR SUSK <Tcode>*) are also shown in color. A short error message appears in the description field.

Important Information Concerning Profile Matchup After Changes in *SU24*

If you have generated authorization profiles with the PG, after making changes to check indicators in transactions, a profile match up is required (even if the PG does not indicate this need for the appropriate authorization profiles).

After making changes to check indicators with *SU24*, remember the transactions that are affected by the change.

1. Find out in which activity groups these transactions are selected. To identify the appropriate activity groups, access the user *Repository Information System*, by entering transaction **SUIM** (or choosing *Tools* → *Administration* → *User maintenance* → *Repository Infosys*).
2. In transaction *PFCG* select the activity group that has to be regenerated. You cannot select more than one activity group at a time. When maintaining the authorization data be sure to select *Expert Mode for profile generation* and then *read old status and merge with new data*.
3. Regenerate the profile.
4. No user master comparison is required. Remember that changes become active with the next system logon.

What Is Special About Parameter Transactions?

The parameter transactions are an exception. These transactions work with a powerful core transaction, which is restricted by the fact that the initial screen of the core transaction is filled and skipped in the parameter transaction.

You cannot exclude authorization objects from direct use in parameter transactions, but only with the corresponding core transaction.

Example:

Parameter transaction = *F48V* (Management of Document Archives)

Core transaction = *SARA* (Archive Management)

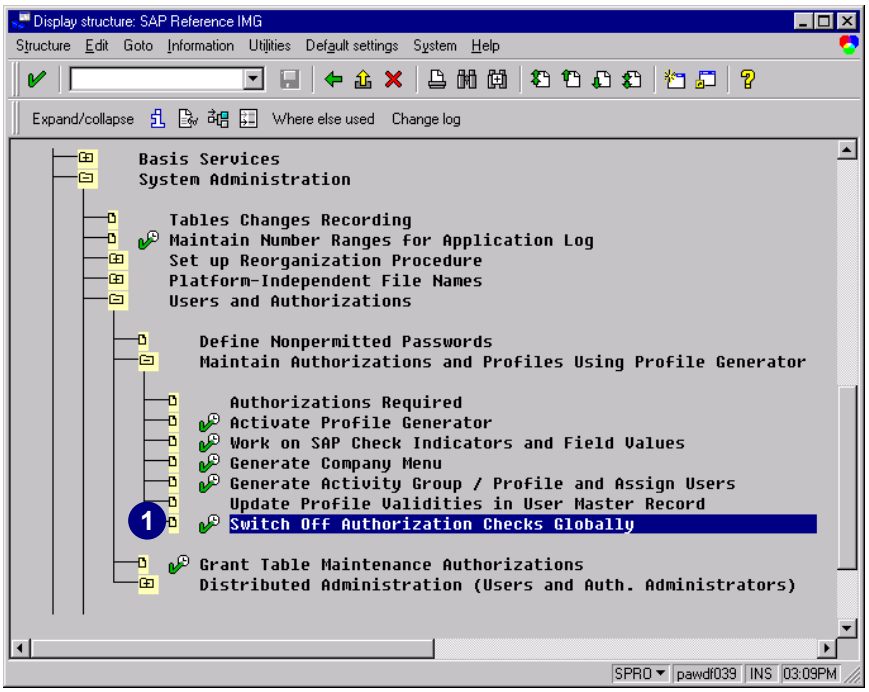
To set the check indicator of transaction *F48V* to *N* (no check), you need to change the check indicator of the core transaction *SARA*. You can find the name of this transaction in the right-hand column *TCode* overview in transaction *SU24*. If you double-click on the parameter transaction code in field *TCode*, the system branches directly into the check indicator maintenance of the core transaction.

If the authorization object for parameter transaction *F48V* is set to *C* (check), but under the core transaction it is set to *CM* (check/maintain), the field values for *SARA* will be suggested as defaults in the PG. If the authorization object is also set to *CM* in *F48V*, the field values maintained for *F48V* will be recommended as defaults in the PG, and the entries for *SARA* will be overwritten. You can maintain or overwrite the field values of the core transaction for parameter transactions in transaction *SU24*.

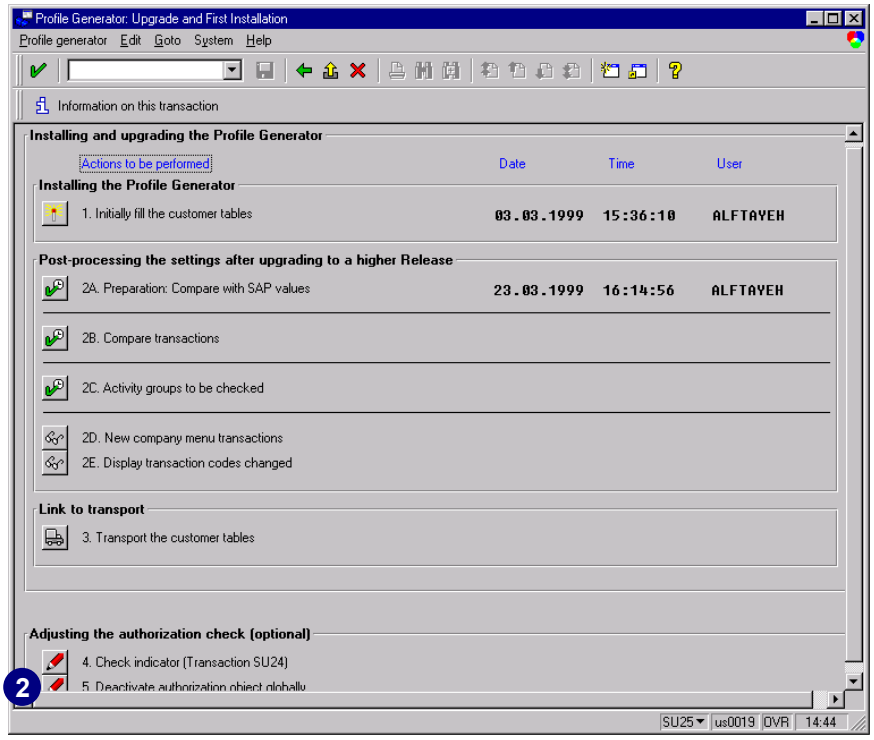
Globally Deactivating or Activating Authorization Checks

You can also globally deactivate or activate authorization checks with transaction *AUTH_SWITCH_OBJECTS*. The system does not execute any authorization checks for deactivated authorization objects. You have several options to reach transaction *AUTH_SWITCH_OBJECTS*. You can use the IMG (see step 1), transaction **SU25** (see step 2) or use transaction **auth_switch_objects** directly.

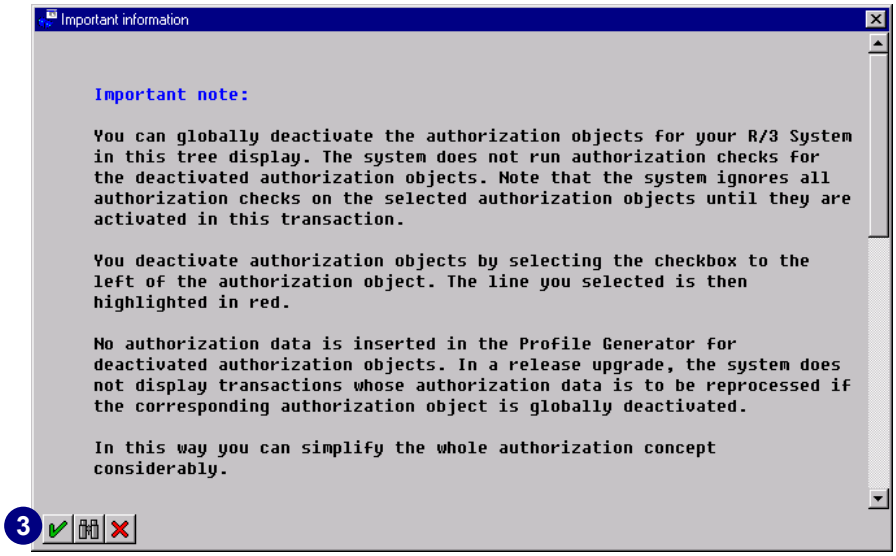
1. Choose *Execute* next to *Switch Off Authorization Checks Globally* and continue with step 3 (or enter **`su25`** and continue with step 2).



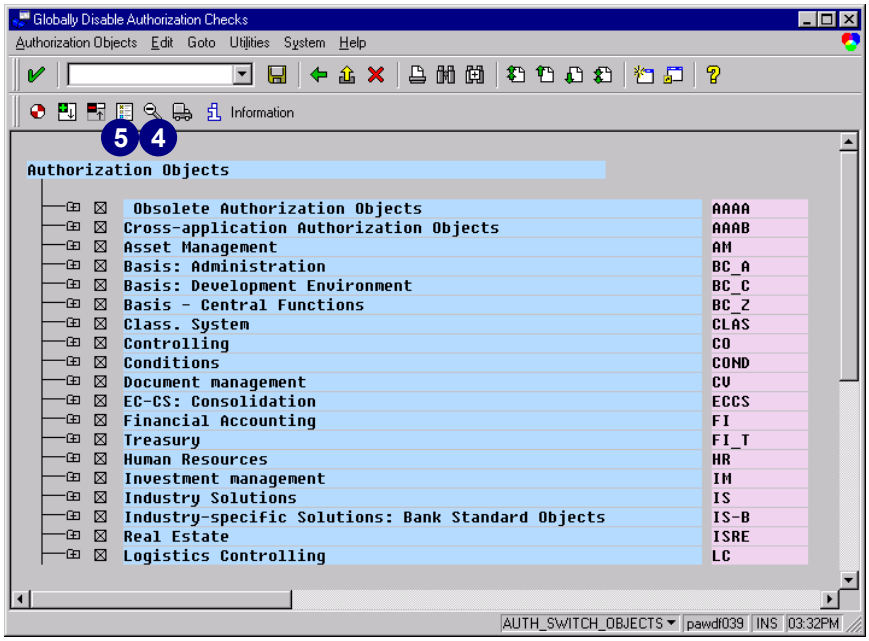
2. In transaction *SU25,* choose *Deactivate Auth. Object* next to 5. *Deactivate authorization object globally.*



3. Choose *Enter*.

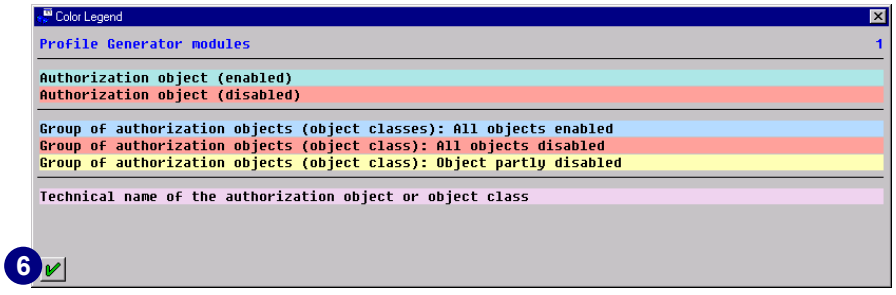


4. To view the technical names, choose the icon *Technical name on/off*.
5. To view the color legend, choose the icon *Color key*.

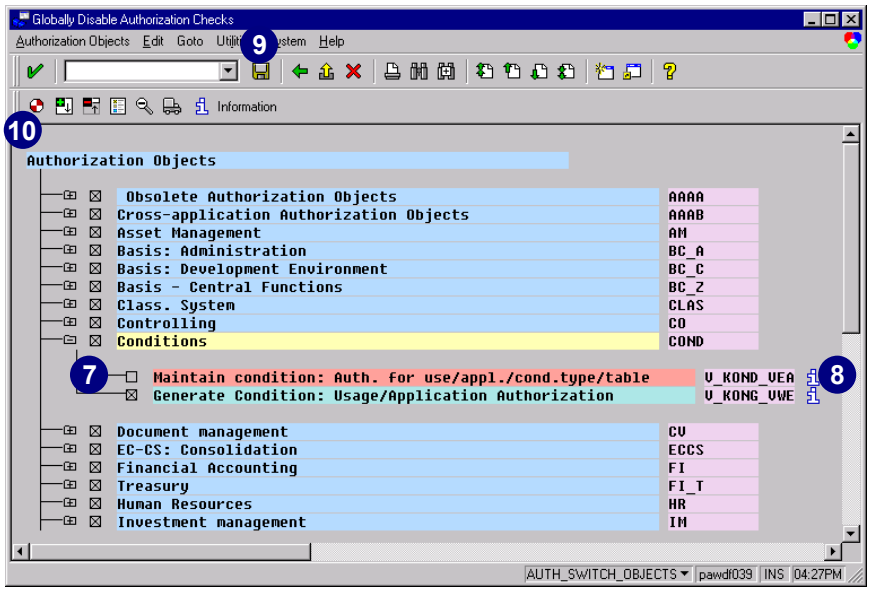


The screen displays the *Color Legend*.

6. Choose *OK* to continue.



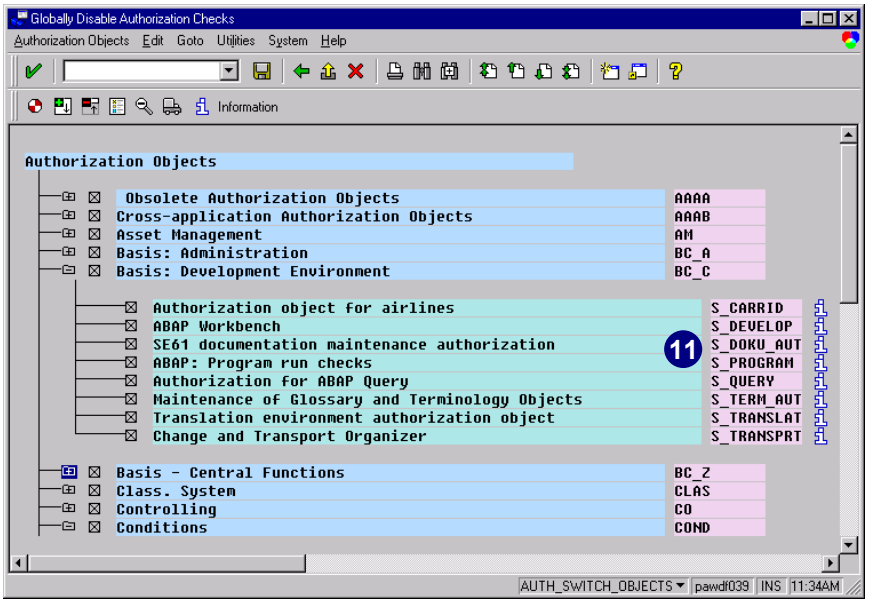
7. Deactivate authorization objects by deselecting the checkbox next to them. The selected line will be highlighted in red.
8. For a detailed explanation about the authorization object, choose the *Information* icon next to the authorization object.
9. Choose *Save*.
10. To activate your data, choose *Activate data*.



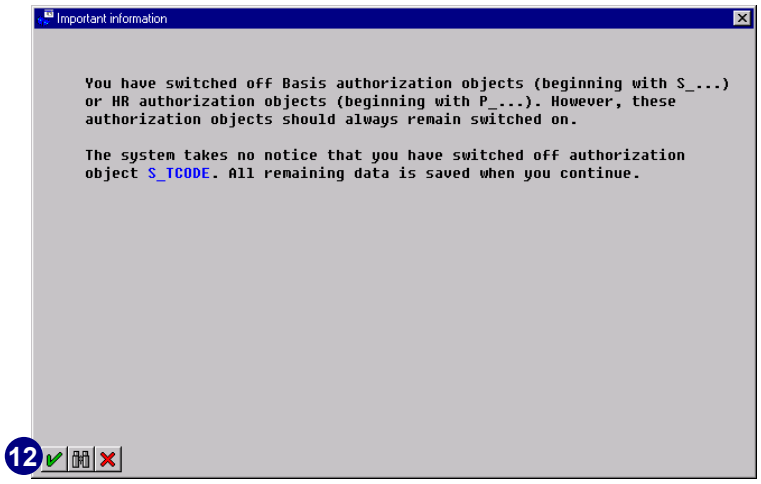
When you save and activate your data, the system also checks the authorization object *S_USER_OBJ*.

The values for the system parameter *auth/object_disabling_active* can be an *X* or blank. The *X* indicates that it is active and the blank indicates that it is not active. If it is not active your changes will not affect anything. However the default value is set to active.

11. Authorization objects beginning with *S_* or *P_* cannot be switched off.



12. Choose *Enter*.



You cannot globally deactivate authorization objects beginning with *S_* (Basis) or *P_* (HR) in transaction *AUTH_SWITCH_OBJECTS*.

No authorization data is inserted in the PG for deactivated authorization objects. In a release upgrade, the system does not display the transactions where authorization data is to be reprocessed if the corresponding authorization object is globally deactivated.

When you activate previously deactivated authorization objects, you may have to maintain the authorization data for a lot of activity groups.

If you activate previously deactivated authorization objects, these objects are not contained in any activity groups. In this case, in the transaction *PFCG* on the *Authorizations* tab, choose *Expert mode for profile generation* to generate profiles and the option *Read old status and merge with the new data*. Maintain any missing authorization values and regenerate the profile.

Generating the SAP Standard Menu and Company Menu

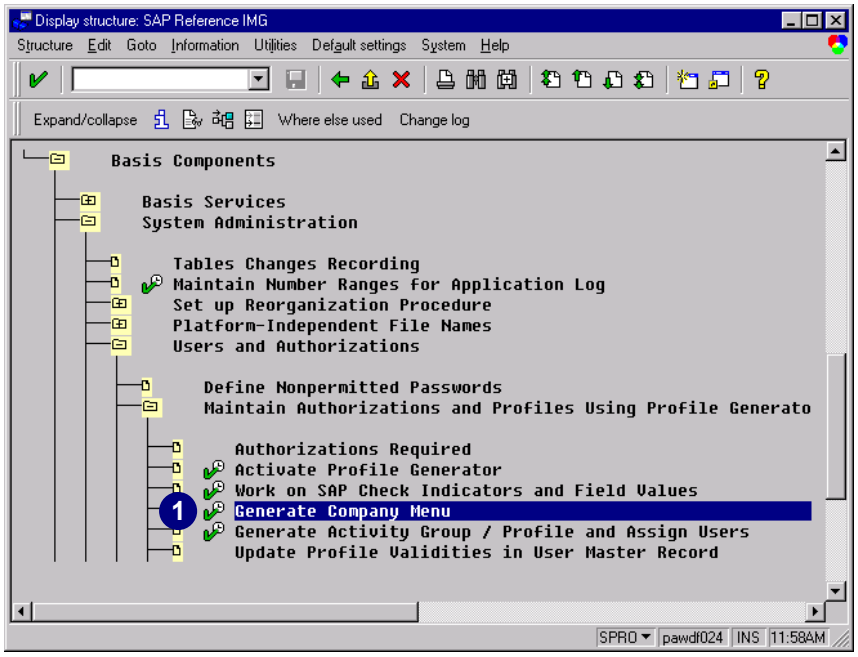
The SAP standard and company menus must first be generated before you can work with the activity group maintenance transaction *PFCG* (PG transaction) or the Session Manager.

Since the generated company menu is based on the application components chosen in the Enterprise IMG, first generate the Enterprise IMG and then generate the company menu.

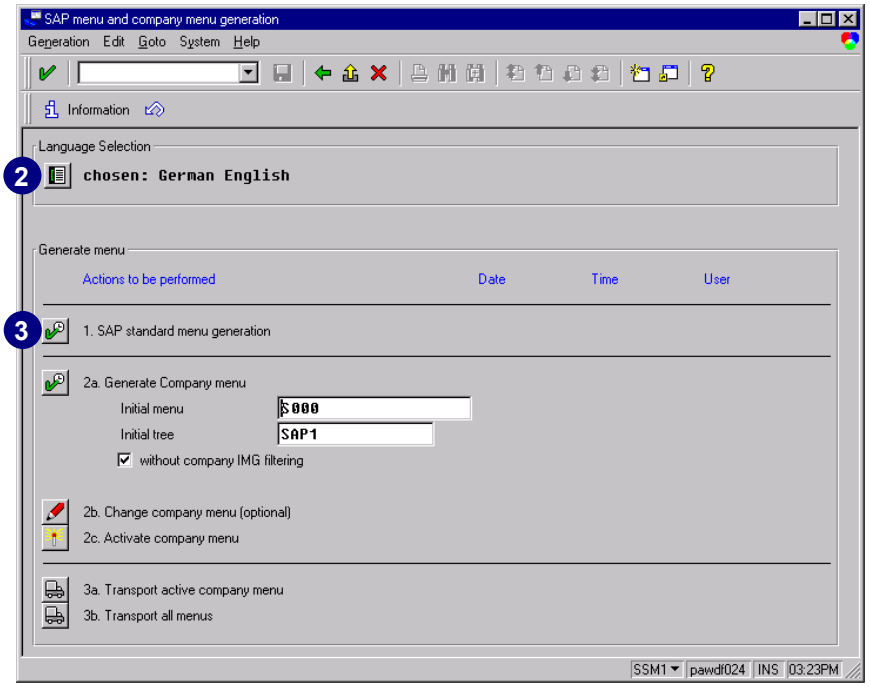
Generating the SAP Standard Menu

Follow the steps below to generate the SAP standard menu:

1. In the *Command* field, enter **`SSM1`** and choose *Enter* (or choose *Execute* next to *Generate Company menu*).



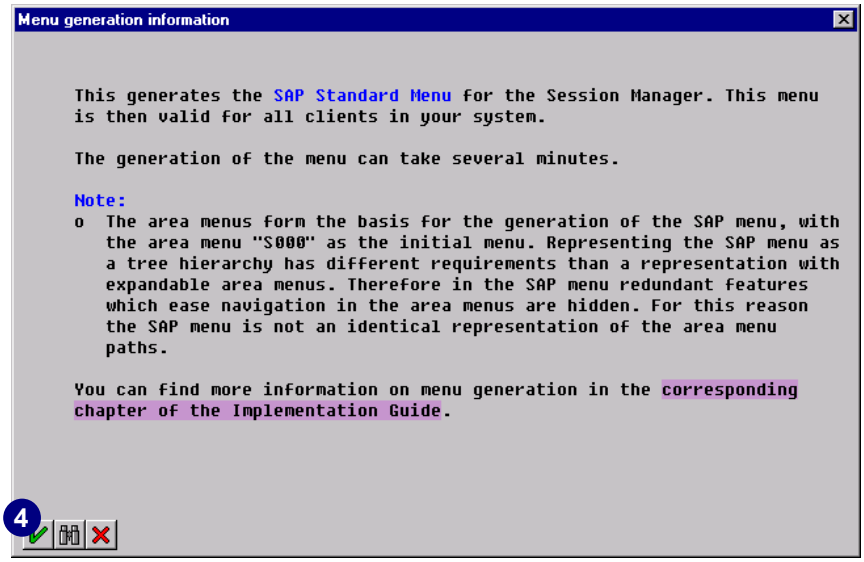
2. Verify the selected language(s). The default is the current language. Choose all the languages for which the menu is to be generated.



If a generation was executed before, you have to reset the generation first by choosing *Generation* → *Reset* from the menu.

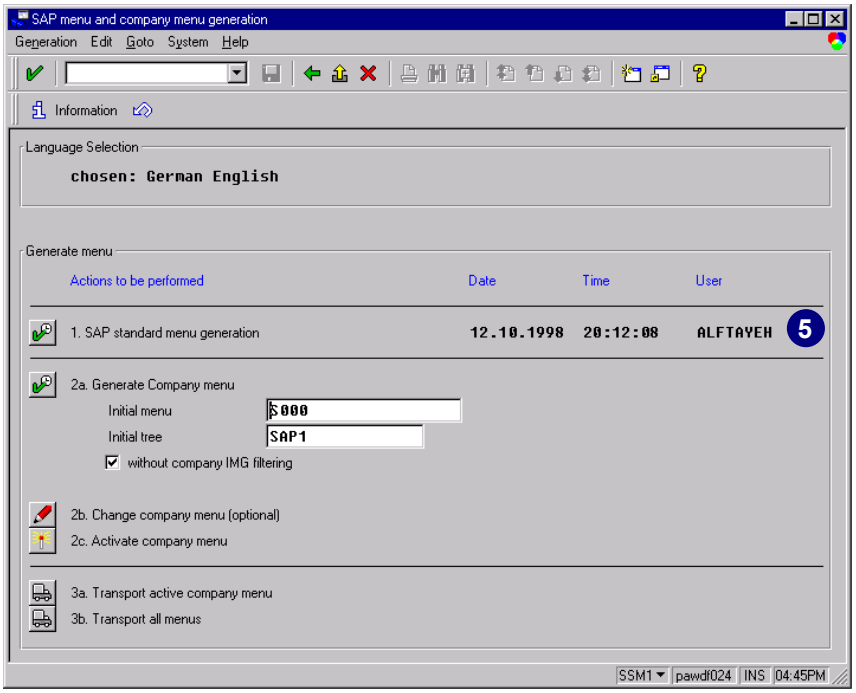
3. Choose *Execute* for *1. SAP standard menu generation*.

4. Choose *Enter* to begin the generation. This process may take a few minutes.



SAP Standard Menu Generation
The SAP standard menu must be generated before the Session Manager can display it. The entire SAP standard menu (menu code *S000*) and the SAP standard reporting tree (reporting tree *SAP1*) are used to generate the SAP standard menu.

5. The date and time information indicates that the generation was successful.



Generating the Company Menu

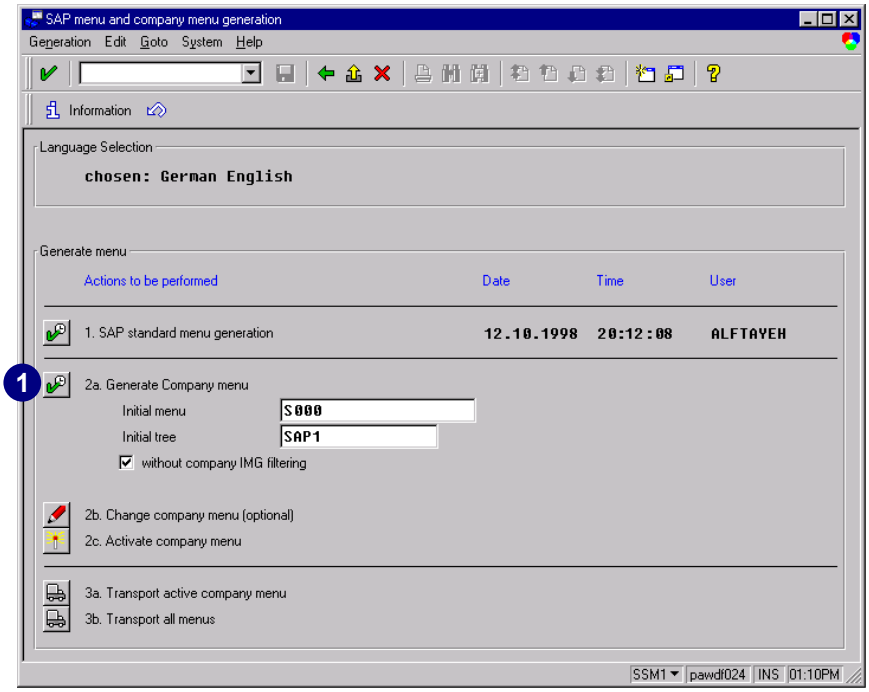
Company Menu Generation
The SAP standard menu (menu code *S000*) is proposed as your initial company menu, and the SAP standard reporting tree *SAP1* is proposed as your initial reporting tree. Therefore, the SAP standard menu must be generated before the company menu. This default setting should not be changed unless you want to use your initial menu or your reporting tree. You may, if you wish, overwrite the default proposal.

The SAP standard menu must be generated before the activity group maintenance transaction *PFCG* or the Session Manager displays it. During generation, the SAP standard menu tree is reduced by the application components that generated the Enterprise IMG. The resulting company menu shows only the transactions and reports you selected before generating the Enterprise IMG.

By default, the checkbox *Without company IMG filtering* is not selected. This default means that after generating the company menu, this menu will consist of only the application components selected during the Enterprise IMG generation.

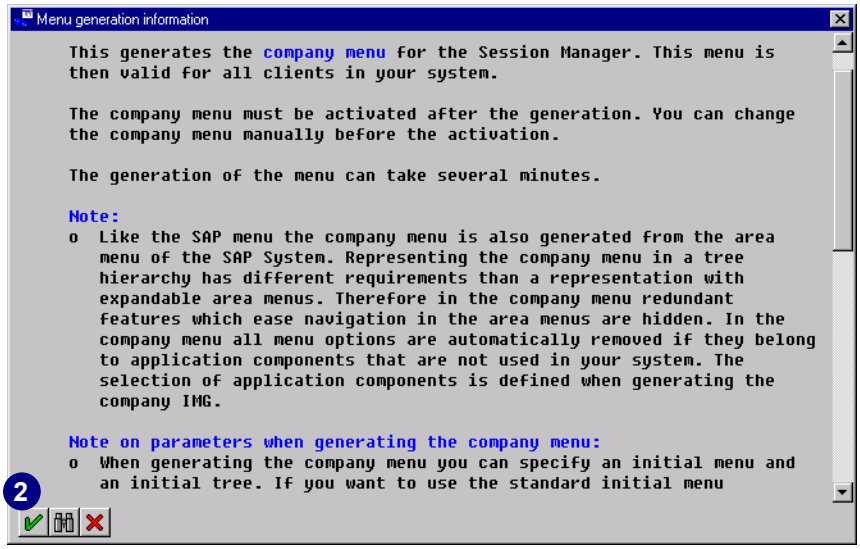
Thus, if you want your company menu to be identical to the standard SAP menu, select *Without company IMG filtering*. You can manually reduce the company menu from *2b* afterwards.

1. To generate the company menu, choose *Execute* next to *2a. Company menu generation*.



2. Choose *Enter* to begin the generation.

   This process may take a few minutes.

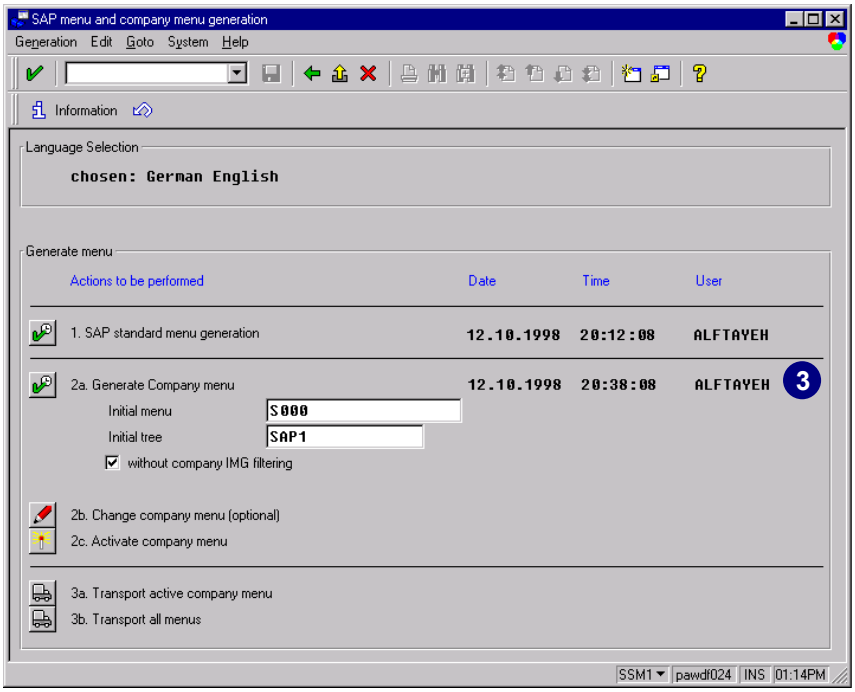


3. The date and time indicate that the generation was successful.

   You can manually change the company menu after it has been generated.

   If you want to change the company menu, follow the instructions in the next section.

   If you do not want to change the company menu, skip that section and continue with *Activating the Company Menu*.



Changing the Company Menu

Changing the Company Menu

If necessary, you can manually change the company menu after it has been generated.

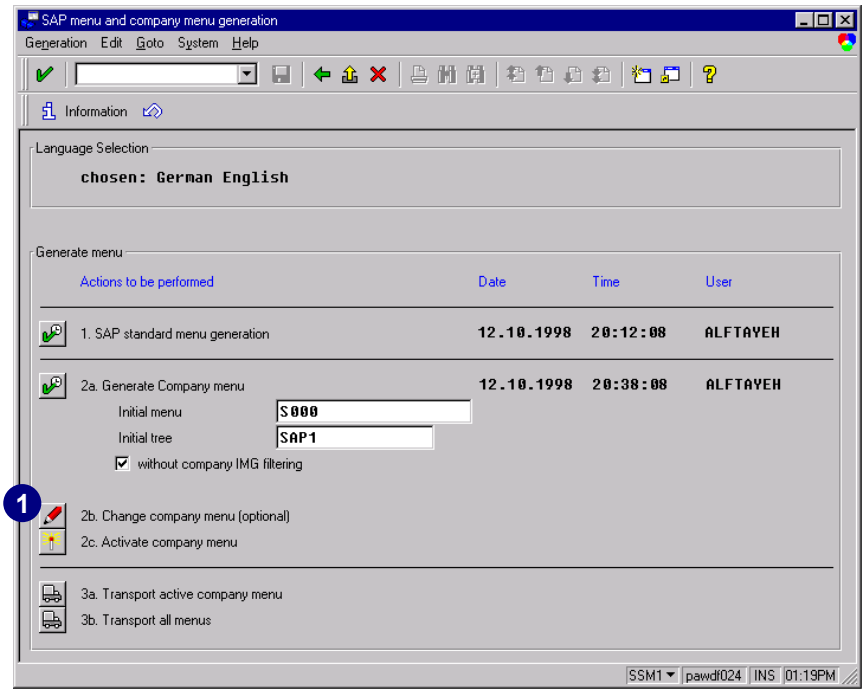
It does not make a difference here whether you have selected *Without company IMG filtering* in *2a* or not. If you did not select *Without company IMG filtering*, the SAP standard menu tree is displayed as your company menu. If you did select *Without company IMG filtering*, a company menu reduced to the application components you selected in the Enterprise IMG is displayed.

In either case, you can create your company menu tree from the displayed company menu. From this menu, only selected items are saved as your menu tree. These changes will take effect when your company menu is regenerated. Any deselected items will no longer appear in your company menu. To reselect these items, return to the menu and select them, and they will reappear when the menu is regenerated.

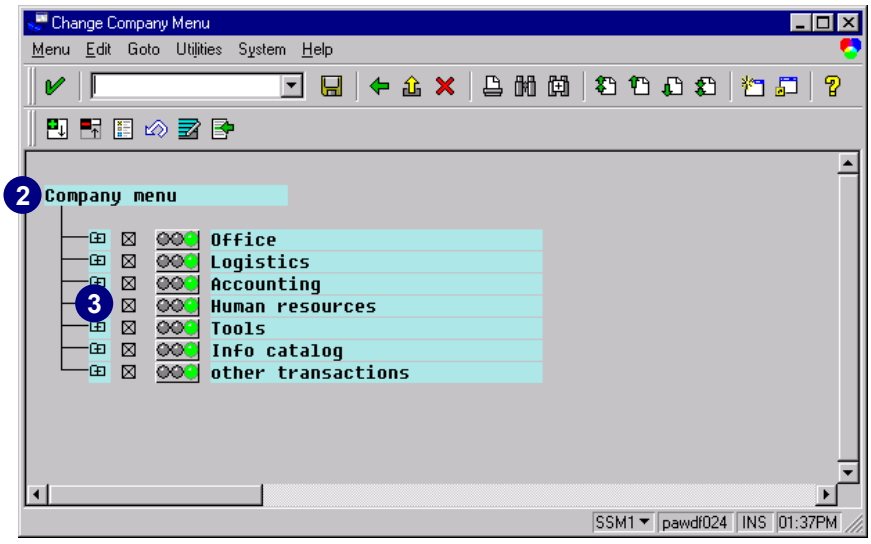
When a menu item is selected for removal, it is disabled at each connecting point to the corresponding area menus. This process assures consistency in the company menu since area menus sometimes reoccur in the same company menu. Therefore, selecting menu items for removal affects all occurrences of these items in corresponding area menus.

You can obtain an overview of menu items in several branches that may have been disabled by selecting *Refresh display* from the *Change company menu* screen.

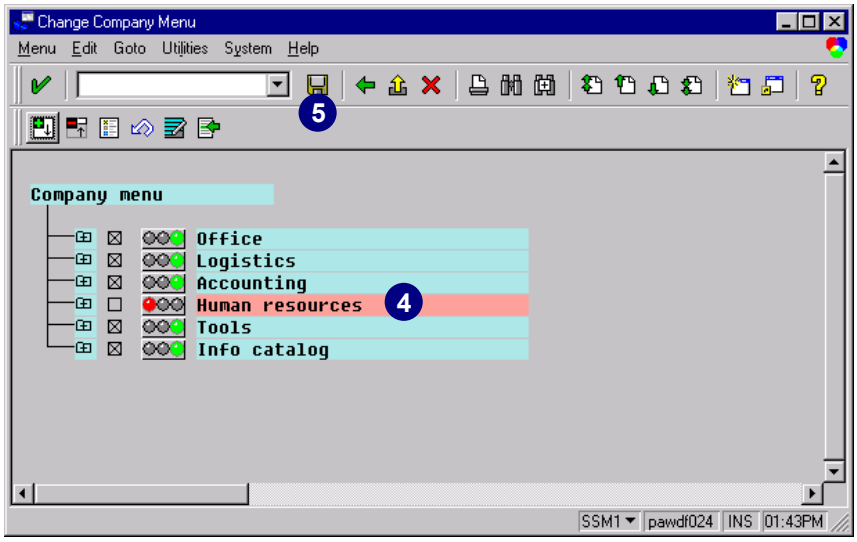
1. Choose *Change* next to *2b. Change company menu (optional)*.



2. You are now in *Change Company Menu* mode. Expand subtrees to deselect a function or a whole subtree.
3. For instance, click the checkbox for the subtree *Human resources*.



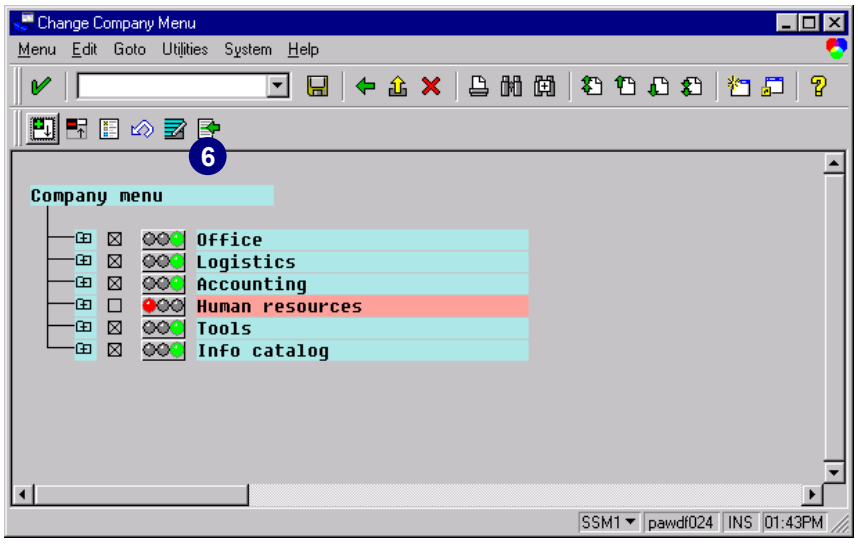
4. The subtree *Human resources* has now been deselected from your company menu.
5. When you have deselected all the items you want to remove from the company menu, choose *Save*.



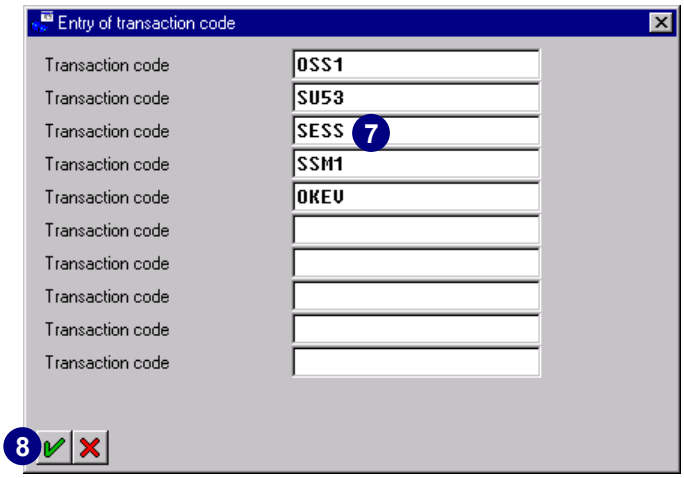
Manually Inserting a Transaction

The following steps illustrate how to manually insert transactions. Note that this transaction cannot be found in the standard menu (*S000*) but only displayed in transaction *PFCG*, in Session Manager, or transaction *SESS*. This method is an easy way to add customer-developed transactions to the company menu tree. Later, you can select the transactions from the company menu tree in the *Activity Group Maintenance* transaction *PFCG*. But then it is also necessary, with transaction *SU24*, to maintain the appropriate transaction code and its authorization checks.

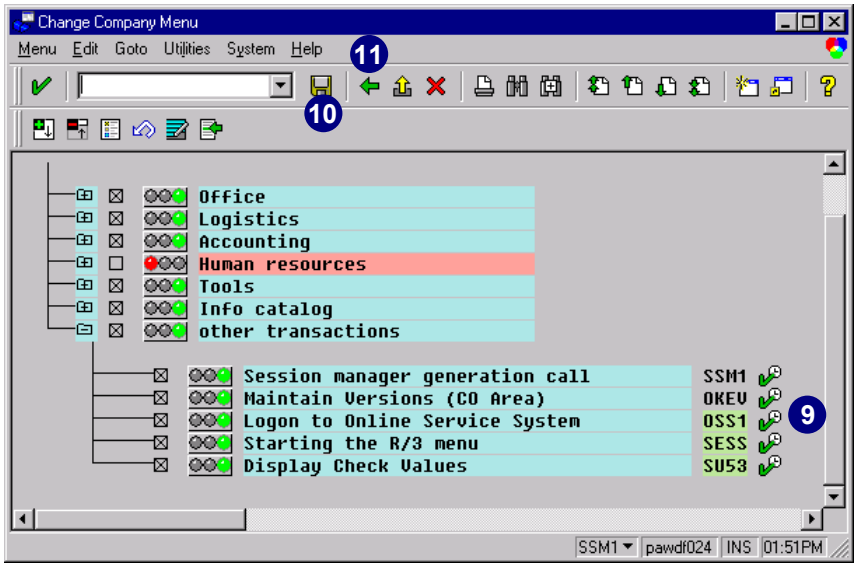
6. Choose *Insert transaction*.



7. Enter the transaction code (For example, **OSS1, SU53, SESS**, **SSM1** and **OKEV**).
8. Choose *Continue*.



9. The new entries are now displayed under *other transactions* in the company menu tree.

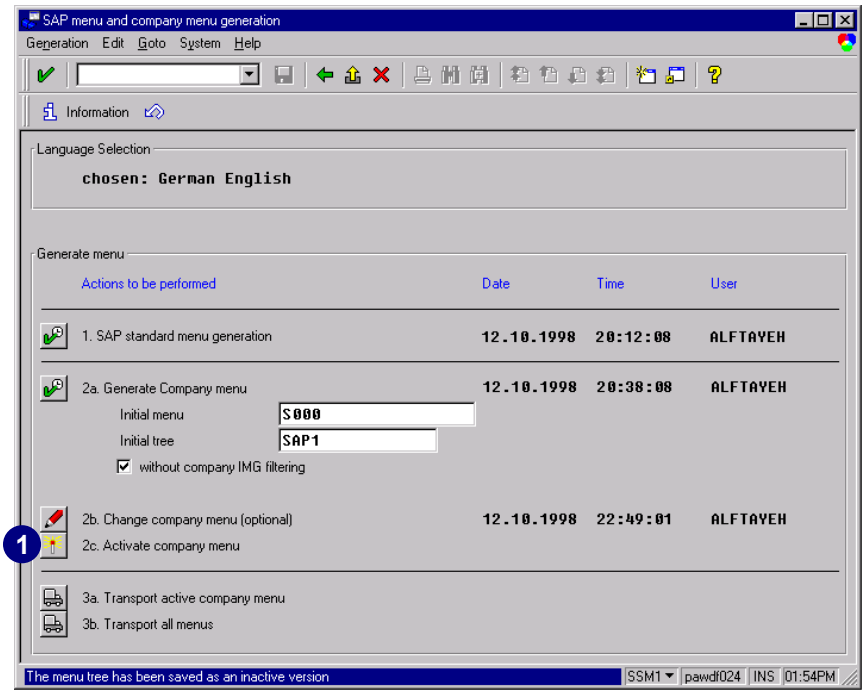


You can turn the technical names on or off, by choosing *Edit→ Technical name→ Technical name on/off.*

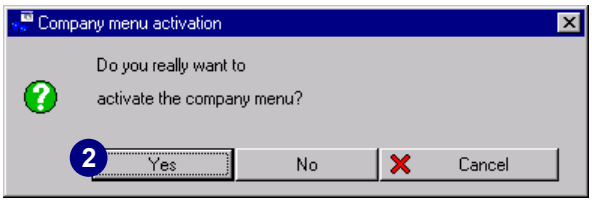
10. After manually inserting transactions, choose *Save*.
11. Choose *Back*.

Activating the Company Menu

1. Choose *Activate* next to *2c. Activate company menu*.

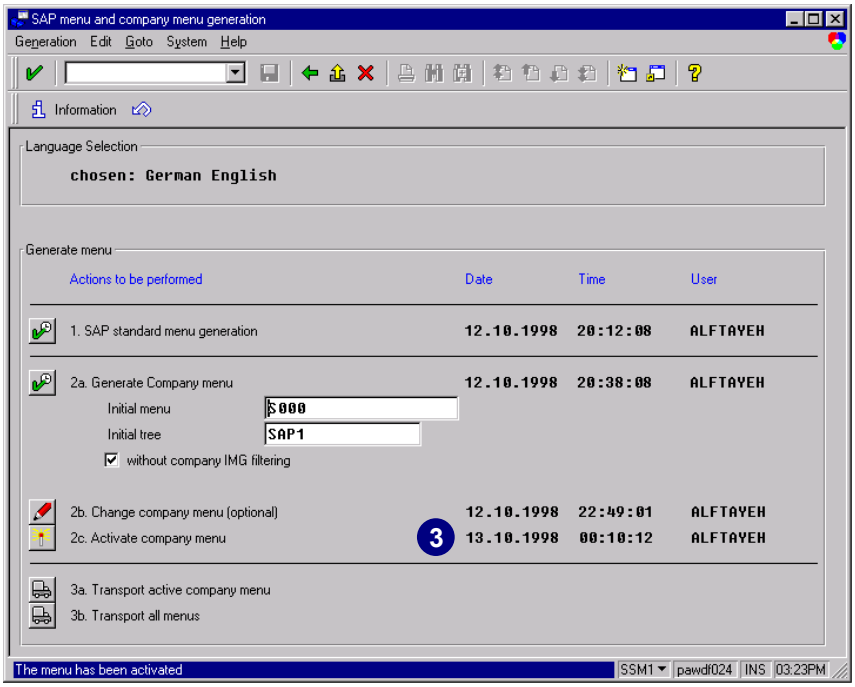


2. Choose *Yes*.



3. The company menu has been activated.

   For more information about the company menu, please read the following *TechTalk*.



Transporting Menus
The menus can be transported, assuming that they were not generated in the production system or that you want to import the menus into a second system with the same menu structure.

There are two variants:

- If only the active company menu is to be transported, complete activity *3a* in the associated section.
- If all menus are to be transported, complete activity *3b* in the associated section. In this case, you can continue to work on the company menu in the target system.

If you used a reporting tree as the initial screen to generate the company menu in activity *2a*, remember that the reporting tree specified as the initial tree must be included when transporting the active company menu.

Client-Independency of the Menu
The company menu generated is cross-client**.** Since the reporting trees are client-dependent, the reporting tree of the current client is used to generate the company menu. Note that regeneration of the company menu also changes the menu structure displayed in the Session Manager in all other clients. Therefore, you should perform the final generation in your production client.

Regenerate the SAP standard menu when the:

- System is reinstalled or upgraded
- Area menus have been changed

The company menu should be regenerated when the:

- SAP standard menu has been generated
- Reporting tree used has been changed
- Application component selection in Customizing has changed

Changing the Company Menu
If you have made manual changes to the company menu (step *2b* of the associated activity), these changes are retained, as much as possible, even after regeneration of the company menu. A regenerated or changed company menu is only displayed in the Session Manager when you have activated it. You can adjust the company menu to new circumstances and simultaneously continue to work with the active version of the Session Manager.

The active company menu is the basis to definite user menus**.** To define these menus:

1. Use transaction *PFCG.*
2. Define activity groups that can be assigned to users.
3. Assign menu items from the company menu to activity groups.

   Changes to the company menu thus affect all user menus.

These menus are also affected when company menu branches are disabled or changed, or if the company menu has been activated. If user menu items cannot be meaningfully assigned, they are flagged in a separate menu branch as "not to be assigned."

Important Note About Regenerating the Company Menu
Major structure changes made when the company menu is regenerated (for example, a changed initial menu or new reporting tree) can require extensive modification of the discarded company menu branches and active user menu items. This aspect should be remembered when making major changes to the company menu.

Generating the Menu in Several Languages
If you want to generate the menus in several languages, select all the languages you want and generate the menus as described earlier. You cannot select additional languages until you reset the generation by *Generation* → *Reset*. If it takes too long to generate several languages at once, generate each language separately.

To generate a language:

1. Select one language.
2. Generate the menus as described in activities 1, 2a, 2b, and 2c.
3. Reset the *Generate* command by choosing *Generation* → *Reset.*
4. Select a second language.
5. Carry out activities 1, 2a, and 2c.
6. Do not change the settings in activity 2a (initial menu and others).
   They should be exactly the same as when the first language was generated.
6. Repeat for additional languages.

Hiding Menus and Special Settings
You can hide menus from the entire company or hide (or show) certain menus for specific users. The standard setting displays all available menus. If you want to change the standard setting, read the section on changing the company menu on page 2–44.

The display of the menu tree can also be influenced in the SAPgui. If you want to change the standard setting, read the section on changing the menu tree display in the SAPgui. Complete those activities to change the standard configuration supplied by SAP.

To use the PC Session Manager you need a Windows '95 or later or Windows NT 3.51 or later frontend. Menu trees can be displayed in the. If you run transaction **`SESS`**, there is a SAPgui Session Manager available.

Getting Support from the Online Service System

A smooth security implementation of your project is important. The top priorities of the Online Service System are to support your work and speed up your implementation. Online Service System is an easy-to-use, direct communication link to SAP so you can quickly and efficiently obtain problem-solving information for R/3. Online Service System gives you a faster response time by allowing you to bypass the SAP help desk and enter problems directly into our database.

By entering problems or inquiries directly into Online Service System, you can:

- Take advantage of R/3 services, regardless of the availability and workload of the responsible help desk personnel
- Quickly report your problems
- Directly submit your problems to first-level customer service for processing

Accessing the Error Notes Database

Online Service System actively involves you in the problem-solving process by giving you direct access to SAP's interactive Error Notes database. This database contains error listings and solutions to common system problems. With Online Service System, you can view these solutions without submitting a problem message to first-level customer service. Direct access to the Error Notes database, with Online Service System, also provides helpful tips on avoiding potential problems.

Now is a good time to look at the Online Service System notes listed in appendix A. These notes will help you prepare for further R/3 security setup tasks.

Here are some hints to help Online Service System support you during the R/3 security setup:

1. Contact your system administrator for any further information about Online Service System.
2. Find out who already has access to Online Service System in your company.
3. Make sure you have access to Online Service System.
4. Log on to Online Service System and browse through the Online Service System notes in appendix A.

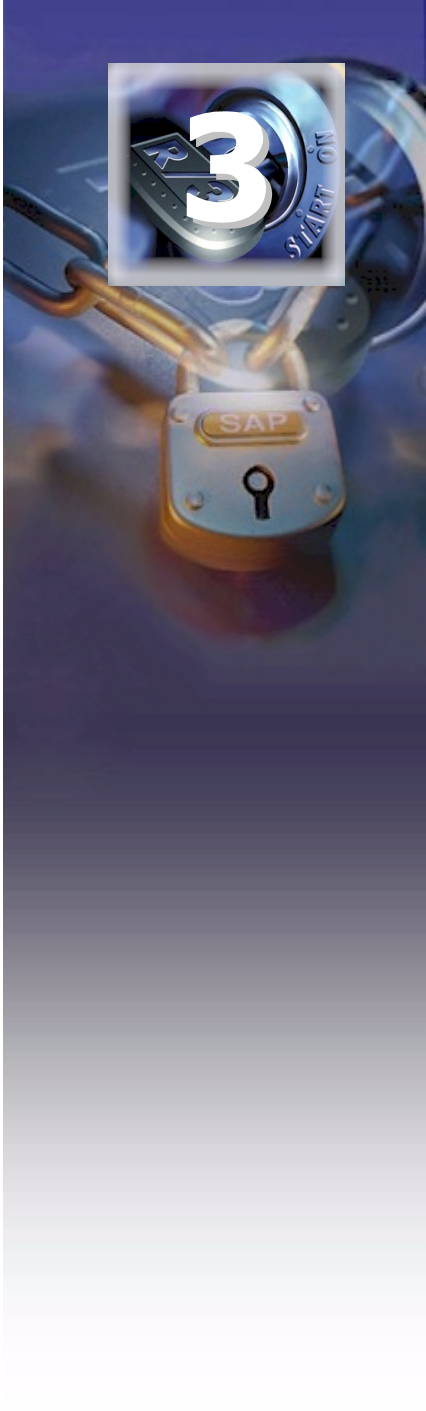
Printing Important Online Service System Notes

Since we will refer to certain Online Service System notes in this guidebook, please learn how to print an Online Service System note. The print function is not supported in Online Service System, so you must first download the note and print it locally. Read Online

Service System notes *26746* and *15641* to familiarize yourself with downloading and printing the notes. Before you continue, print out the Online Service System notes in appendix A and keep them as handy reference tools.

Applying Advance Corrections to Your R/3 System

The R/3 System needs certain corrections to perform properly. To apply these corrections in advance, refer to the following important Online Service System notes. Please check Online Service System note *97612* for the availability of the PG hot packages for Releases 4.5A and 4.5B.



Chapter 3: User Administration

Contents

Overview

R/3 allows you to define and maintain users and user authorizations by giving you precise control over user access. The definition and validation of authorization technology is integrated into the SAP development environment and is easily added to customer modules.

User administration in a productive environment is an ongoing process where users and authorization objects are:

- Created
- Deleted
- Changed
- Monitored

An administrator's role in this process differs depending on how user administration tasks are delegated.

System Users

Users are client-specific, which means that users must be separately defined for each client in your system. A user definition has many of the following components:

- Basic user data
  - Name
  - Password
  - Address
  - Company information
- User defaults
  - Logon language
  - Default printer
  - Date and decimal formats
- User profile information
  - Parts of R/3 a user can access
  - User groups
  - Active and expiration dates of a user's account

There are two ways to create users. First, from scratch, by defining the various user components; and second, by copying an existing user. When copying an existing user, you may also copy the defaults, address, and memory parameter settings.

External R/3 Users

External users include those created for Windows NT activities (<SAPSID>adm, Administrator, and SAPService <SAPSID>), and Database connections (SAPR3, DB Administrator, and SQL users).

Internal R/3 Users

Internal users are created and maintained in R/3. Each user is assigned one **user type**, which controls how the user interacts with R/3.

Internal user types include:

- Dialog
- Batch Data Communication (BDC)
- Background
- CPIC

Dialog

This user type handles online transactions and applies to the majority of your user population. Dialog users may log on and interactively work with R/3. These users are subject to authorization checks, require authorization profiles, and a password. Although it is not required, these users should be assigned to a user group**.**

Batch Data Communication (BDC or Batch Input)

This user type is used for authorization checks when processing a batch input session. These users cannot log on or work interactively and are subject to authorization checks.

Background

This user type runs background jobs. These users cannot log on and work interactively. The administrator can create background users with the necessary authorizations to perform a series of tasks. To define the background jobs, change the user field to the background user name you created. All authorization checks will go against the background user rather than the user creating the job. Although background users are unaffected by password control parameters, such as password expirations or character length, these users are subject to authorization checks.

CPIC

The CPIC user is delivered in client 000 with no authorizations and performs logons with the CPIC interface. This interface does not work interactively with R/3. The CPIC user receives return codes from external programs and the **statistic collectors** (refer to Online Service System note *3310*). SAPCPIC is no longer required for the transaction *SM51*.

This user, like all users, requires an authorization to perform the necessary activities in the R/3 System and is subject to authorization checks.

Special R/3 Users

SAP*

In clients 000 and 001, the R/3 System includes the default super user *SAP**. During installation, a user master record is defined for *SAP**. However, *SAP** is programmed in R/3 and does not require a user master record. After installation, once the user master record exists, use the password **06071992**. If the *SAP** user master record is deleted and a user logs on again as **SAP***, with the initial password **PASS**, then *SAP** is not subject to authorization checks and has the password **PASS**, which cannot be changed.

DDIC

The *DDIC* user maintains the ABAP Dictionary and the software logistics. A *DDIC* user master record is automatically created in clients 000 and 001 when R/3 is installed and has standard password **19920706**. This is the only user that can log on to R/3 during a new release installation. Protect the DDIC user from unauthorized access by changing the initial password in clients 000 and 001. This user is required for certain installation and setup tasks, so it should not be deleted.

EarlyWatch

The EarlyWatch user is only delivered in client 066 to every R/3 System with the initial password **SUPPORT**. It has access only to monitoring and performance data, and it is the user with which SAP's EarlyWatch experts work. This user should not be deleted, and the password should be changed. EarlyWatch should not be used for any purpose other than EarlyWatch functions.

Creating Users

User master records and authorization components are client-specific and must be separately defined for each system client.

Users are created either from scratch, using transaction *SU01*, or from a copy by:

- Using transaction *SU01*
- Creating a template user
- Copying it to other similar users
- Manually entering each password

The hierarchical security effect of user groups enables the administrator to distribute user maintenance tasks and maintain high security. Within a specific group, security tasks can be distributed in such a way that three people are required to create users and manage activity

groups and authorizations. Thus, user and authorization administrators can only complete certain parts of the required tasks. This process ensures that no one person can circumvent R/3's authorization scheme. If a company has a centralized organizational structure, all maintenance tasks may need to be performed by a single user, the so-called superuser.

For security reasons, the responsibility for the following maintenance tasks should be distributed among three different administrators (see chapter 1 for additional information).

User Groups

User groups enable the administrator to provide application managers with the rights required to control their users. Thus, these managers can control all users in their user groups and users not yet assigned to a user group. Application managers cannot, however, alter users in other user groups.

Although a user group affiliation is not required when you create users, this affiliation is necessary to delegate user maintenance tasks to application managers and staff. Later, we will show how to distribute user administration tasks to the appropriate application personnel.

User groups are normally based on the requirements dictated by the different application groups. The number of users in each user group also influences these groups. Since user groups distribute user administrative tasks, your user groups will be based on the available organizational support structure. A few things to remember when working with user groups are that:

- User groups are created with transaction *SU01* (*Tools* → *Aministration, User maintenace* → *Users, Environment* → *User groups*).
- User groups affect nothing until you set up your group administrators within a user group.
- Each user can only belong to one user group.
- User groups can be maintained before they are assigned to users.

Authorizations and Authorization Profiles

Authorization profiles allow you to organize access privileges by task or job function. Specifically, this profile contains the access privileges needed to perform particular jobs, such as data entry or application maintenance. To authorize a user for a job, you only need to give the user the corresponding authorization profile. The Profile Generator (PG) simplifies the task of setting up authorization profiles.

Mass Operations

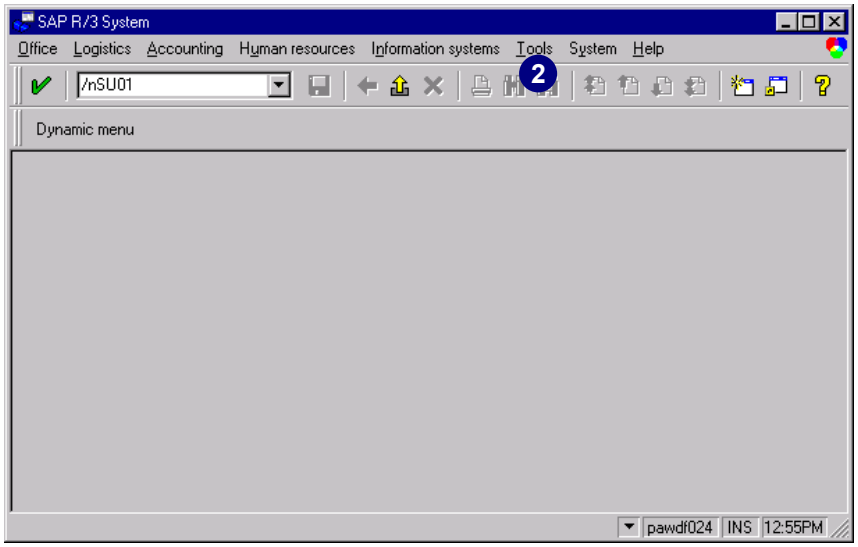
The R/3 System provides two utilities for performing operations on all, or a selected set, of users:

- Choose *Environment* → *Mass changes* → *Delete all users* to delete all users from a designated client. A confirmation screen appears before the deletion is carried out.
- In a client, choose *Environment* → *Mass changes* → *User profile* to add or delete a profile from all or a selection of user master records. Use this utility only if you have manually maintained the authorization profile in these user master records. That is, you did not assign activity groups to these users nor update the user masters.

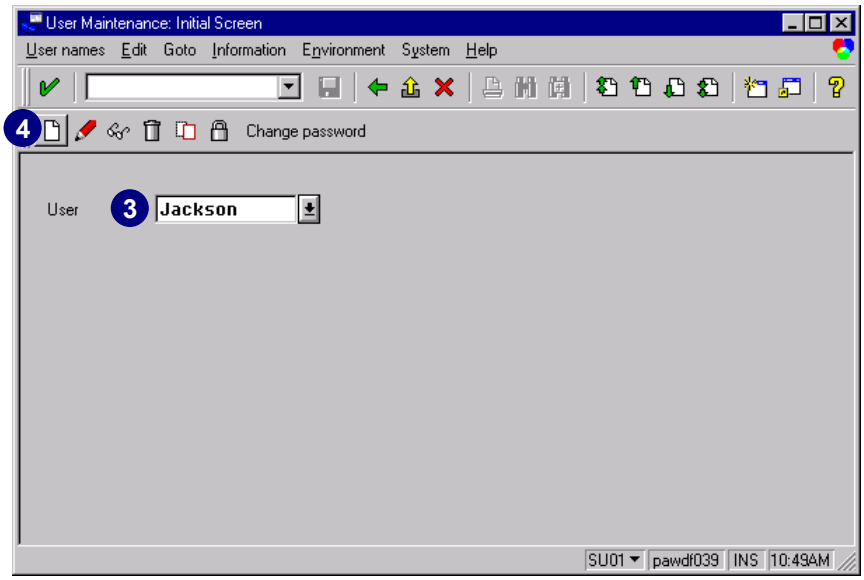
Creating a New User

Do not create or change users in clients 000, 001, or 066. Client 000, the standard SAP client, should be copied to create other new clients.

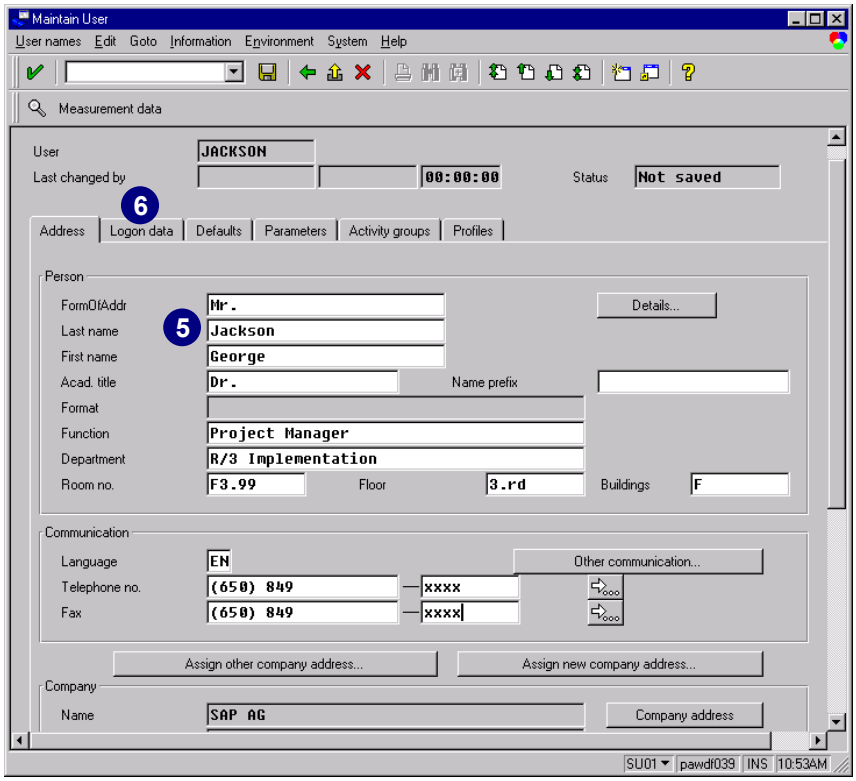
1. Log on to the SAP client where you wish to create a new user.
2. In the *Command* field, enter transaction **SU01** and choose *Enter* (or choose *Tools* → *Administration* → *User maintenance* → *Users*).



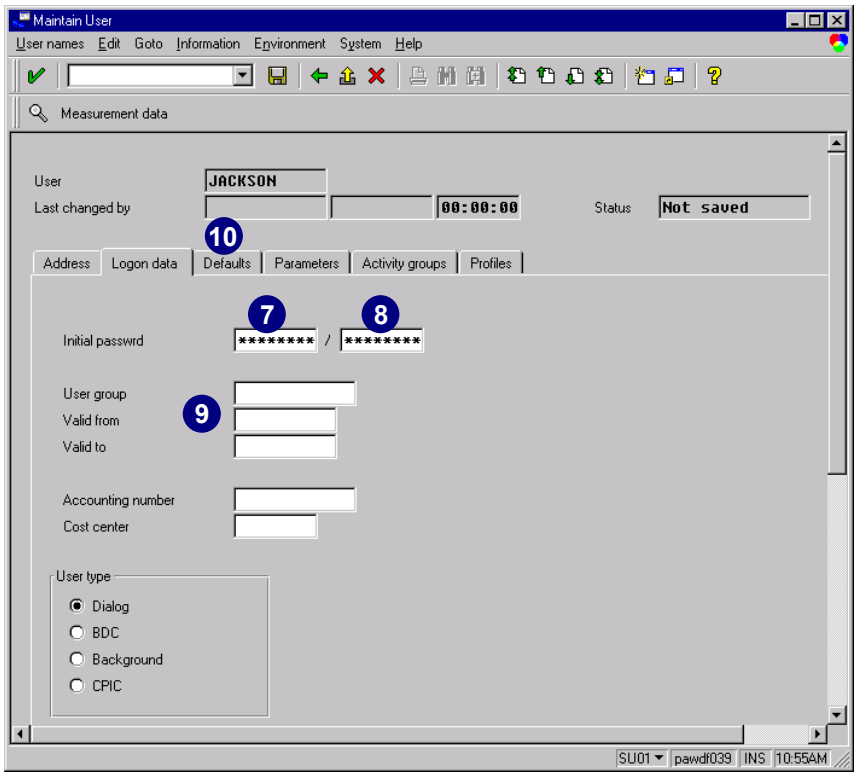
3. In the *User* field, enter the new user name.
4. Choose *Create*.



5. Enter at least the last name. You may enter the *Person, Communication*, and *Company data* now, or return to it later.
6. Choose the *Logon data* tab.



7. Enter an *initial password* (for example, **`init`**).
8. Press *Tab* and re-enter the password to verify the spelling.
9. You may edit other *Logon data* fields, such as *User group*, *User type* as needed (see TechTalk below).
10. Choose the *Defaults* tab.



Logon Data Field Definitions

User group

Assigning users to groups allows the user maintenance task to be distributed among several user administrators. A user may only belong to one user group.

Valid from/ Valid to

These fields are useful if you are creating a temporary user, such as a contractor. To immediately activate the user, leave the *Valid from* field blank. For a user with no anticipated termination date, leave the *Valid to* field blank, which allows indefinite access.

Accounting number

This field is for a freely selectable accounting name or number. If you use the SAP accounting system, the user's system usage is assigned to this account. The accounting name or number may be unique to each user or can be shared among groups of users.

Cost Center

Use this field for the user's cost center number.

Dialog

Select this field for normal dialog users.

BDC

When you process a batch input session, select this field for users who are only used for the authorization check.

Background

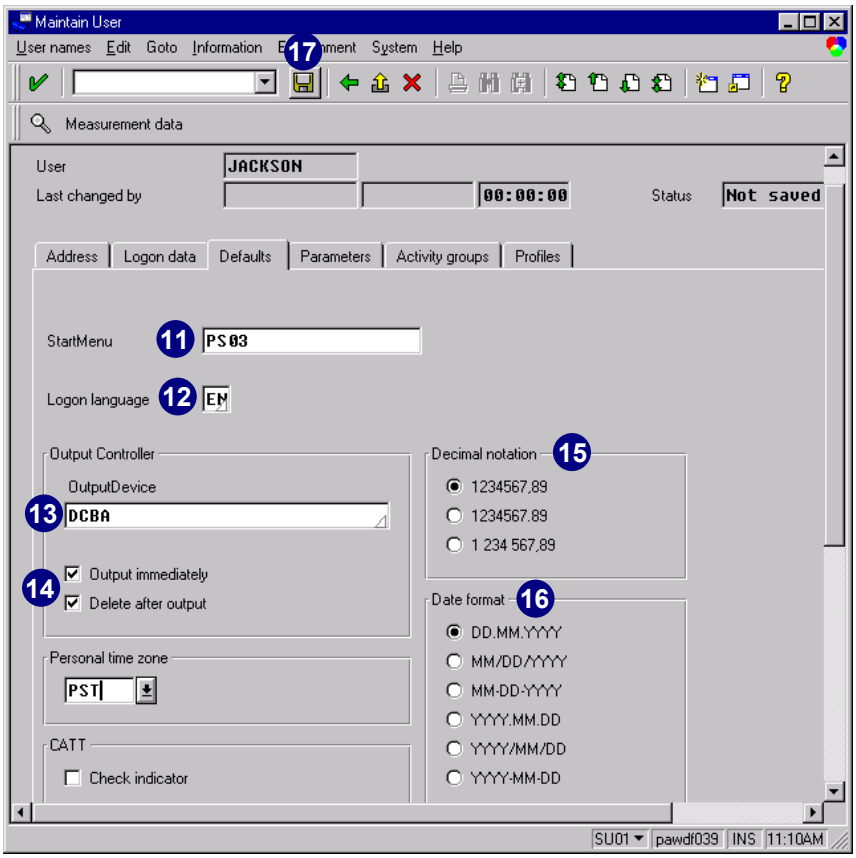
Select this field for users who are authorized to execute batch runs.

CPIC

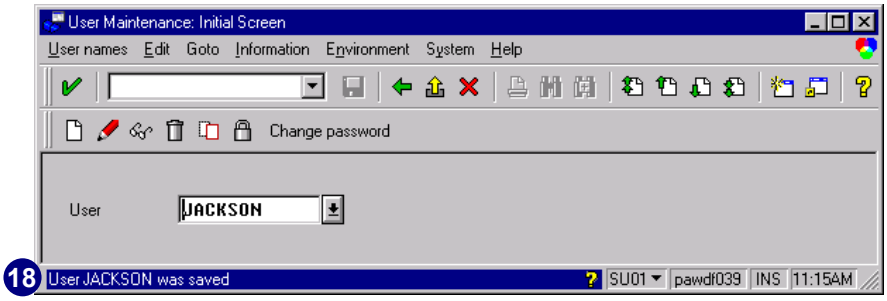
Select this field for users who are authorized to execute CPI-C calls.

11. You may either enter a *StartMenu* or leave the field blank.
12. Enter a language code in the *Logon language* field.
13. Enter a default *Output device* (the printer or file to which the user will automatically print).
14. We recommend selecting *Output immediately* and *Delete after output*.

    Output immediately releases spool requests. Otherwise, spool requests stay in the spool system until manually released. The *Delete after output* option prevents spool requests from being retained after printing.
15. Select the *Decimal notation*.
16. Select a *Date format*.
17. Choose *Save*.



18. The new user was saved.



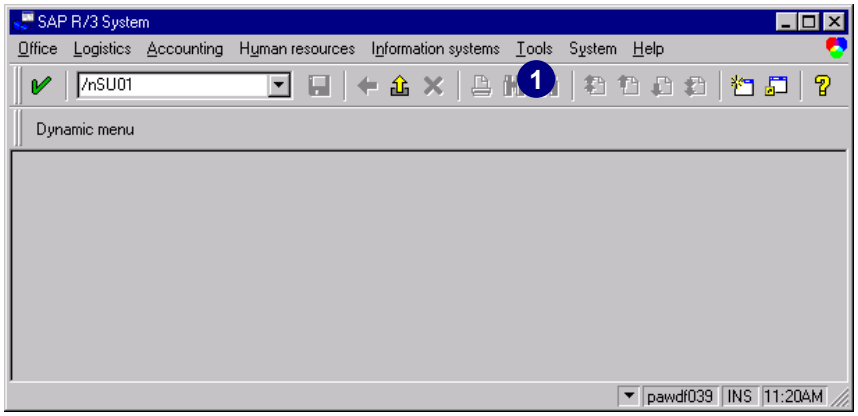
For each user, field defaults or **parameters** store default values for R/3 fields. When a field is displayed, the parameter's value (if any) is a default value. User parameters are optional and do not yet need to be defined.

To assign an authorization profile to your new user master record:
1. Create the activity group (see chapter 4).
2. Generate authorization profiles for the activity groups (see chapter 5).
3. Assign activity groups to new users and transfer profiles (see chapter 7).

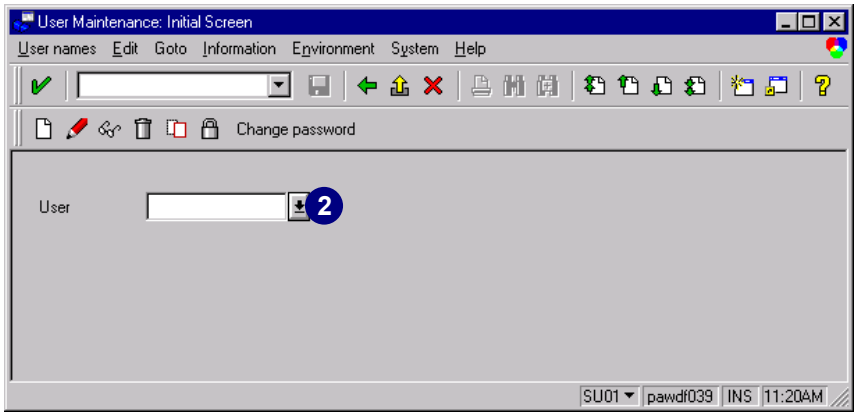
For more information transporting user master records, please refer to chapter 11.

Listing All Defined System Users

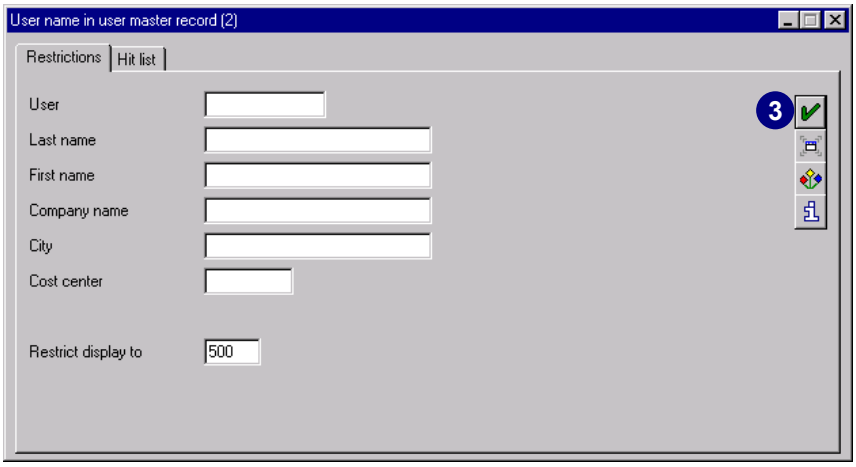
1. In the *Command* field, enter transaction **`SU01`** and choose *Enter* (or choose *Tools* → *Administration* → *User maintenance* → *Display users*).



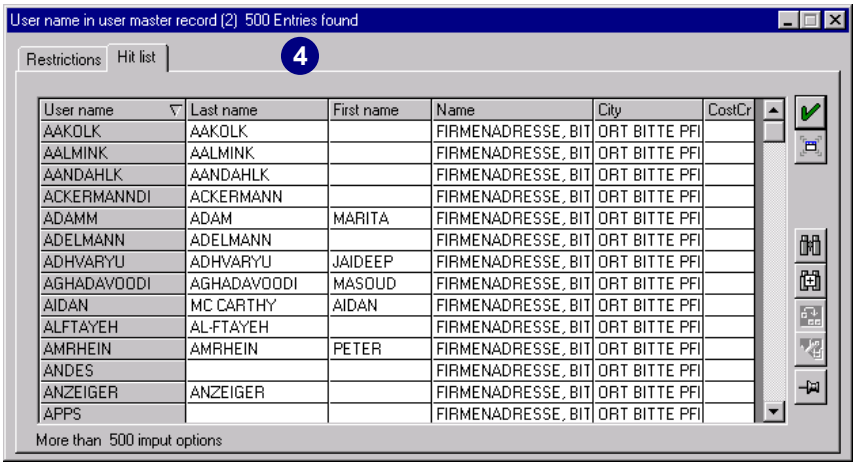
2. For *User* choose *possible entries*.



3. To display a list of all defined users, leave the available fields blank and choose *Start search*.



4. A list of all system users now appears.

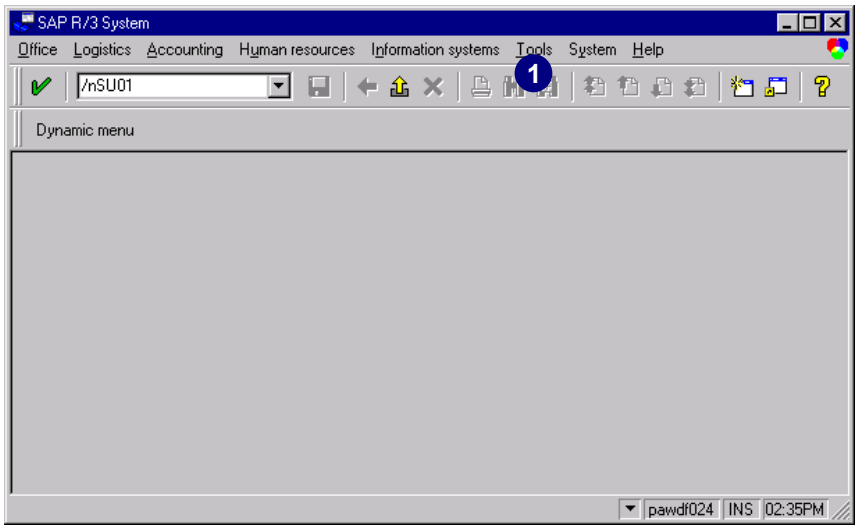


Changing a User's Password

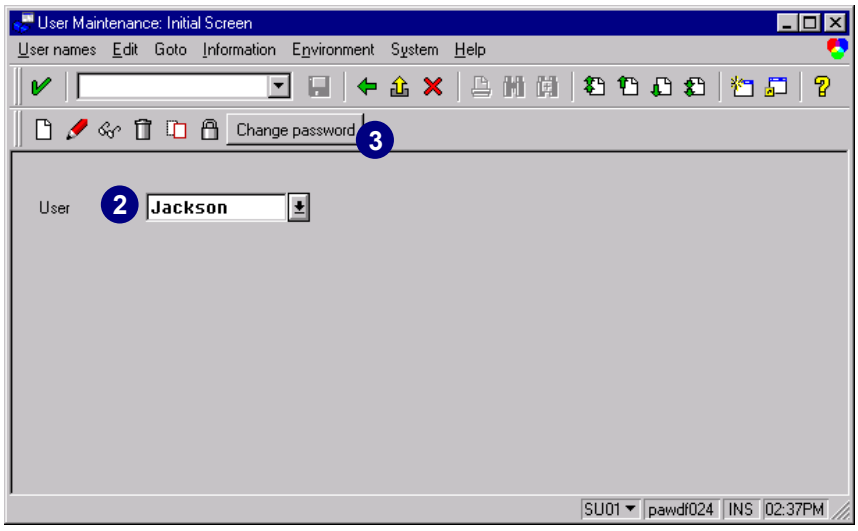
Users can change their own passwords and administrators can change any user's password. Users may only change their passwords once a day; however, an administrator can change passwords whenever required. An administrator may need to change passwords after a new installation (when the default password should be changed for security purposes), or when users lose or forget their passwords. When an administrator changes a password, the new password is only temporary. At the next logon, the user enters this password and then selects a permanent one. Please refer to the table at the end of this chapter for password requirements.

Users are client specific. Before proceeding, be sure that you are logged on to the SAP client that contains the user whose password you want to change.

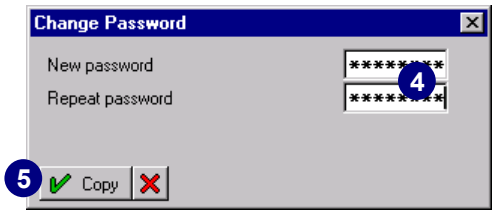
1. To change a user's password, in the *Command* field, enter transaction **`SU01`** and choose *Enter* (or choose *Tools* → *Administration* → *User maintenance* → *Users*).



2. Enter the name of the user whose password you would like to change.
3. Choose *Change Password*.



4. Enter the new initial password (for example, **`init`**). Press *Tab* and re-enter the password for verification.
5. Choose *Copy* to change the password.



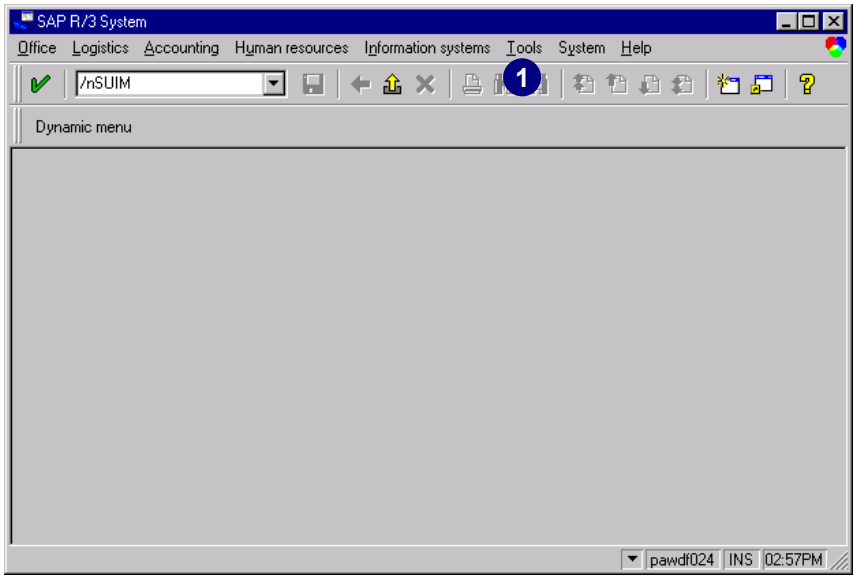
Password Requirements

The following table is a list of password requirements and whether these requirements can be customized. Appendix C also lists important system profile parameters to customize password settings.

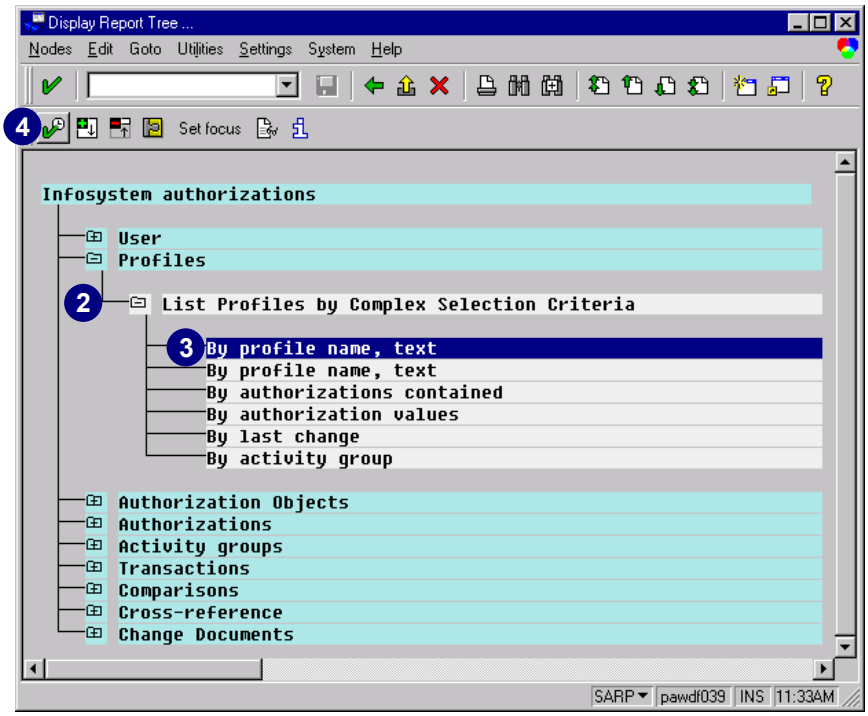
Password Requirements	Default	Options
Minimum length is three characters		Minimum length can be increased.
Expiration	Password must not be changed	Number of days after which a password must be changed can be set.
Password may not be set to any value in a lockout list	No passwords are blocked other than PASS and SAP*	Can be customized.
First character may not be an exclamation point (!) or question mark (?).	Fixed in the R/3 System	
First three characters may not appear in the same sequence in the user ID.	Fixed in the R/3 System	
First three characters may not be identical.	Fixed in the R/3 System	
Space character not allowed within first three characters.	Fixed in the R/3 System	
Password may not be **`PASS`** or **`SAP*`**.	Fixed in the R/3 System	
Any keyboard character is allowed in a password. Passwords are not case-sensitive; no distinction is made between upper- and lowercase letters.	Fixed in the R/3 System	
Users can change their passwords only once a day. This restriction does not apply to user administrators.	Fixed in the R/3 System	
A password may not be changed back to a user's previous five passwords. This restriction does not apply to user administrators.	Fixed in the R/3 System	

Displaying a Generated Authorization Profile and its Authorizations

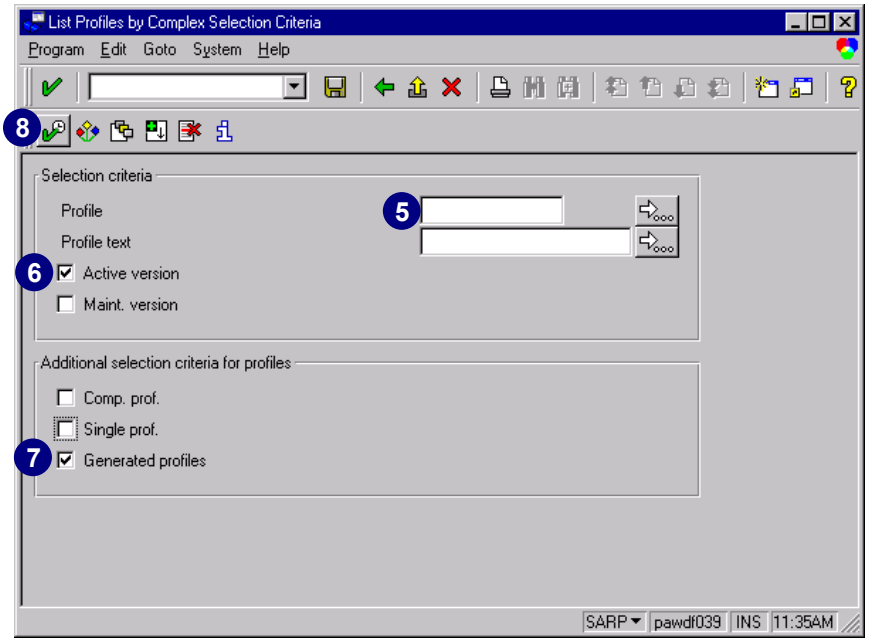
1. In the *Command* field, enter transaction **SUIM** and choose *Enter* (or choose *Tools* → *Administration* → *User maintenance* → *Repository Infosys*.).



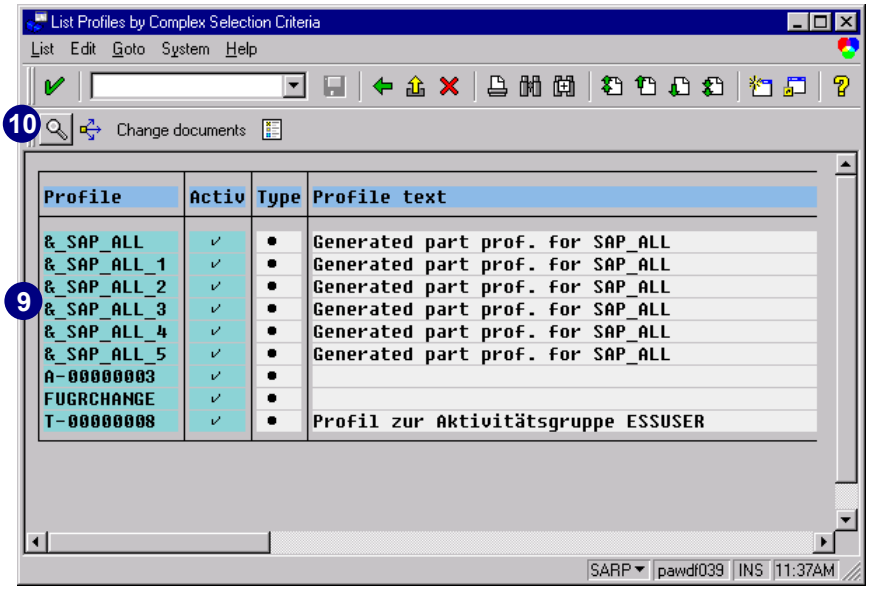
2. From the *Infosystem authorizations* tree, choose *Profiles* → *List Profiles by Complex Selection Criteria* → *By profile name, text.*
3. Select the line *By profile name, text.*
4. Choose *Execute.*



5. In the *List Profiles by Complex Selection Criteria* screen, enter either the name of your generated authorization profile or leave the *Profile* field blank.
6. Select *Active version*.
7. Select *Generated profiles*.
8. Choose *Execute*.

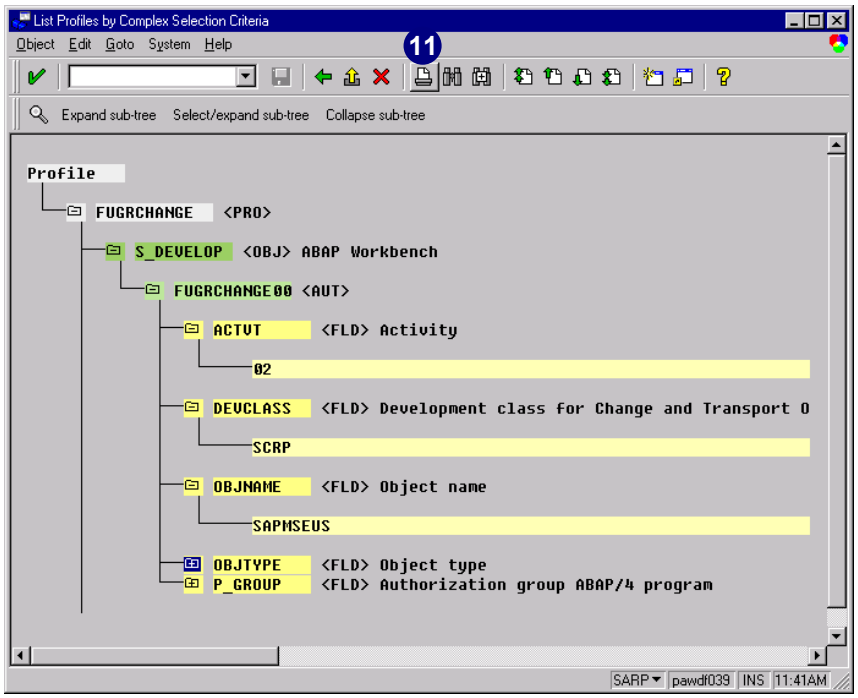


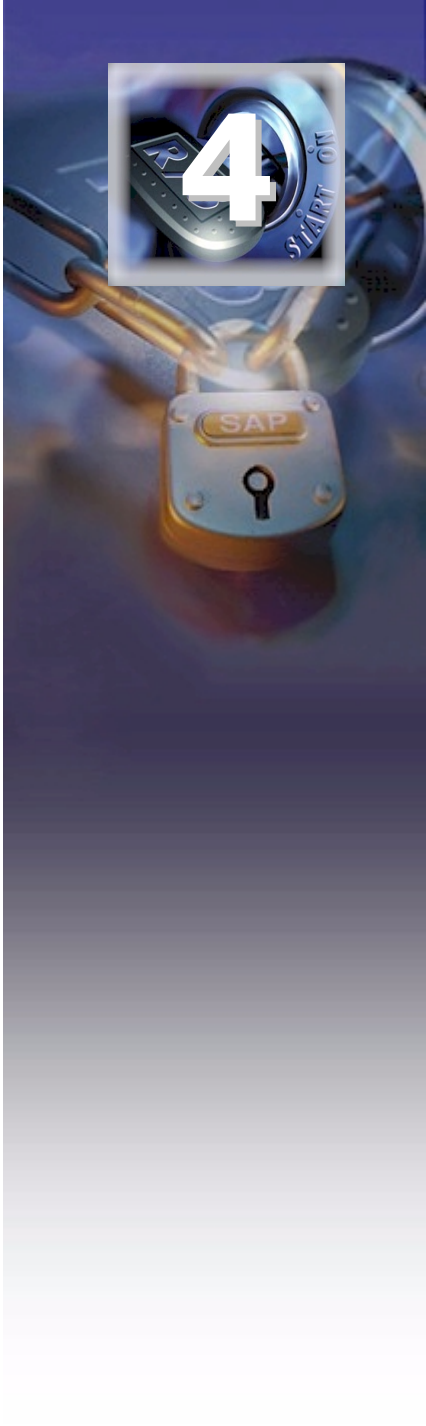
9. Position the cursor on the authorization profile you would like to look at.
10. Choose *Choose*.



11. The selected authorization profile appears with all its authorizations.

    Choose *Print* to print the list.





Chapter 4: Working with Activity Groups

Contents

Overview

The activity group maintenance transaction *PFCG* allows you to create, maintain, and assign activity groups to objects such as:

- R/3 users
- Positions
- Persons
- Jobs
- Organizational units
- Work centers

Activity groups are used by the Profile Generator (PG) to generate authorization profiles. The first priority is to select transactions and reports from the menu tree. This information (transactions codes, menu paths, report names, etc.) is saved in an activity group, which serves as a database to help the PG determine the necessary authorizations and generate the profile(s).

The activity group maintenance transaction assists and supports employees working with *SAP Business Workflow*, *SAP Session Manager*, and *Personnel Planning and Development* (PD). These areas require activity-oriented information to function. The activity group maintenance transaction streamlines processes so that maintaining this information is faster and easier.

You may set up as many activity groups as your company requires. A single activity (a transaction, a report, or a task) can be included in many different activity groups, and an activity group can include as many single activities as needed.

To set up activity groups:

1. Provide basic information to identify the activity group.

   This task is mandatory. Please see *Providing Basic Details* on page 4–5 for more information.

2. Select the reports and transactions that should be included in the activity group.

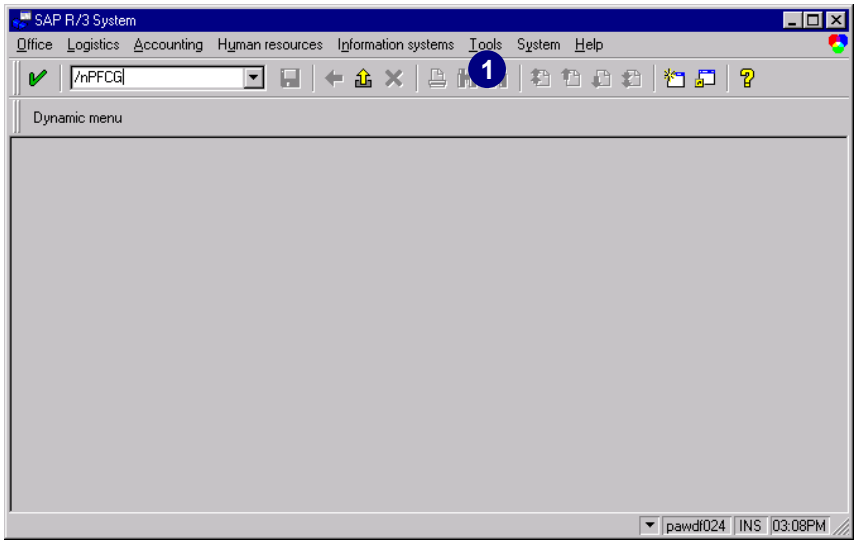
   This task is not mandatory but is usually recommended. Please see *Selecting Reports and Transactions* on page 4–6 for more information.

3. Choose the tasks that should be included in the activity group.

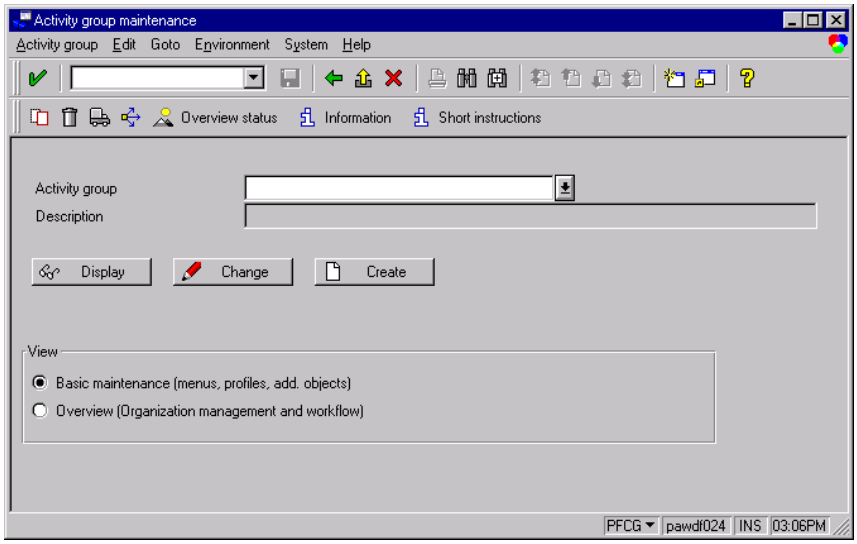
   Although this task is not mandatory, it is recommended if you use SAP Workflow. Please see *Selecting Workflow Tasks* on page 4–27 for more information.

Starting Activity Group Maintenance (PFCG)

1. In the *Command* field, enter transaction **PFCG** and choose *Enter* (or choose *Tools* → *Administration* → *User maintenance* → *Activity groups*).



The *Activity Group maintenance* window appears.



Selecting Views in Activity Group Maintenance

In the *Activity Group Maintenance* window, you can toggle between *Basic maintenance* and *Overview*.

Basic Maintenance

Select *Basic maintenance (menus, profiles, add. objects)* to create activity groups and assign these groups to R/3 users.

Overview (Organization Management)

Select *Overview (Organization management and workflow)* to create activity groups and assign these activity groups to R/3 users or PD objects. *Overview* gives you full access to all activity group maintenance functions, including organization management and the related time dependencies. For example, when you are creating or changing an activity group, you can only link workflow tasks to an activity group in *Overview*.

Creating Activity Groups

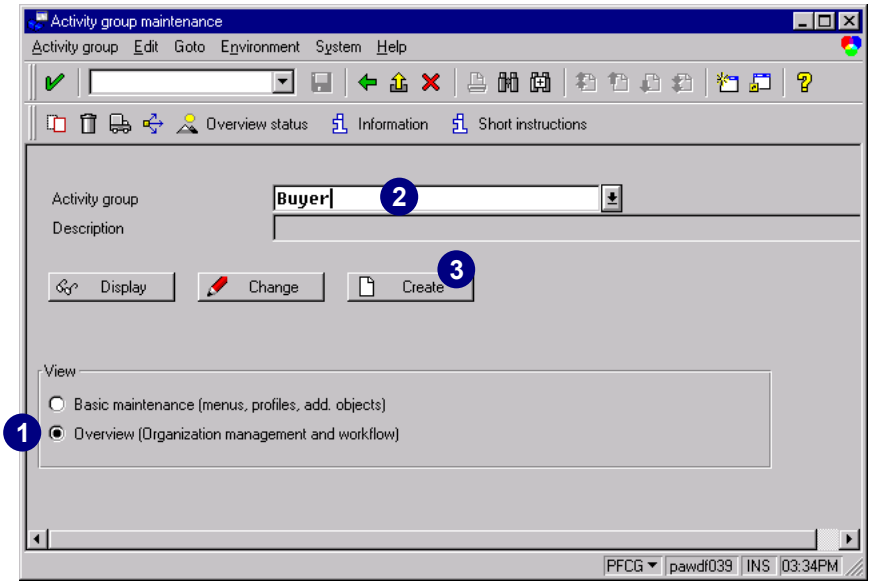
Creating activity groups involves three tasks:

- Providing basic details
  This task is mandatory.
- Selecting reports and transactions
  This task is not mandatory but is usually recommended.
- Selecting tasks
  This task is not mandatory, but if you use SAP Workflow, it is recommended.

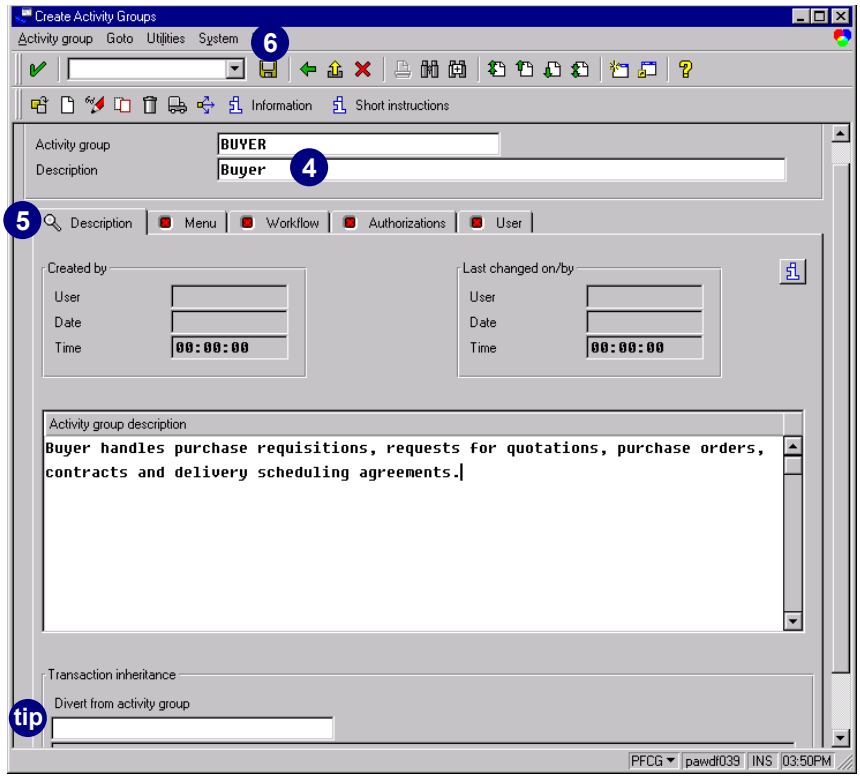
Each of the above tasks is described in greater detail in the following section.

Providing Basic Details

1. Select *Overview* (so we can use Organizational management and workflow).
2. Enter the name for your new activity group in *Activity group*. The name can be any name that does not begin with a namespace prefix or the prefix SAP (for example, **BUYER**).
3. Choose *Create*.



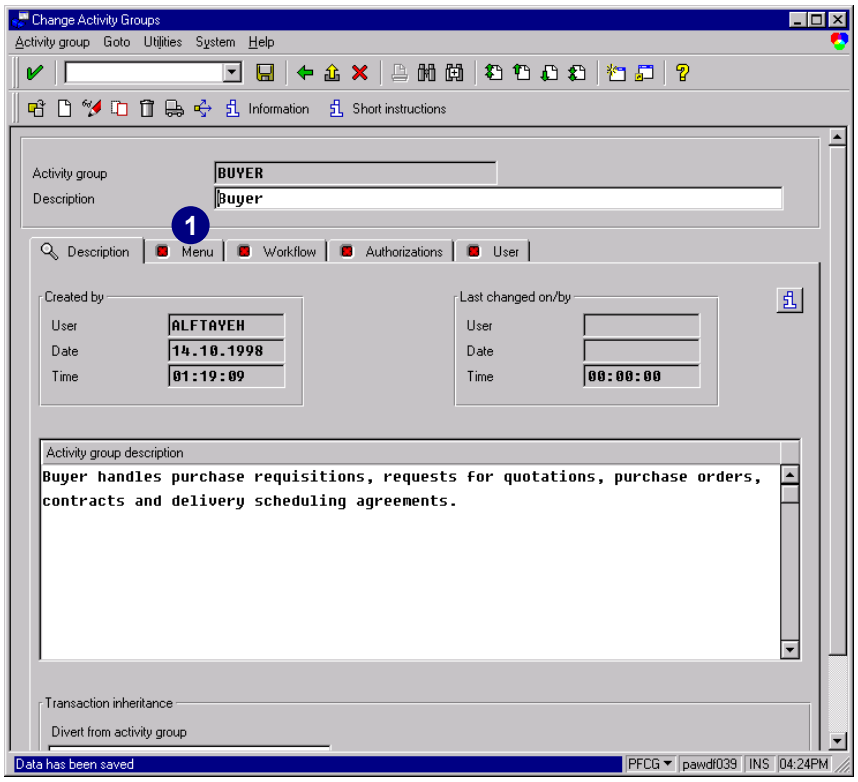
4. Enter a short description for your activity group, no more than 63 characters (for example, entered **Buyer**).
5. The *Description* tab contains creation and change information that was created automatically for the *User*, *Date,* and *Time* after you save. You can also create a detailed description for the activity group in the field *Activity group description*.
6. Choose *Save*.



If you enter the name of an activity group in the *Divert from activity group* field (the translation is wrong it should say derived from activity group), its transactions will be inherited by the new activity group. (See the section *Deriving Activity Groups* on page 4–18.)

Selecting Reports and Transactions

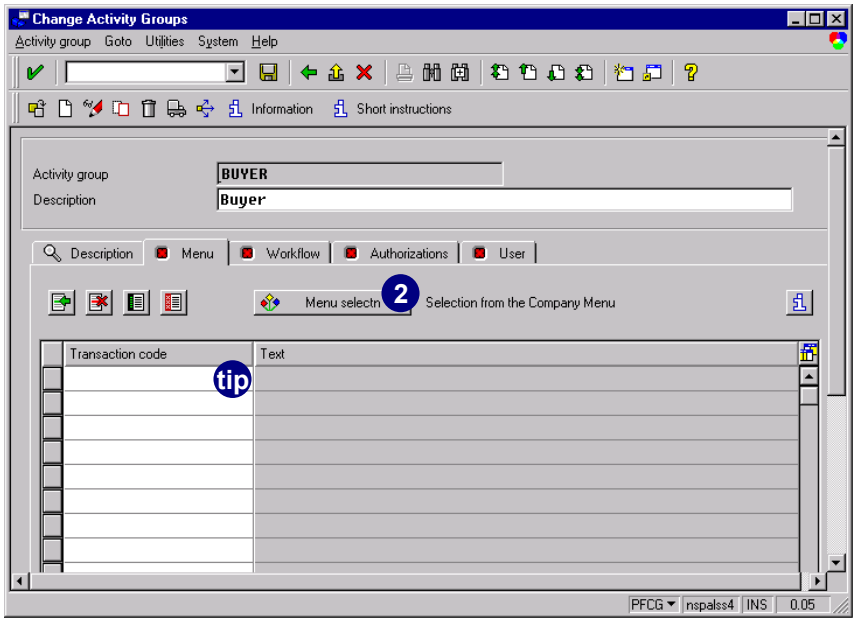
After you have saved the activity group's basic data, identify the reports and transactions that should be included in the activity group.



1. Choose the *Menu* tab to continue.

Tips & Tricks

The *Workflow* tab is only displayed if you selected *Overview (Organization management and workflow)*)at the beginning of transaction *PFCG*. If you do not see this tab, you probably marked *Basic maintenance (menus, profiles, add. objects)* .



2. Choose *Menu selectn* to assign R/3 functions (transaction codes) from the hierarchy tree of the company menu.

Tips & Tricks

You can also enter the transaction code directly into the *Transaction code* column. For a list of transactions, use *possible entries*. The text in the *Text* column is then automatically displayed after you select the transaction code. However, using *possible entries* may take significantly longer, because all transaction codes from your menu will be read and displayed.

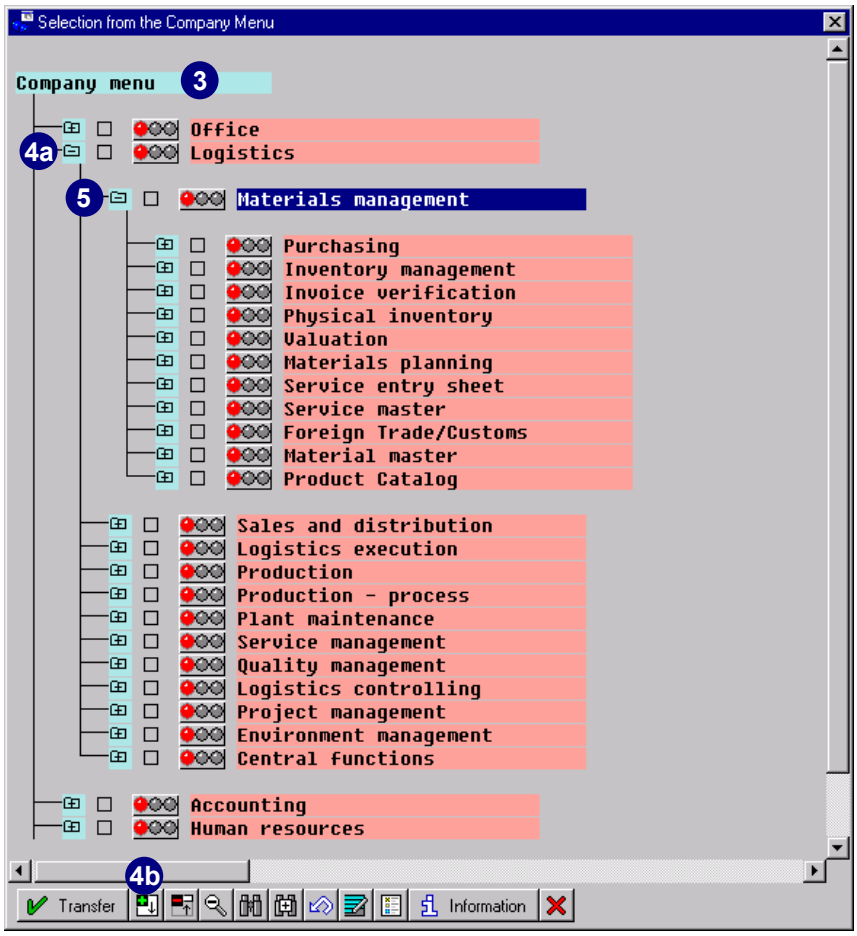
3. The *Selection from the Company Menu* screen appears and lists the company menu.

4. Expand the desired submenu using one of the following methods:

   a. Click the node (+) that corresponds to your desired menu entry (for example, *Logistics*).

   b. Choose *Expand branch* to expand the desired area.

5. Expand *Materials management*.



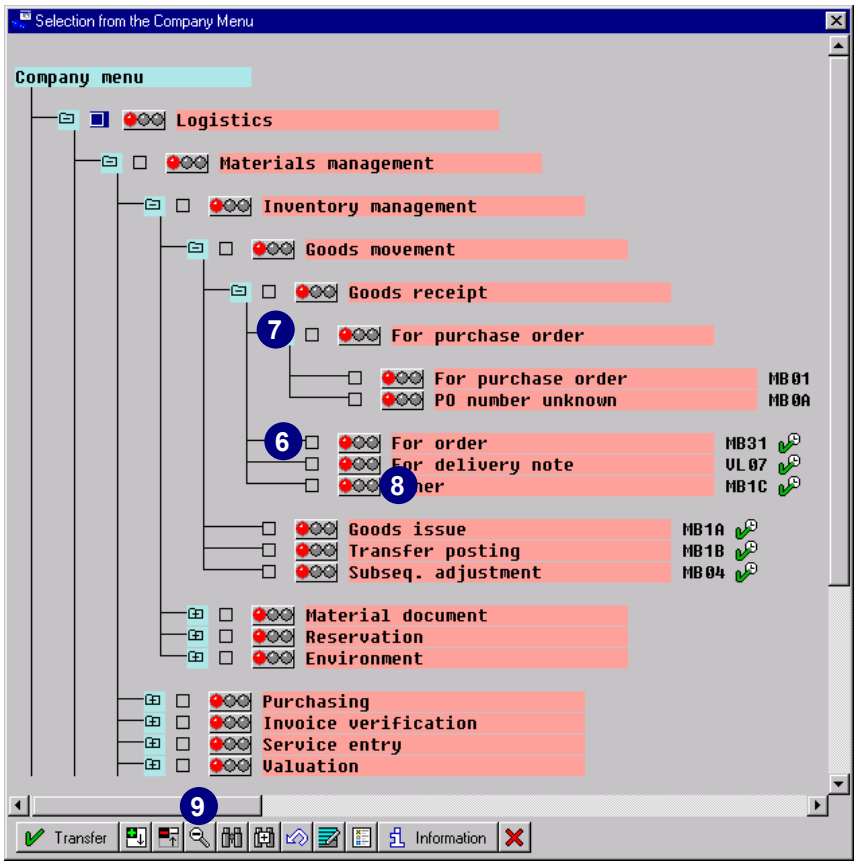
If you created the menu options by directly entering the transaction code, they are listed in the display in the menu option *Created manually*.

In the following we will show how to select transactions through the menu tree. The selected menu options are going to change from a red light to green and will be displayed in the menu tree if possible.

Choose one of three options (6, 7, or 8) to select the transactions or reports that you want in this activity group:

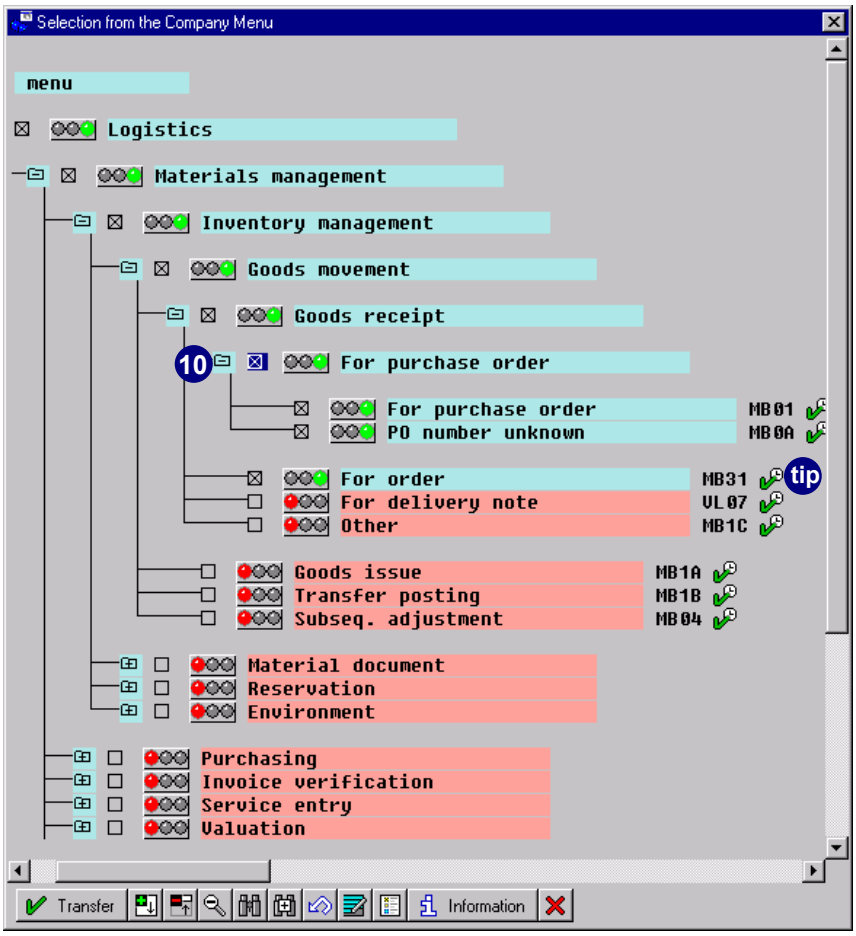
6. Click a checkbox to select (or deselect) a single transaction
7. Click a checkbox of a menu branch to select the entire menu branch underneath this node.
8. To select (or deselect) an item, you may also double-click the traffic light or the menu item text.

9. To switch the transaction code and the report names on or off in the company menu tree, choose the *Technical Name* button.



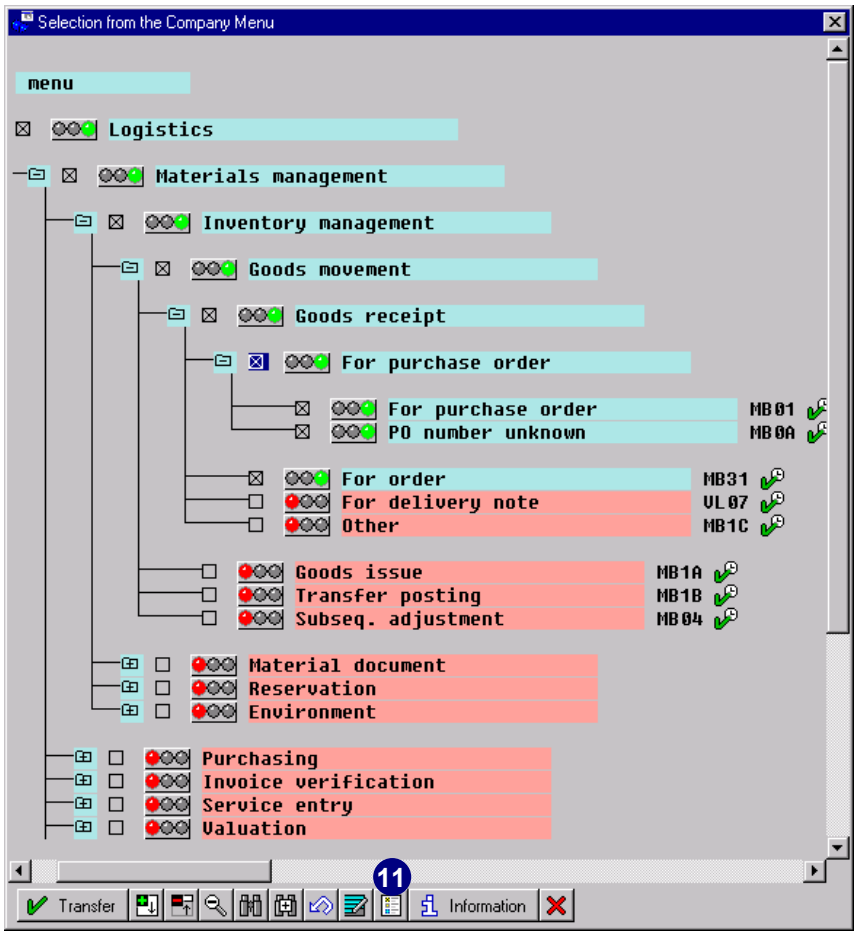
If you select a whole menu branch, all transaction codes underneath that branch will be selected as well.

10. In this example, we selected the menu branch *For purchase order* and the item *For order*.

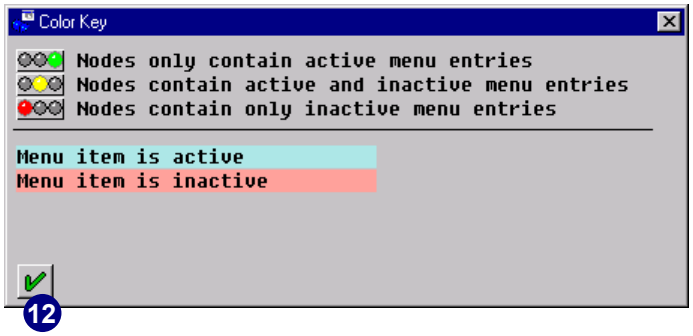


If you wish to view the actual transaction in the R/3 System, choose *Execute* next to the transaction code. You can return to your company menu tree by choosing *Back* or *F3*.

11. For an explanation of the traffic lights' displayed colors, choose *Color key*.

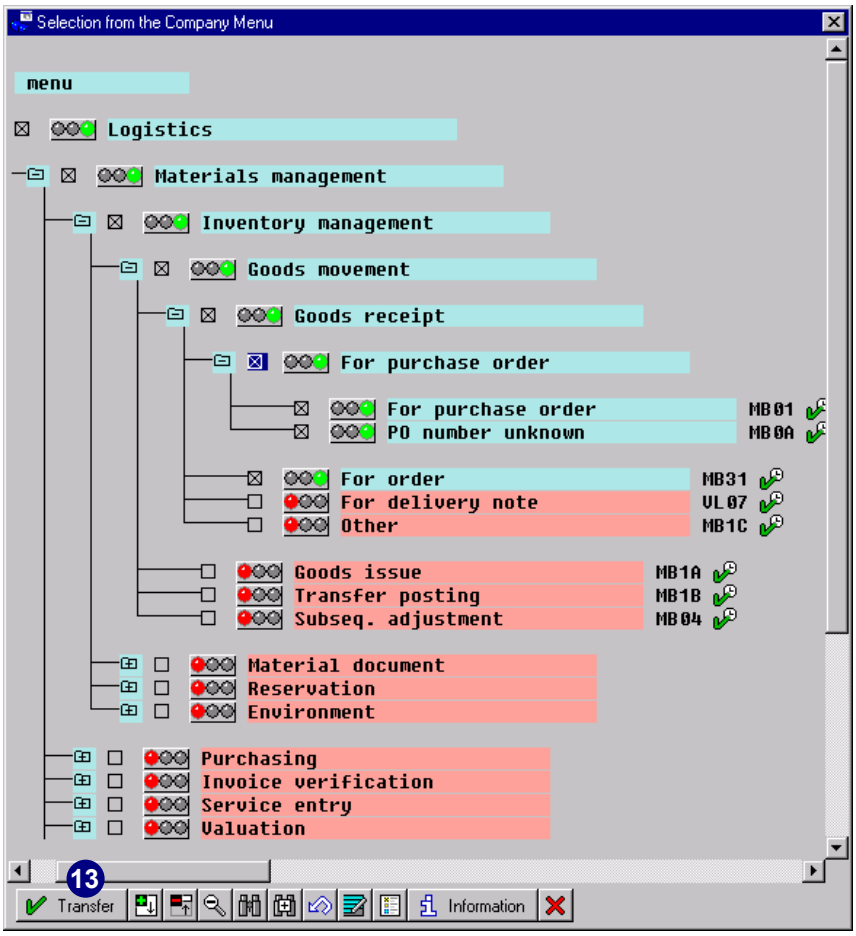


The *Color Key* popup window appears. The color of the menu item indicates whether an item has been selected.

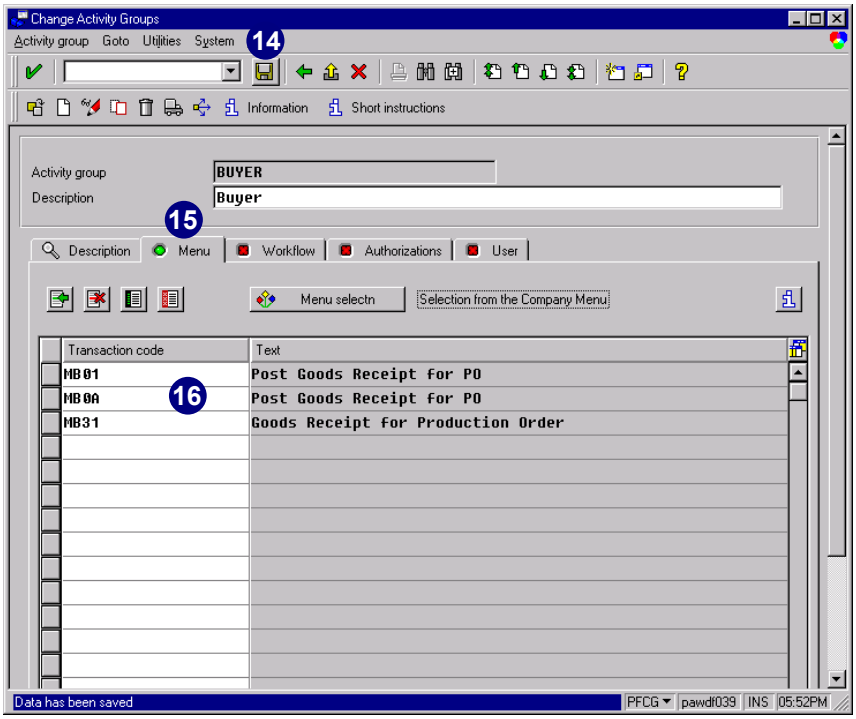


12. Choose *OK*.

13. To transfer your selection and return to the *Change Activity Groups* screen, choose *Transfer*.



14. Choose *Save* to save your selection.
15. The green light in the *Menu* tab indicates that you have maintained a menu selection for this activity group.
16. The transactions selected earlier in this procedure appear in the *Transaction code* column.



After selecting the transaction codes the next step would be to generate the authorizations. Because of its importance this topic deserves its own chapter. Therefore chapter 5 discusses, in detail, all the tasks for generating authorizations.

Copying and Deriving Activity Groups

Basics About Duplicating Activity Groups

It is entirely acceptable to utilize only activity groups in your implementation and to create them as needed. However, SAP provides two mechanisms to make activity group maintenance easier.

These two core mechanisms include:

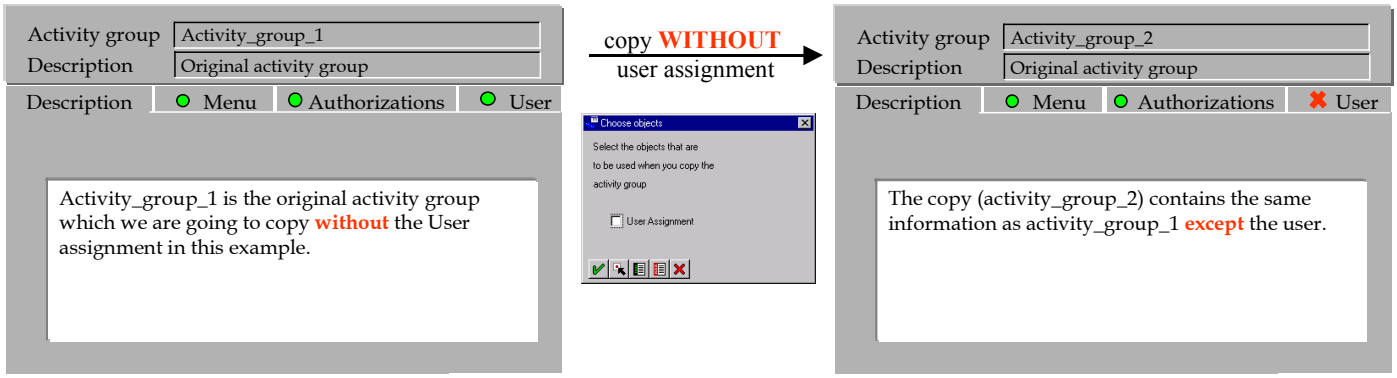
- Copying activity groups
- Using derived or inherited activity groups

The diagram below gives an overview what to expect from those options.

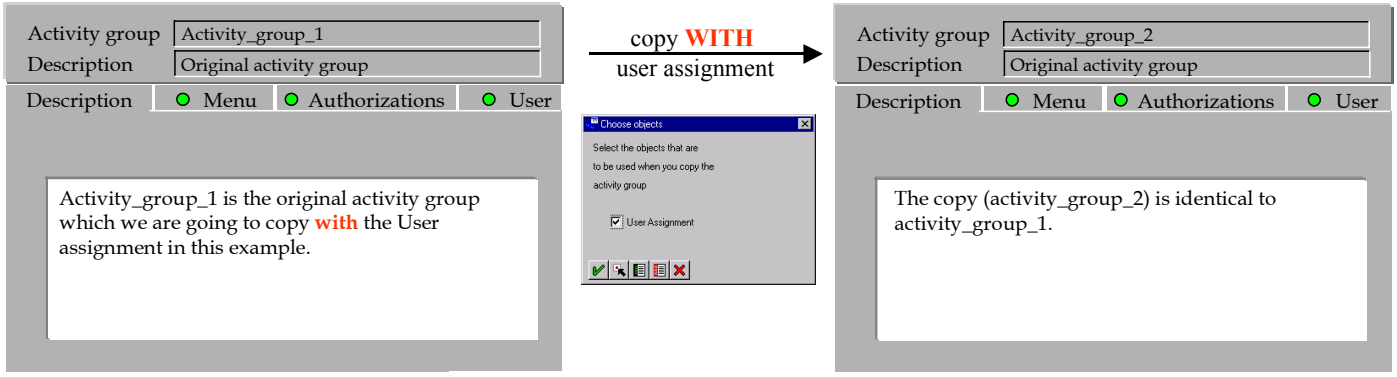
● - The green circle indicates that maintained or assigned items exist.

✖ - The red cross indicates that **no** maintained or assigned items exist.

Copying an activity group without a user

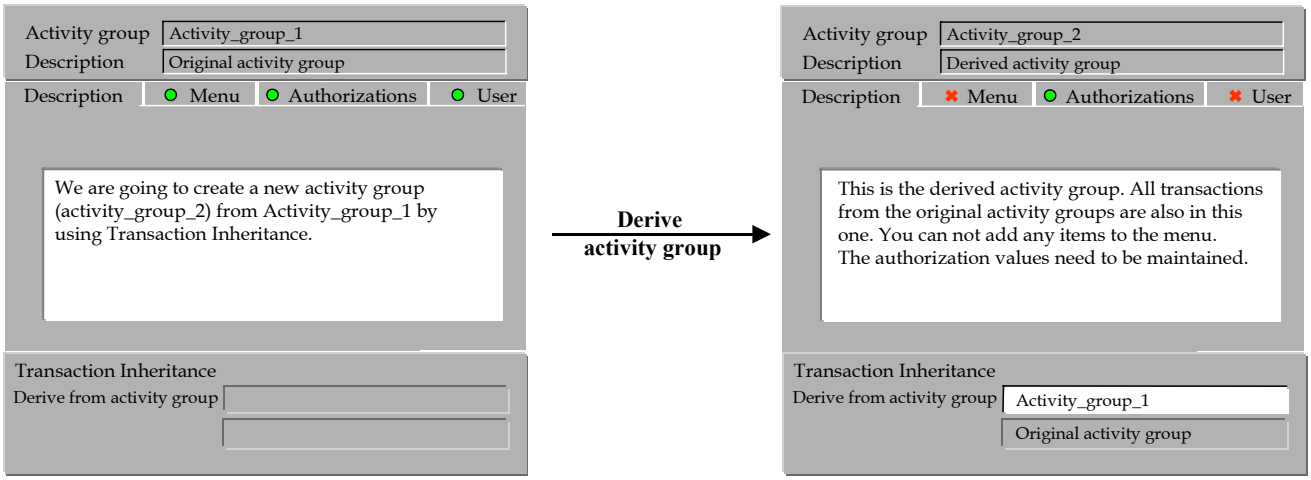


Copying an activity group with a user



There is no linkage between *activity_group_1* and *activity_group_2* after the copy process is performed in the two cases above.

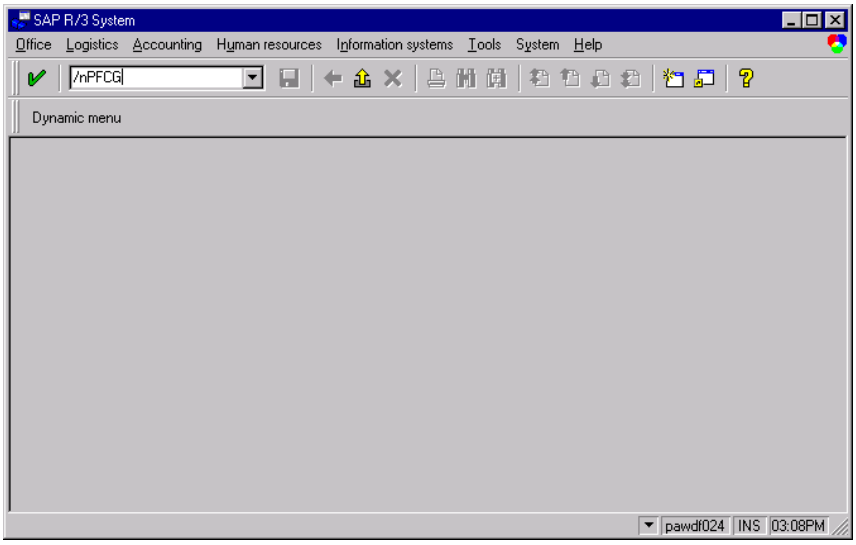
Deriving an activity group



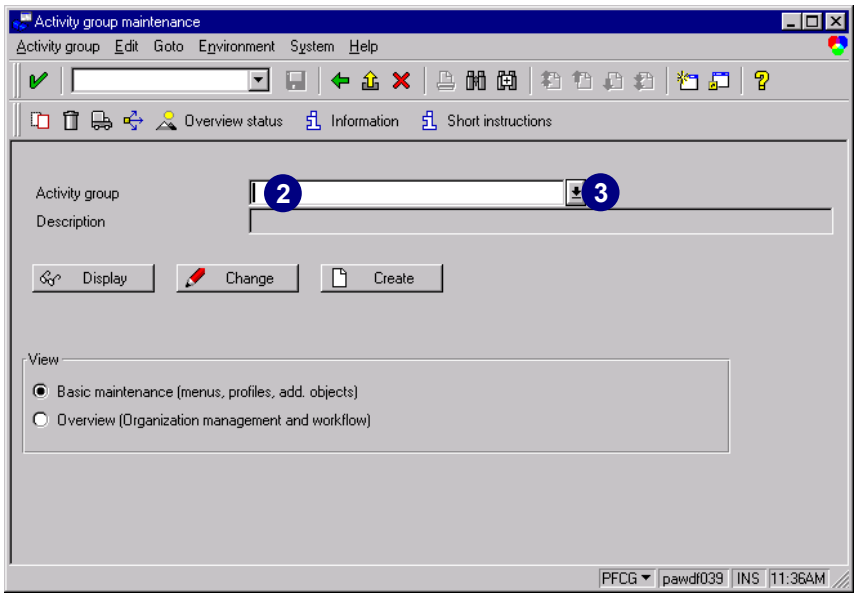
Adding transaction codes to *activity_group_1* after *activity_group_2* is created or generated, automatically impacts *activity_group_2*. Linkage between *activity_group_2* and *activity_group_1* is always updated automatically when *activity_group_1* has new transaction codes added to it.

Copying Activity Groups

1. In the *Command* field, enter transaction **PFCG** and choose *Enter* (or choose *Tools* → *Administration* → *User maintenance* → *Activity groups*).

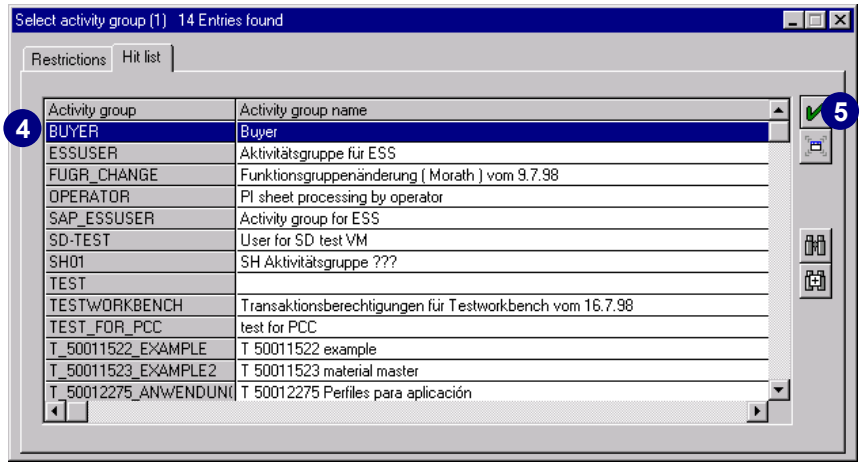


2. Position the cursor in *Activity group*.
3. Choose *possible entries*.

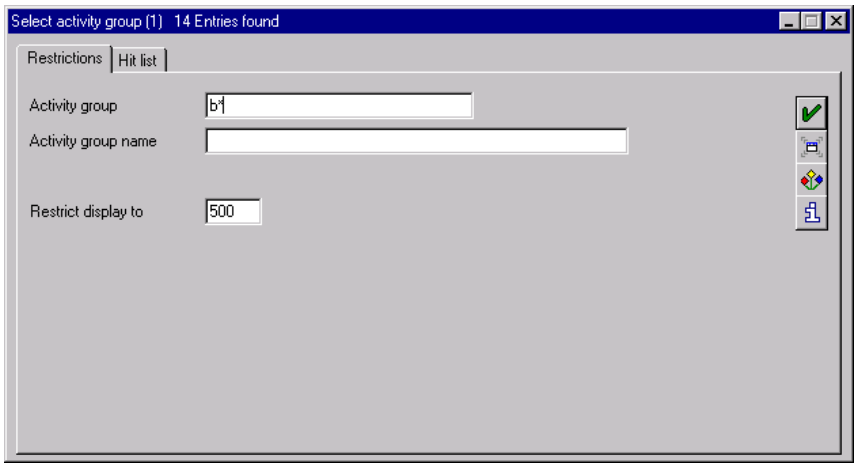


A *Hit list* appears.

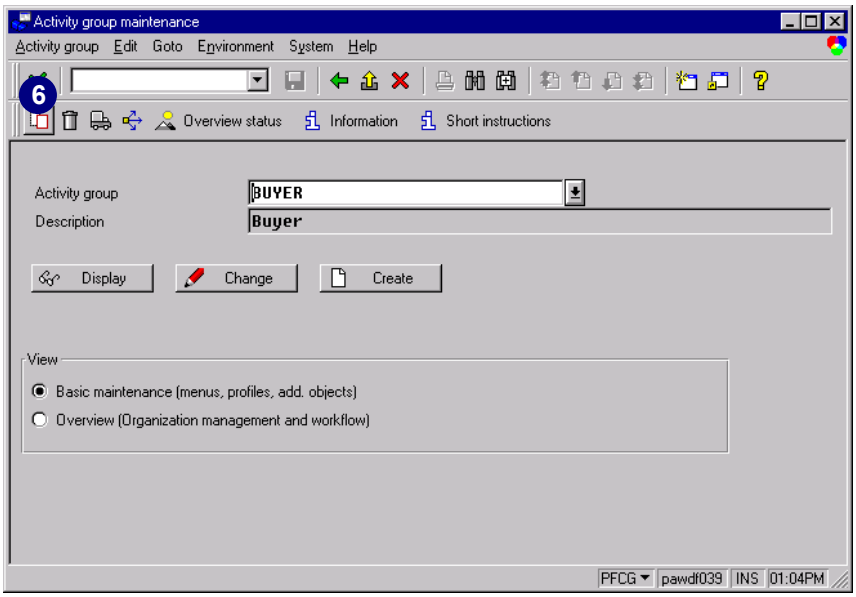
4. Select the activity group you want to copy.
5. Choose *Copy*.



If the *Hit list* is too long, choose the *Restrictions* tab to narrow your search. Enter the first letters of the activity group you are looking for and choose *Start search*.



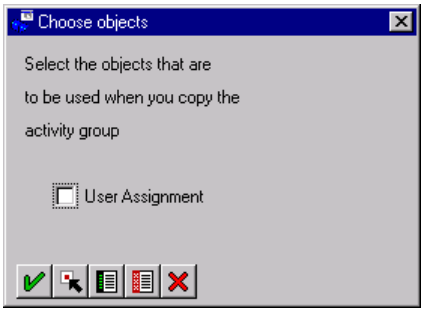
6. Choose *Copy*.



7. Enter a new activity group name for the target activity group (do not use blank characters in the name).

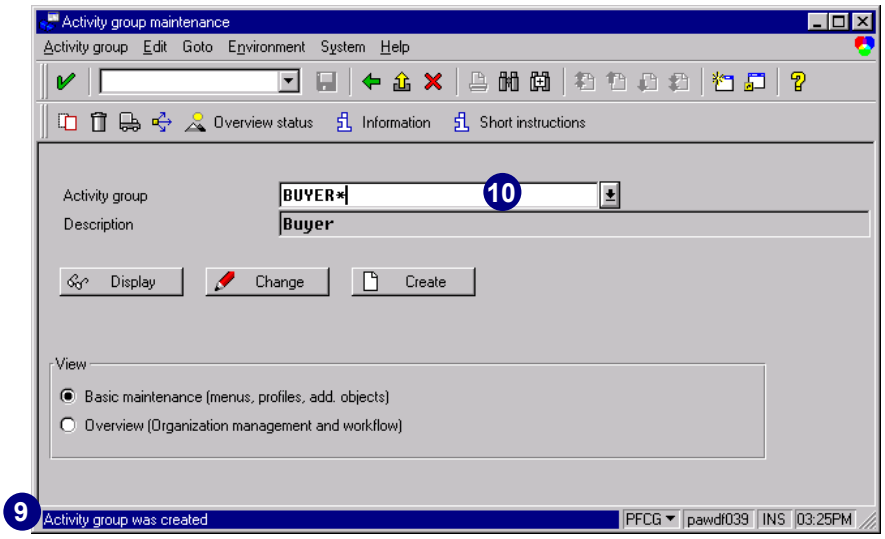
   In this example, we are copying the activity group **`Buyer`** to the new activity group **`Buyer_US_Market`**.

8. Choose *Copy all* to copy all data from the source activity group.

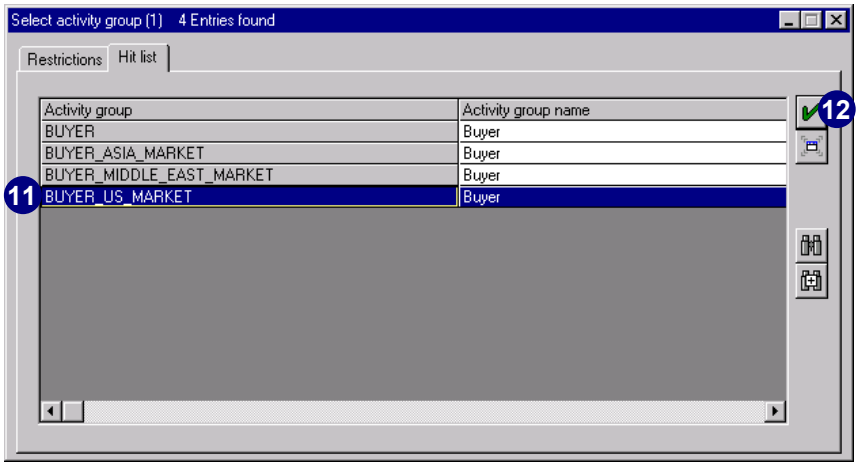


If you only want to copy some activity group subobjects from your source activity group instead of all related data, choose *Copy selectively*. Select the objects and choose *Enter*.

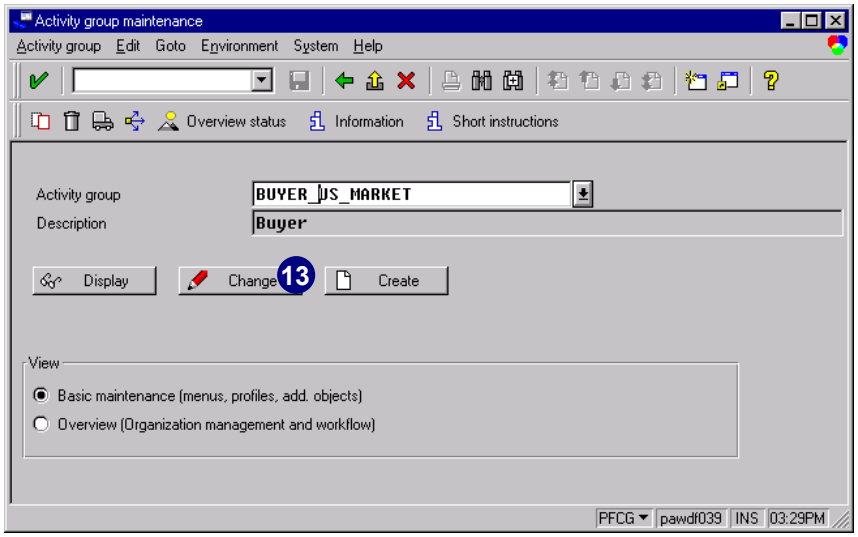
9. A new activity group was created.
10. Choose *possible entries,* or enter the name of the newly created activity group (or the first characters plus an asterisk (*), as in this example) directly into the field *Activity group* to display or change the activity group.



11. Select the newly created activity group.
12. Choose *Copy*.

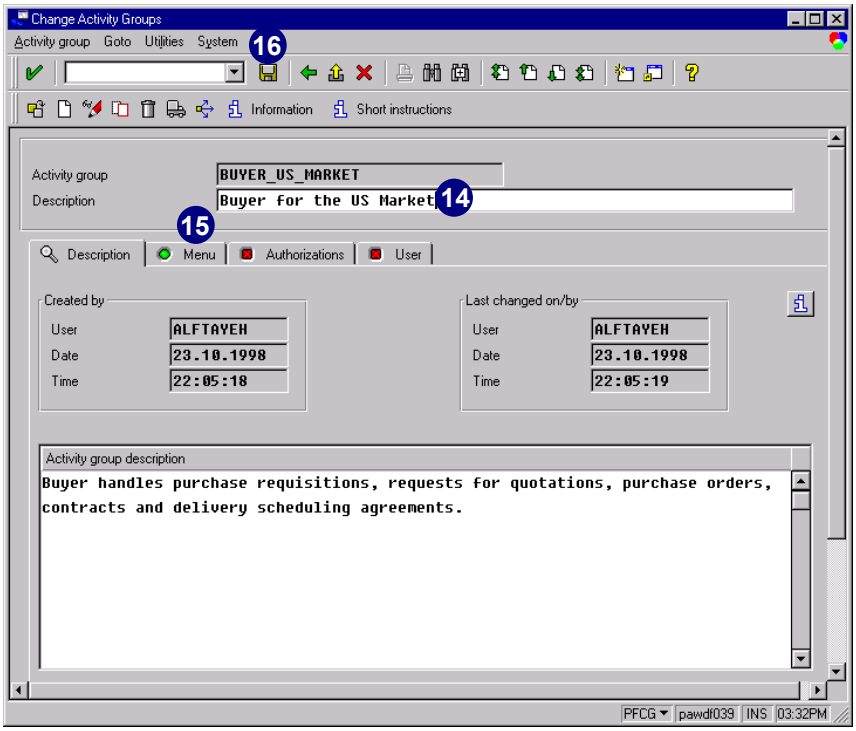


13. Choose *Change*.



14. Describe your new activity group in the field *Description*.
15. Choose the *Menu* tab to edit and adjust your selection of transactions and reports for this activity group.
16. Choose *Save*.

    Follow the instructions in the section *Selecting Reports and Transactions* starting on page 4–6.



The red light on the *Authorizations* tab indicates that the authorization profiles for the new activity group need to be regenerated after being copied. Please see chapter 5 for information on regenerating profiles.

The red light on the *User* tab indicates that no users are assigned to that activity group.

Deriving Activity Groups

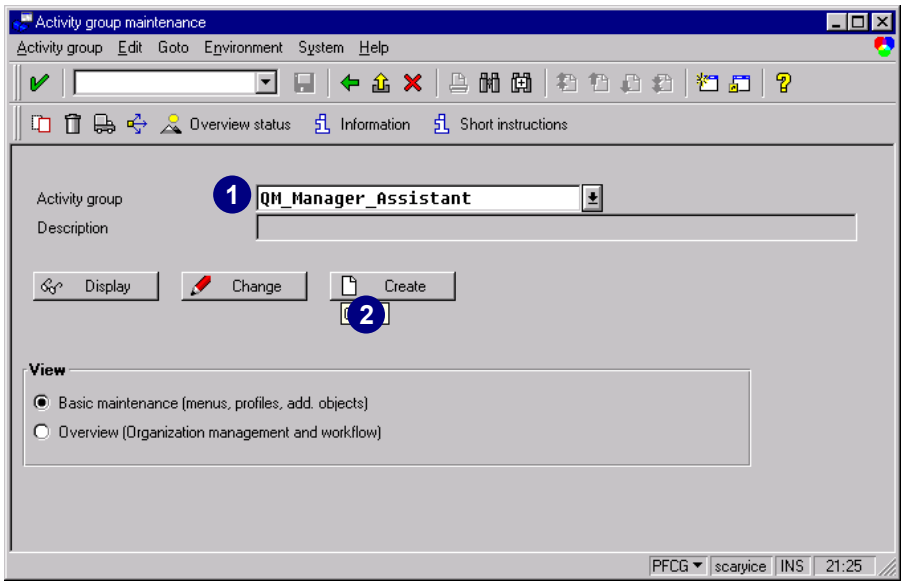
Deriving an activity group (also called transaction inheritance) means you can use an existing activity group as a reference. Essentially, the system transfers the transactions from an existing activity group. This process of deriving one activity group from another is only possible if you have not yet assigned any transactions to the new activity group. Otherwise, the previous activity group passes on its transactions to the activity group dependent on it. If you use derived activity groups it is easy to maintain consistency between access to transaction codes.

If you are going to use derived activity groups, it does not make much sense to use templates or manually inserted authorizations with the original activity group. **Only** the transaction codes are passed along to the derived activity group. The manually inserted authorizations and the templates in AG1 will not be copied into AG2 (nor will the linkage be maintained if manually inserted in AG2).

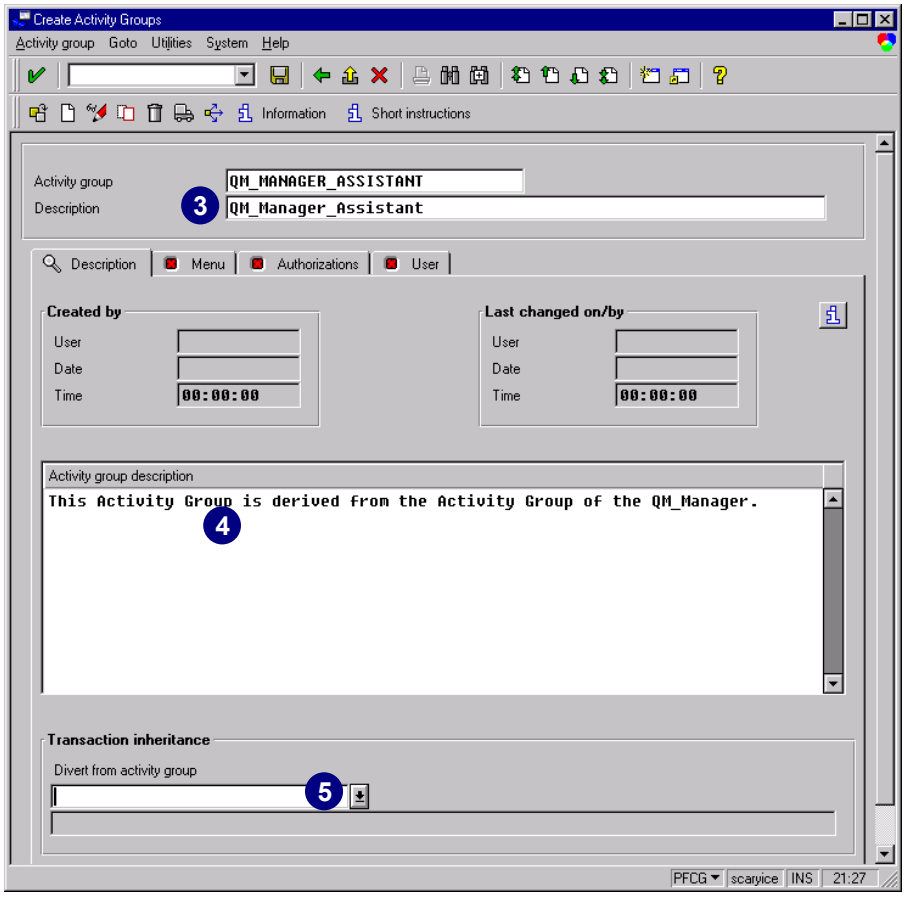
Example: Usage of Derived Activity Groups

A manager wants all of the people that work for him to have access to the same transactions that he has. However, his employees are **not** to have all the functionality that each of the transactions offer. As such, we could create an activity group with the transaction codes and call that activity group, for example *MANAGER-A-ACCESS*. We would also maintain all the authorization field values for this activity group. Then we would create an activity group called *EMPLOYEES-MANAGER-A* and use *MANAGER-A-ACCESS* as the derived activity group (On the *EMPLOYEES-MANAGER-A* activity group's description screen in transaction *PFCG*, in the field "Divert Activity Group", we would place *MANAGER-A-ACCESS*). As only the transactions are copied into (derived from *MANAGER-A-ACCESS*) the "menu," we still need to maintain the authorization field values for the *EMPLOYEES-MANAGER-A* activity group.

1. Access the *Activity group maintenance* screen and enter the name for your new activity group in the *Activity group* field.
2. Choose *Create*.

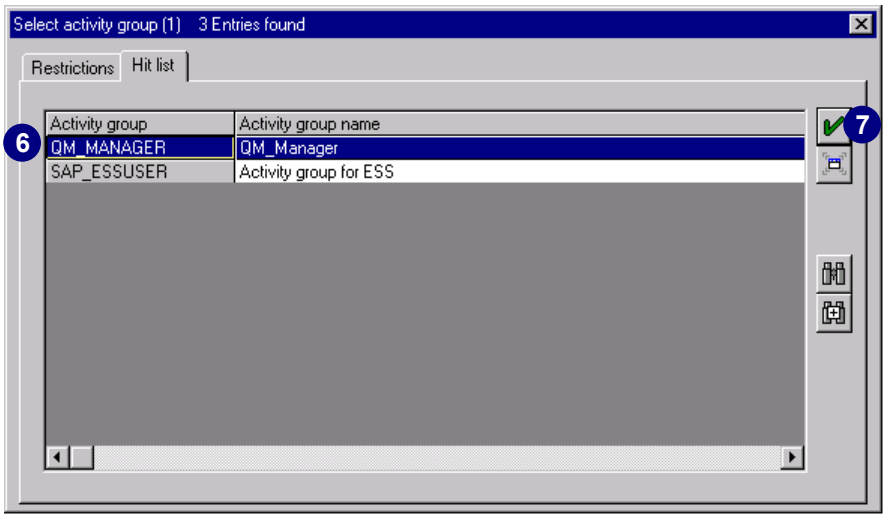


3. Enter a short description in the *Description* field.
4. Enter a long description in the field *Activity Group Description*.
5. Select an activity group from which you want to inherit the transactions, by entering the name in *Divert from activity group* (this translation is not correct, it should say derived from activity group) or choosing *possible entries*.

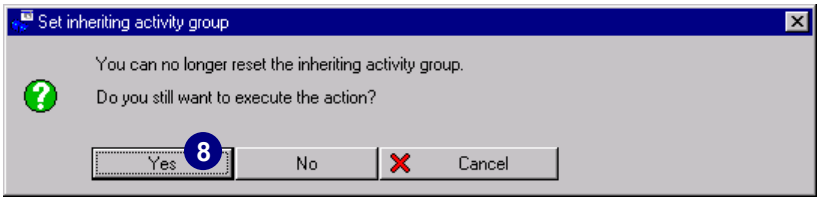


The field name *Divert from activity group* is not correct. It should say *Derived from activity group*.

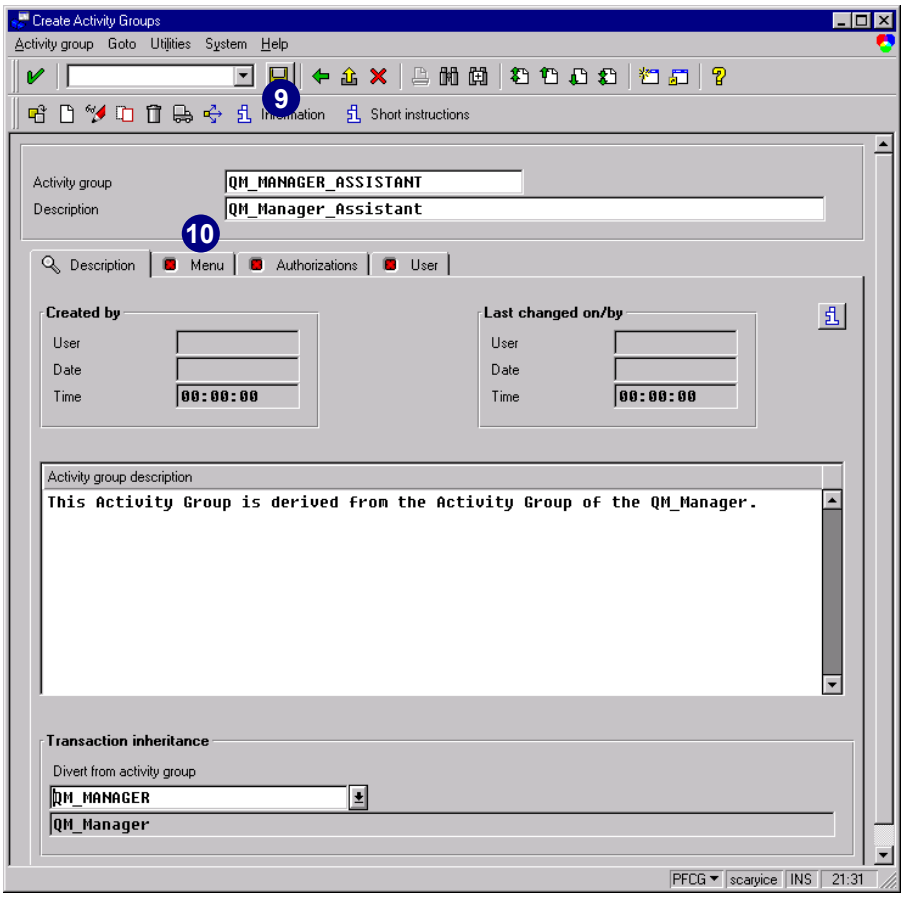
6. Select the activity group.
7. Choose *Copy*.



8. Choose *Yes*.



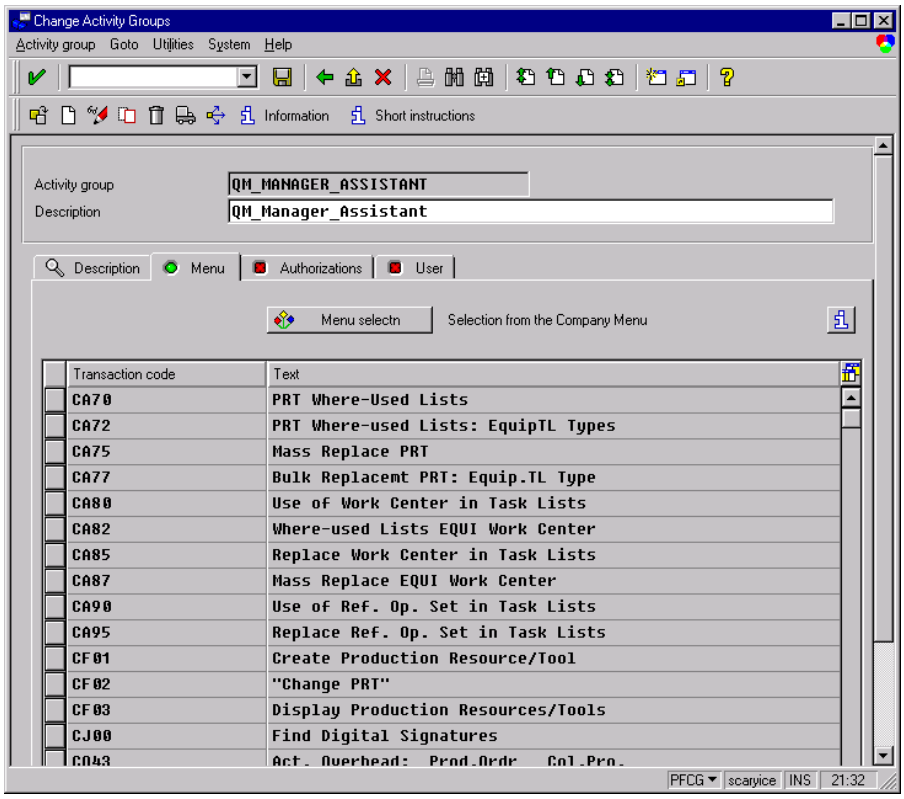
9. Choose *Save*.
10. Choose the *Menu* tab.



You have just created a derived activity group.

You can see that all the transaction from your original activity group have been inherited. Since the background is gray, it indicates that you can not edit or add any transactions to it.

Now you have to maintain the Authorizations for the activity group. How to do this will be shown in the next chapter.



Choosing the Correct Menu Path in Session Manager

If you plan to use the Session Manager, please read this section first. Even if you plan on using the Session Manager later, you should read this information. If you do not plan to use the Session Manager, you may skip this section.

In R/3, the same transaction or report can be executed in multiple branches under the SAP menu tree. The Session Manager shows the menu path for the transaction you have chosen. Therefore, it is important to choose the correct menu path when you select transactions or reports for an activity group. After selecting transactions or reports, assign the activity group to an R/3 user. When users log onto the Session Manager, they will see the corresponding menu path for the transaction or report.

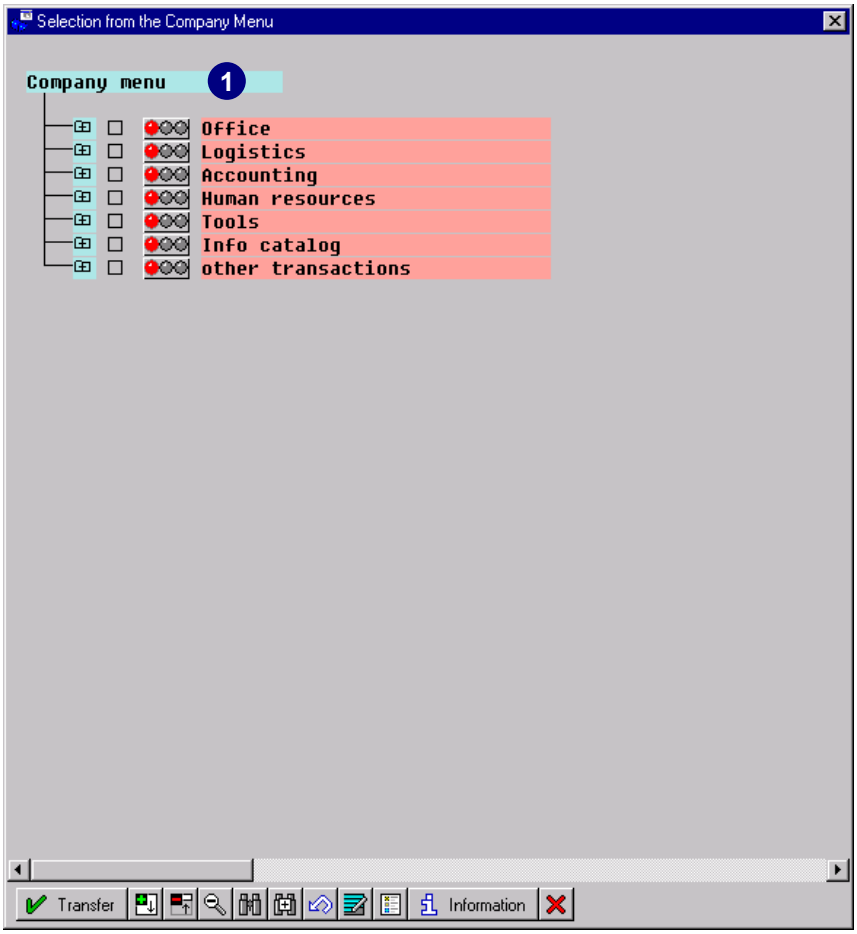
The following example will help you ensure that the correct menu path choice was made for a transaction. This way, when users log onto the Session Manager, they will see the correct menu path for the transaction.

To access the screen for the following section, access the Profile Generator, select the *Menu* tab and choose *Menu selectn*.

1. Start with the *Company menu* selection window to select the transactions and reports you want to assign to your activity group.

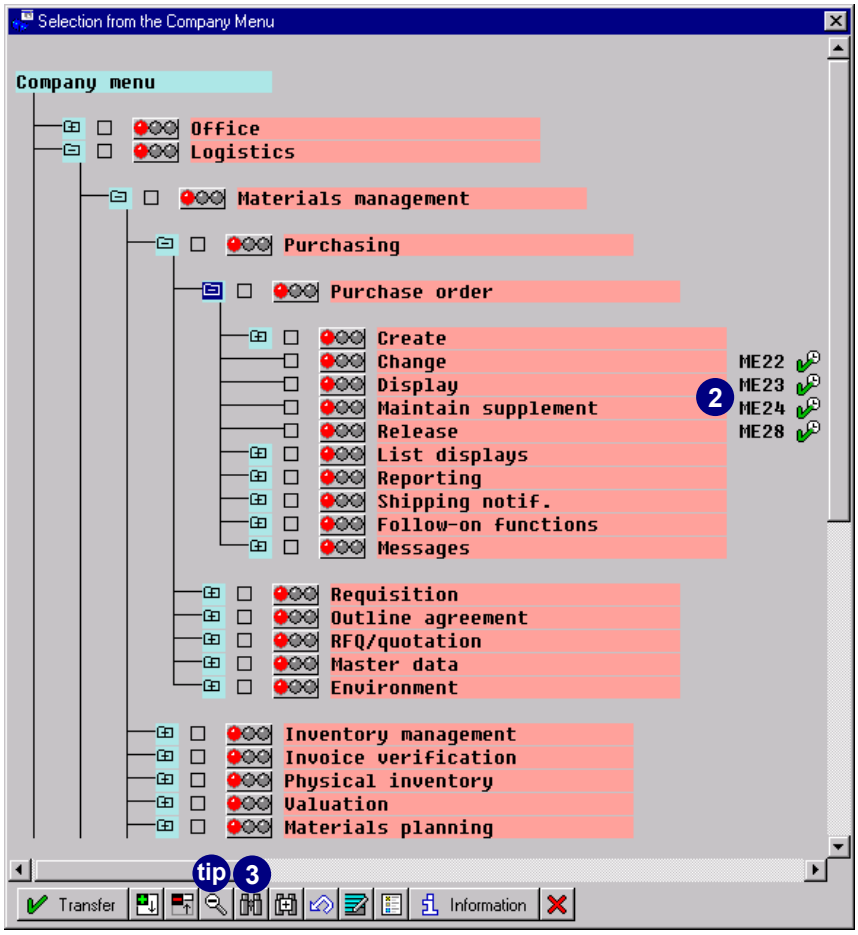
   In this example, we want to assign the display transaction *Purchasing Documents for Vendor* to the activity group.

   Expand the nodes (+) in the *Company menu* until you see the desired menu item.

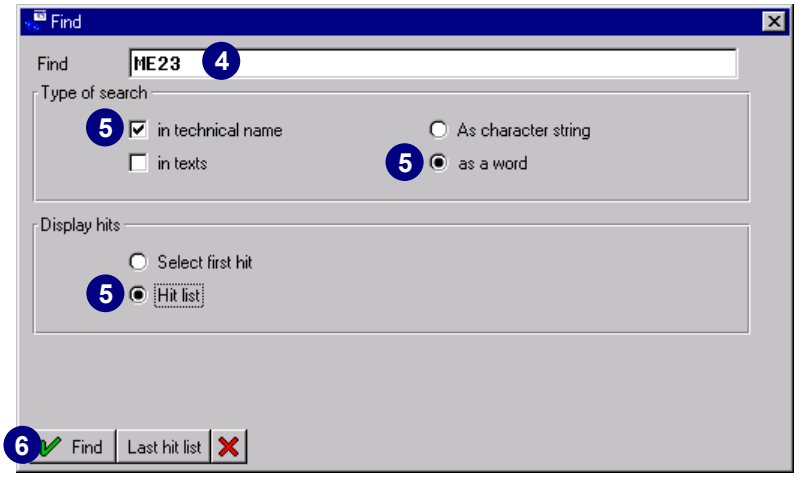


To display the transaction codes next to the menu items, choose *Technical name on/off*.

2. Identify the transaction code for the relevant menu item. In our example, *ME23* is the transaction code for *Purchase order* → *Display*.
3. Choose *Find*.

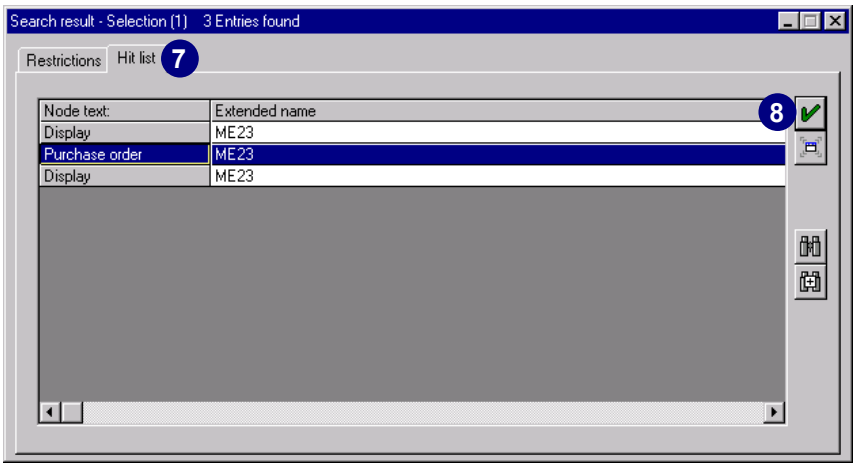


4. In the *Find* field, enter the transaction code you wish to search for (for example, **ME23**).
5. Select the following properties:
   - *in technical name*
   - *as a word*
   - *Hit list*
6. Choose *Find* to continue.



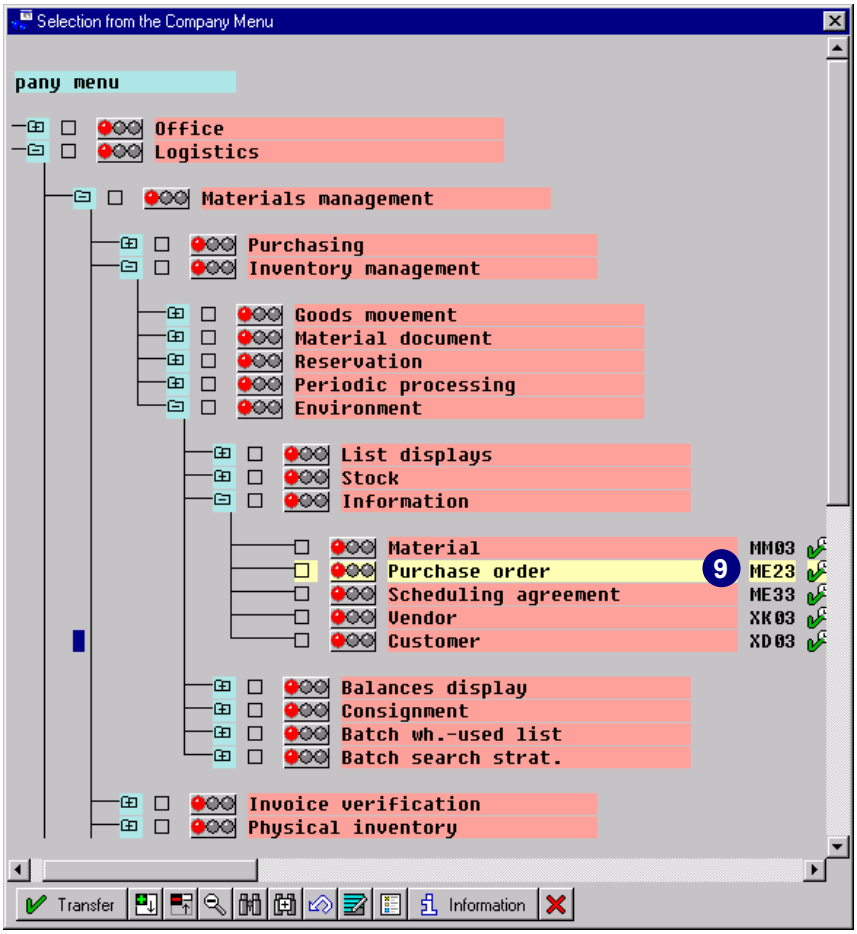
If you search for a transaction code and it exists only once, you are taken directly into the menu tree where the transaction is highlighted. The search result screen below is skipped in this case.

7. A *Hit list* appears indicating how many times the transaction was found in the company menu.
8. Double-click on an entry from the *Hit list*, or select and choose *Copy*.

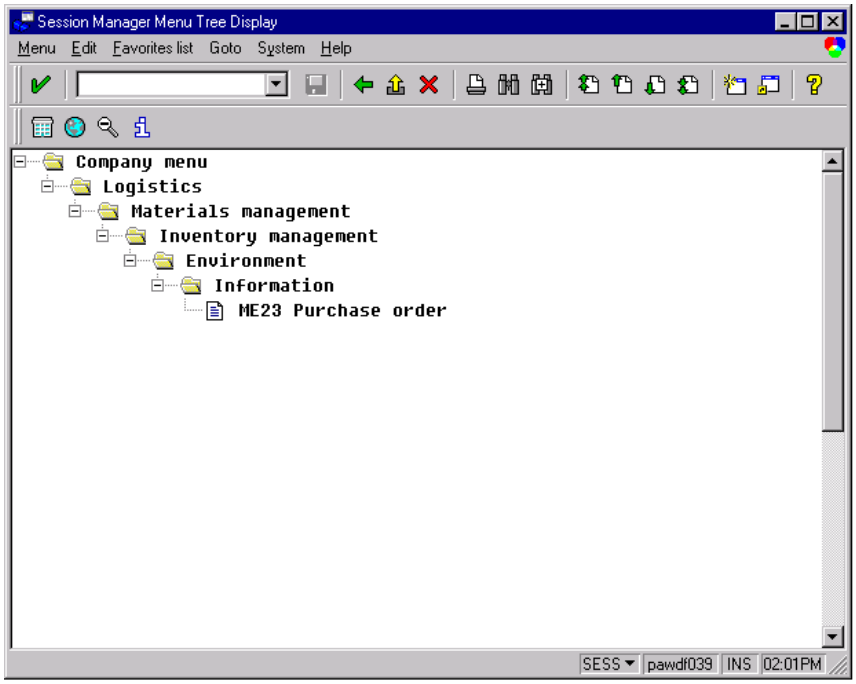


9. The appropriate transaction is highlighted in yellow in the *Company menu* tree.

   The path is *Logistics* → *Materials management* → *Inventory management* → *Environment* → *Information* → *Purchase order*.



Assume that we have created an activity group with only the *Purchase order* transaction selected, and we assigned this activity group to an R/3 user. The user sees the adjacent menu path displayed after logging on to the corresponding R/3 System with Session Manager (transaction **SESS** in the R/3 System).



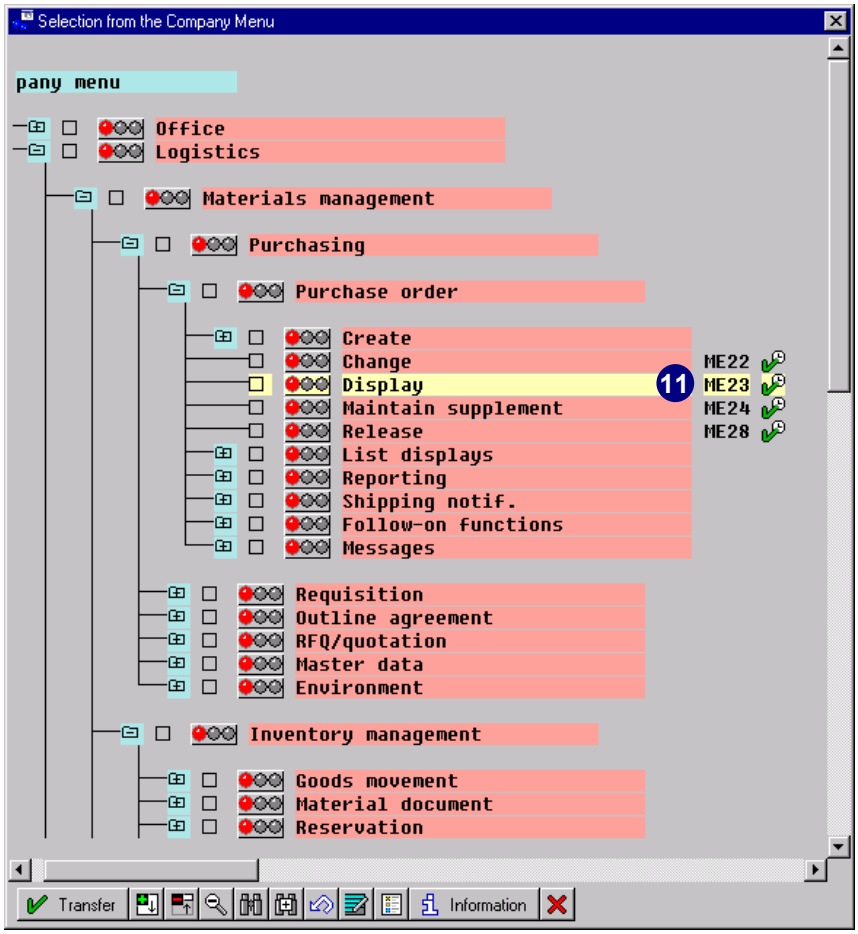
If your selection from the hit list does not produce the desired menu path, repeat steps 3–8.

We will assume that the first path was not the correct one and continue by checking the second entry.

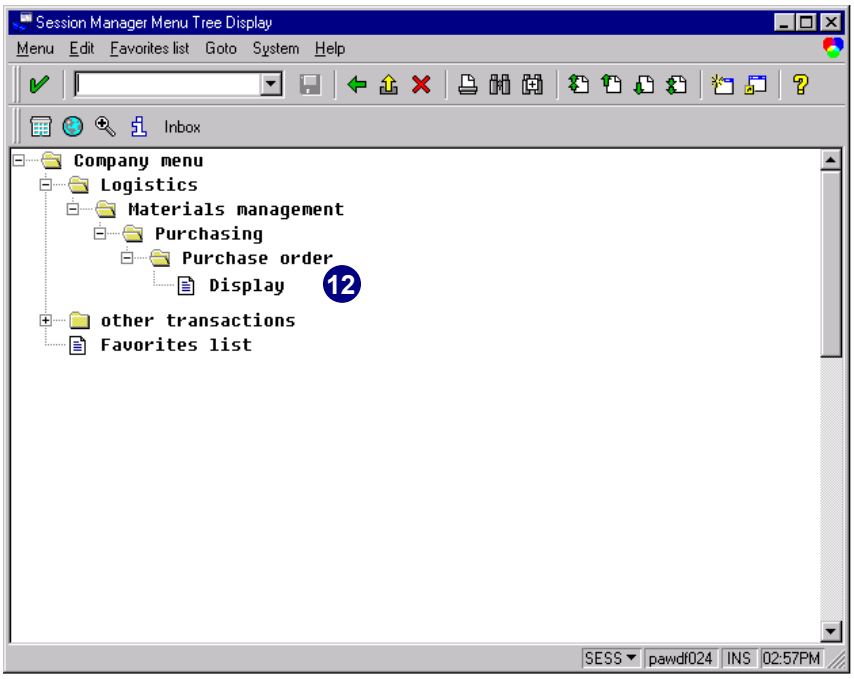
10. Select the next entry in the *Hit list*.
11. The next entry in the *Hit list* highlights the same transaction underneath a different menu branch of the *Company menu* tree. Now, we can easily find the menu path that leads through this transaction.

In our example, you find the following menu path:

Logistics → *Materials management* → *Purchasing* → *Purchase order* → *Display (ME23).*



12. Assume that we created an activity group with this particular transaction selected and assigned this activity group to an R/3 user. The user would then see the menu path after logging on to the appropriate R/3 System with the Session Manager (by entering transaction **SESS** or choosing *Dynamic Menu*).



Choosing the Correct Menu Path and Locating All Transaction Instances

If you select the desired transactions and reports while browsing through the correct submenus, there is no need to check for other instances under the SAP menu tree. If you only have the transaction codes and need to create an activity group for that selection, search for the relevant transaction in the company menu tree and choose the correct menu path. Remember, if you do not use the Session Manager, choose the transaction from the menu tree as shown and do not worry about the menu path.

Selecting Workflow Tasks

If you do not want to select workflow tasks for your activity group, skip this section. The red light in the *Workflow* tab indicates that no tasks have been assigned for the activity group. Please see chapter 5 for more information on generating and maintaining authorization profiles.

Selecting *Workflow tasks* has no impact on the to-be-generated authorization profiles.

What You Should Know About Workflow

This section provides a step-by-step sample *SAP Business Workflow* and an explanation of what you should know about the tasks before you assign them to your activity group.

Sample Workflow for a Notification Absence

This process begins when an employee submits a completed *Request for Leave* form. This form is automatically forwarded to that employee's supervisor. If the supervisor approves the request, the employee is informed, and the workflow ends. If the supervisor rejects the request, the employee must decide whether he or she wants to revise the request, or withdraw it completely. If the employee decides to revise the request, the form is automatically returned to his or her inbox, and the workflow begins again.

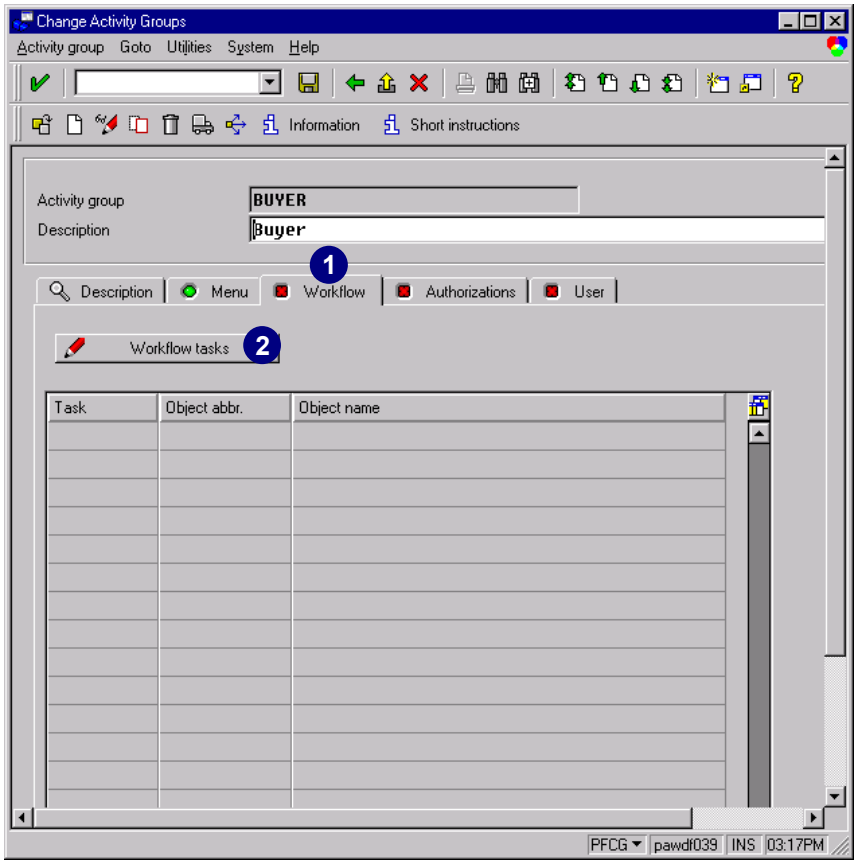
Tasks are used to expedite a business procedure. A task can be either a **single-step task** or a **multi-step task**. In our example, creating the *Request for Leave* form and checking this request are both single-step tasks. The procedure for processing a *Request for Leave* form is a multi-step task, consisting of several combined single-step tasks.

There are differences between the single-step standard tasks and customer tasks and between the multi-step workflow templates and workflow tasks. Standard tasks are the single-step tasks used in SAP's workflow templates. Standard tasks and workflow templates are provided by SAP and should not be changed by customers. Customers can, however, copy and modify these templates to create their own customer tasks and workflow tasks.

SAP-defined template	Customer-defined
Standard tasks	Customer tasks
Workflow templates	Workflow tasks

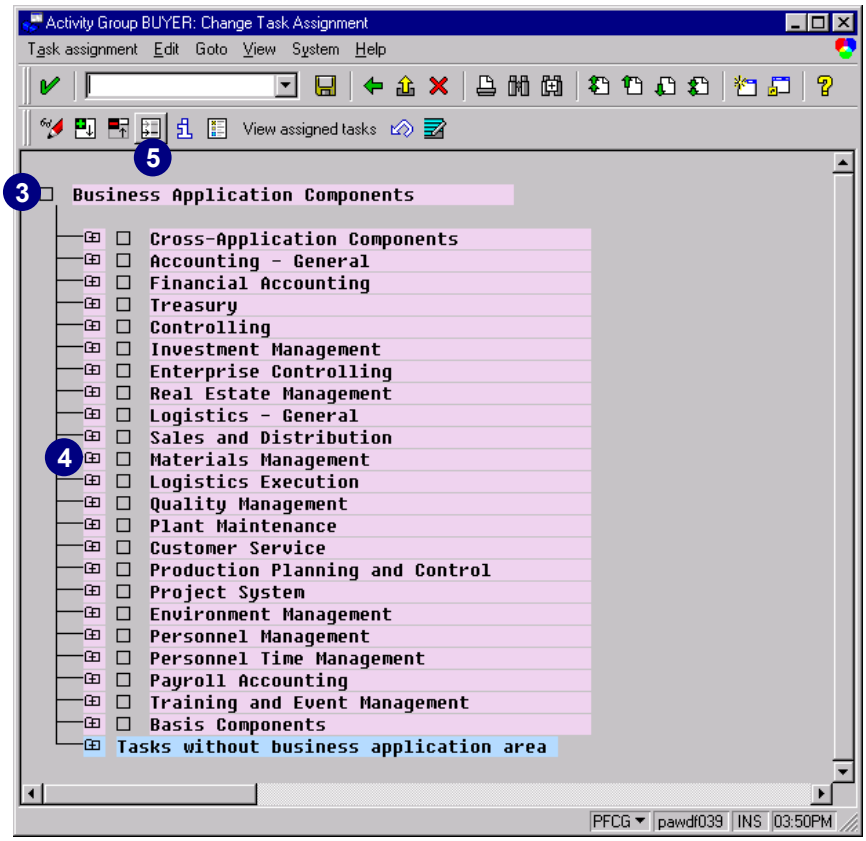
To access the screen for the following section, access the Profile Generator by selecting *Overview*.

1. Choose the *Workflow* tab to select *Workflow tasks* for the activity group.
2. Choose *Workflow tasks*.

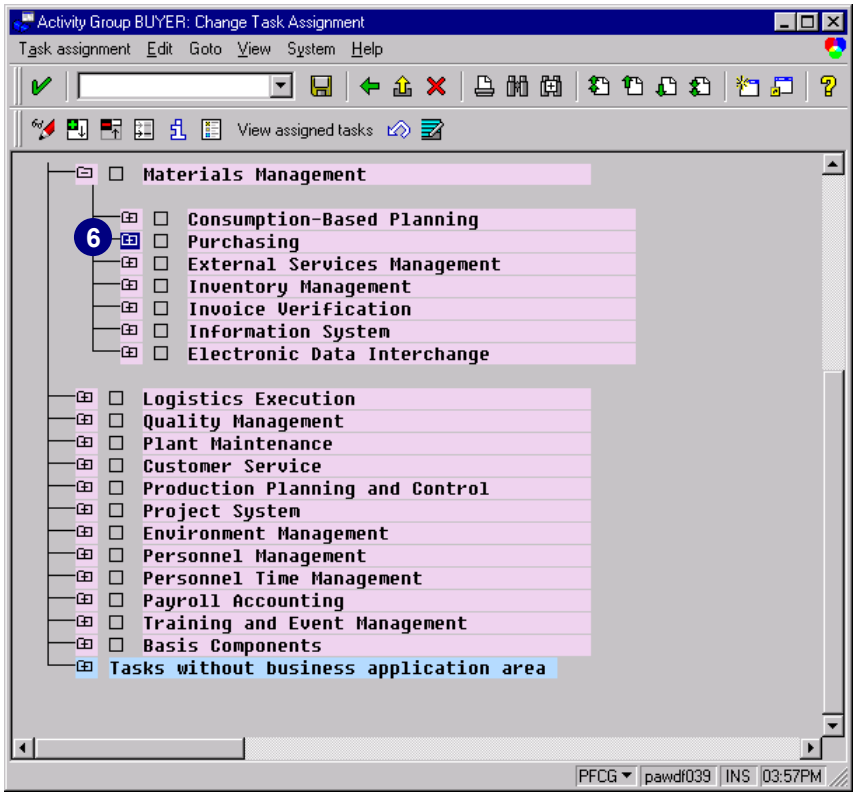


This *Workflow* tab is only displayed if you selected *Overview (Organization management and workflow)* at the beginning of transaction *PFCG*. If you do not see this tab, you probably marked *Basic maintenance (menus, profiles, add. objects))*.

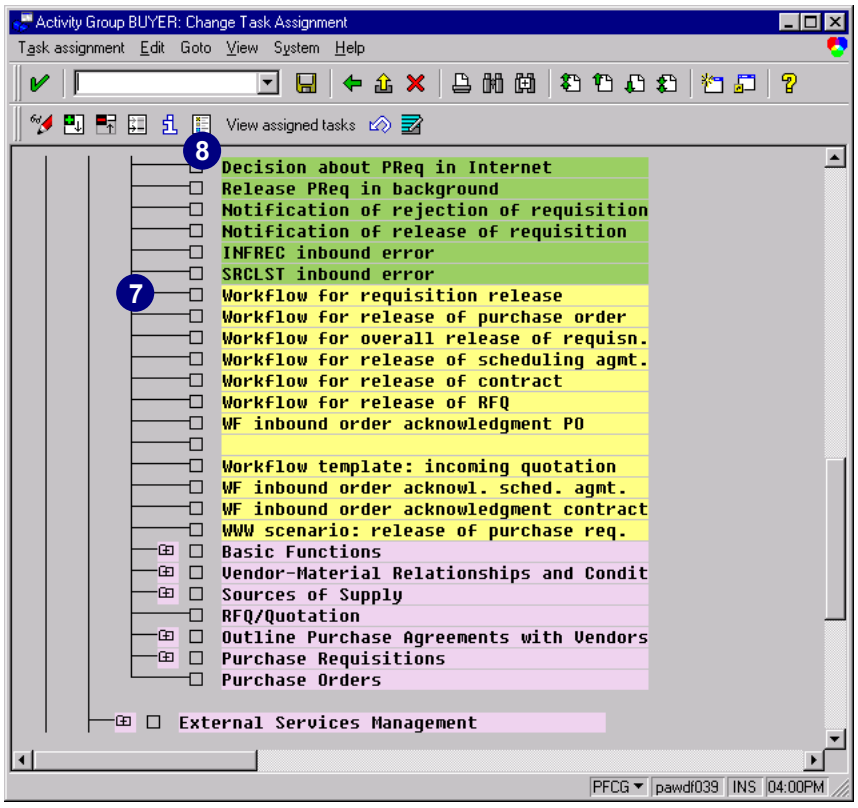
3. A tree with the *Business Application Components* appears.
4. Click the node (+) of the application area where you would like to include a task. For example, choose *Materials Management*.
5. Choose *Position* to position the marked item as the first item in the list.



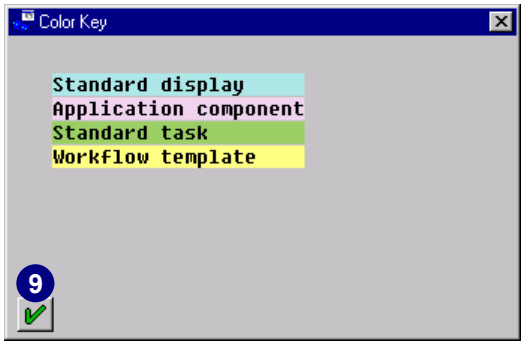
6. Click the node (+) of the desired business area underneath *Materials Management* (for example, *Purchasing*).



7. The available standard tasks and workflow templates available appear.
8. To view the color legend, choose *Color legend.*



9. Review the colors. Then choose *Enter* to continue.

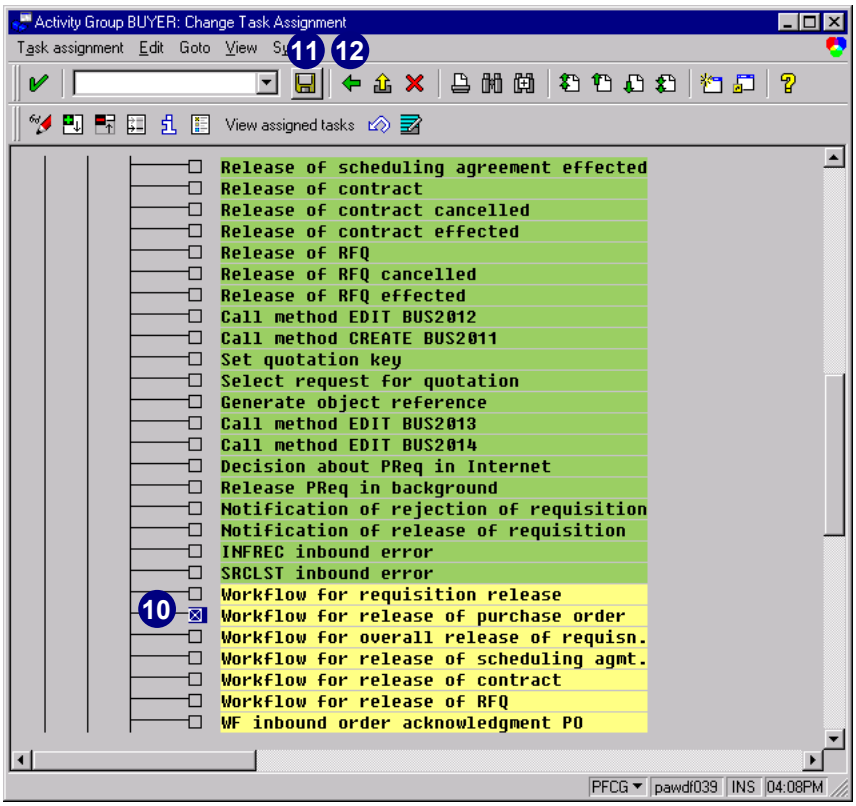


10. Select the desired workflow template (for example, *Workflow for release of purchase order)* to assign it to your activity group.

    Select all the tasks you want in your activity group.

11. Choose *Save* to save your selection.

12. Choose *Back*.

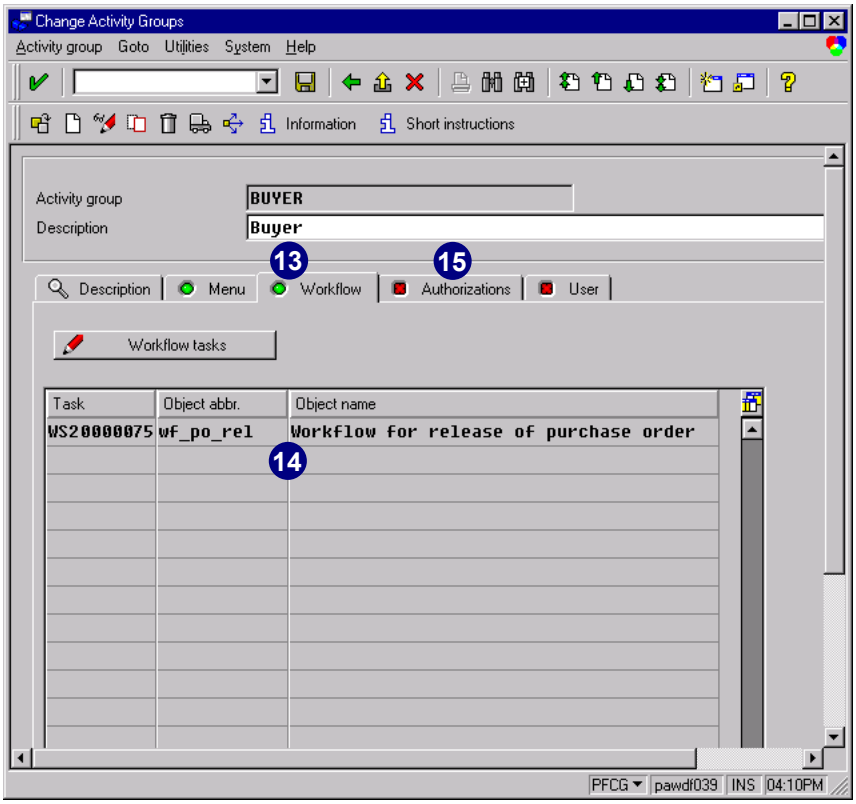


13. The green light on the *Workflow* tab indicates that you have created and saved workflow tasks for this activity group.

14. In the on-screen table, all selected workflow tasks including object abbreviation and full name, are shown.

15. The red light on the *Authorizations* tab indicates that you have not yet generated the authorization profiles for your activity group.

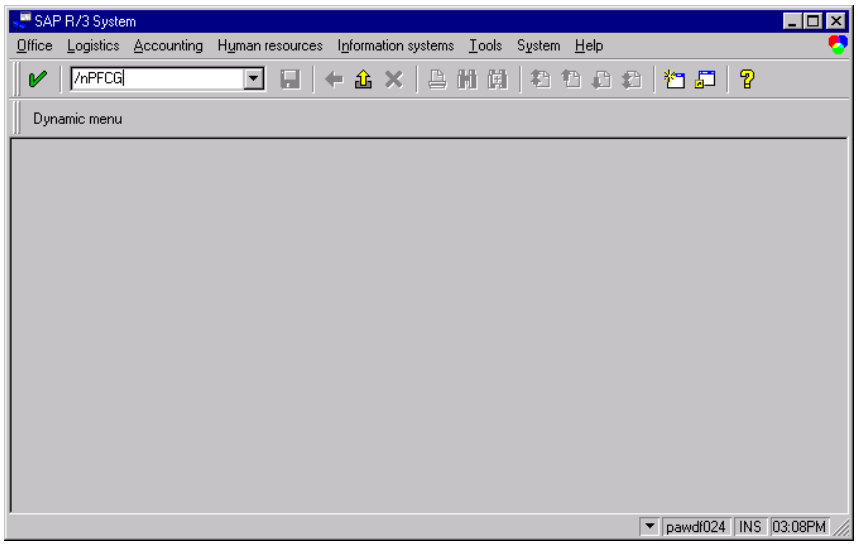
    The next step is to generate the authorization profiles. Please see chapter 5 for more information.



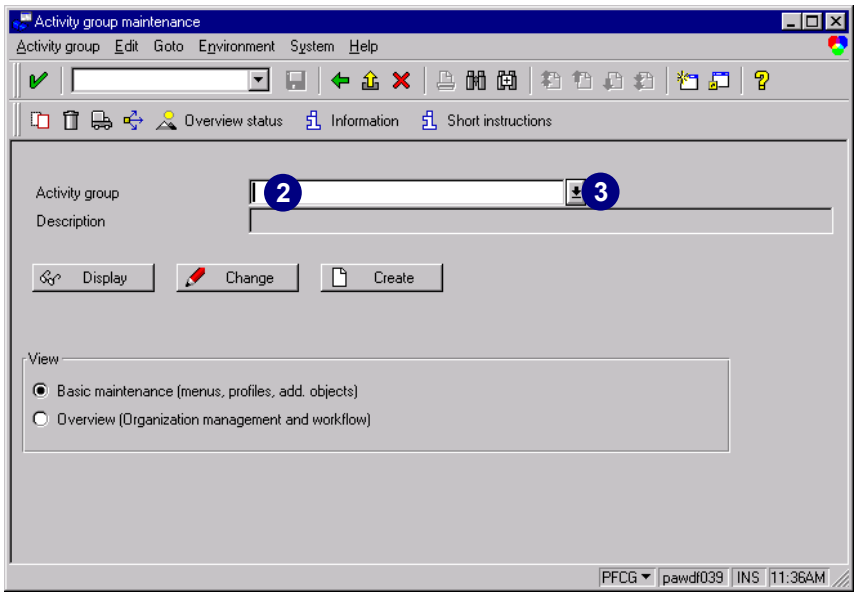
Displaying Activity Groups

Display activity groups to review the basic details of each group or verify the selected activities. You cannot make any changes to the activity groups in display mode.

1. In the *Command* field, enter transaction **PFCG** and choose *Enter* (or choose *Tools* → *Administration* → *User maintenance* → *Activity groups*).

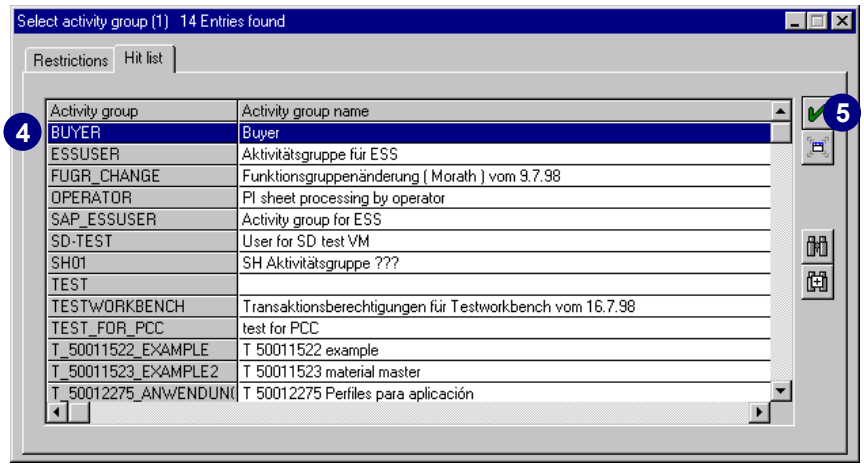


2. Position the cursor in the *Activity group* field.
3. Choose *possible entries*.

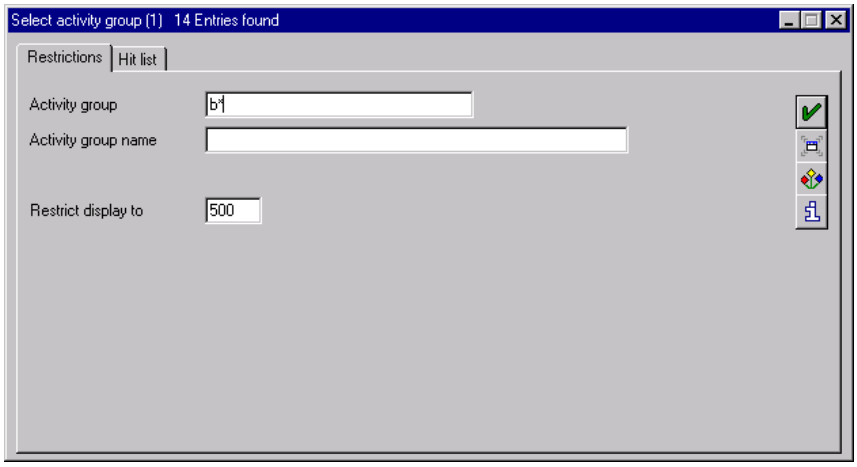


A *Hit list* appears.

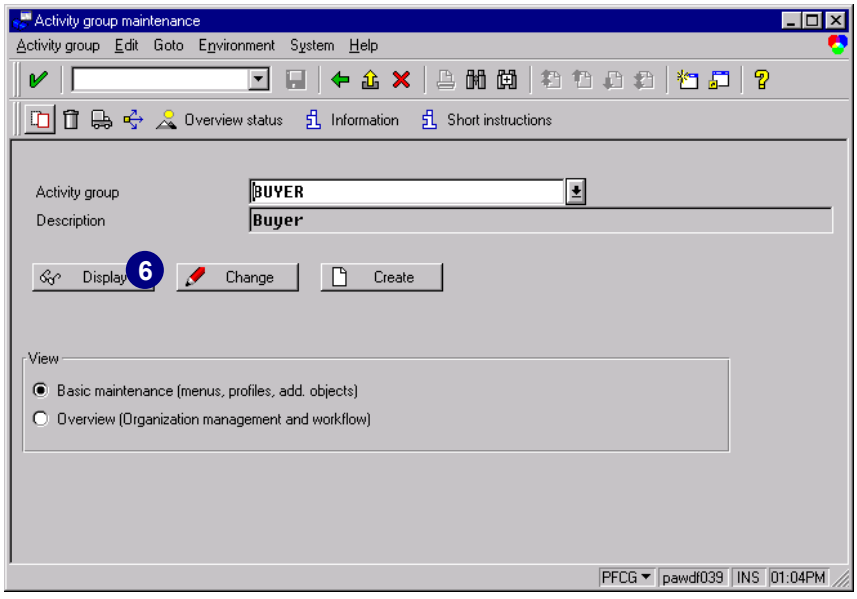
4. Select the activity group you want to display.
5. Choose *Copy*.



If the *Hit list* is too long, choose the *Restrictions* tab to narrow your search. Enter the first letters of the activity group you are looking for and choose *Start search*.

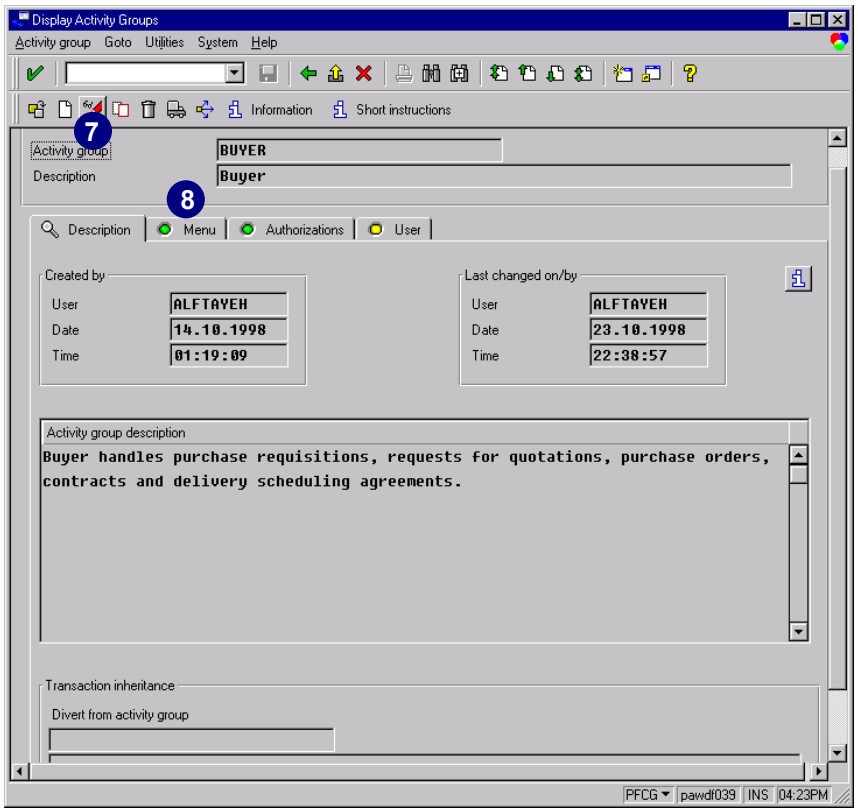


6. Choose *Display*.



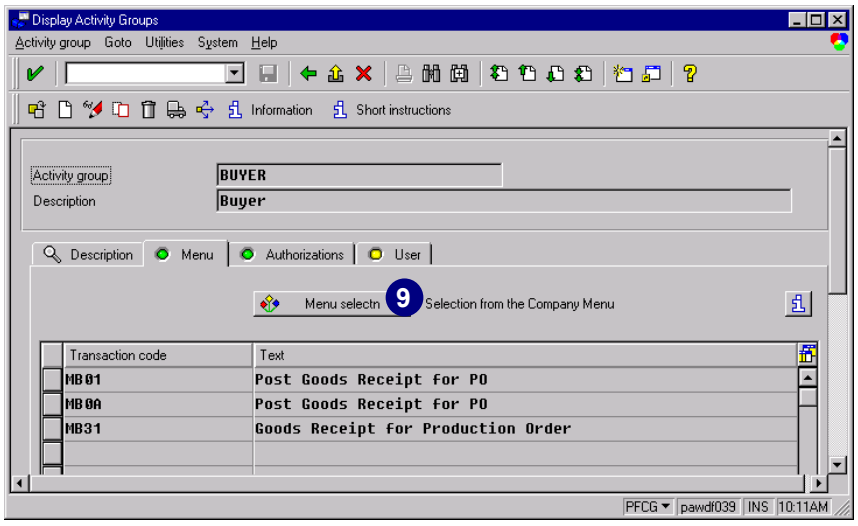
You are now in the display mode. Changes cannot be made in the *Display Activity Groups* window.

7. You can choose *Display* <-> *Change* to toggle between the display and change mode.
8. Choose *Menu* to review your transactions and reports selection for this activity group.

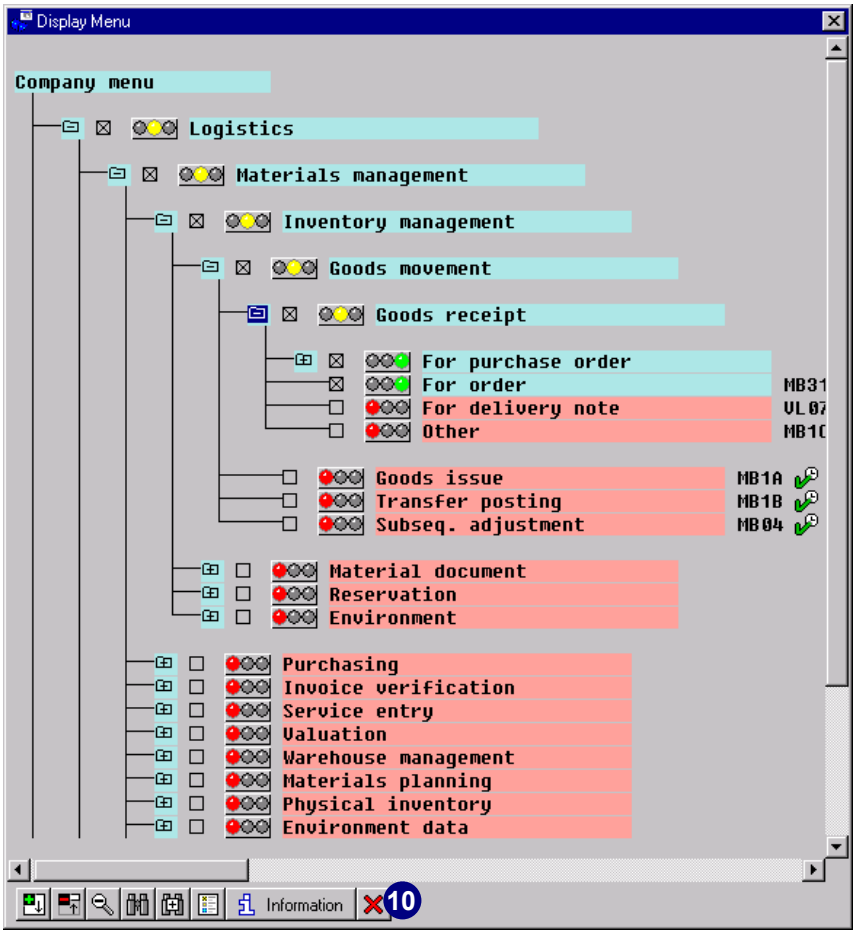


The selected transactions and their descriptions appear.

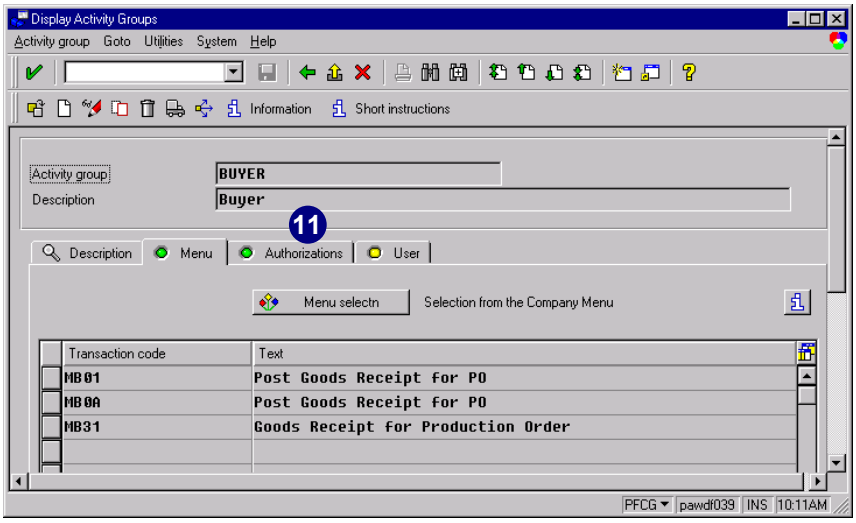
9. Choose *Menu selectn* to display the company menu structure.



10. Choose *Cancel* to go back.

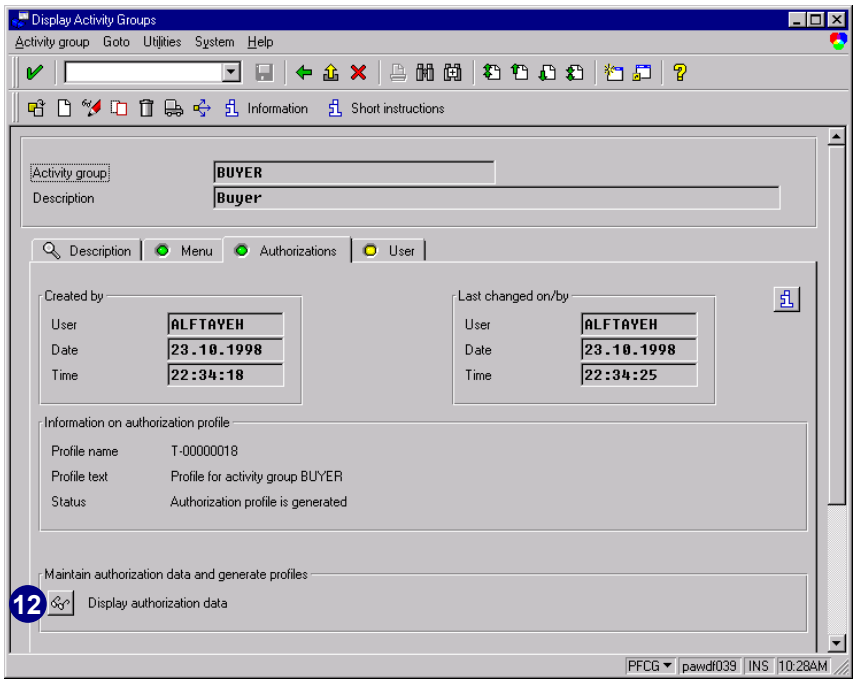


11. Choose the *Authorizations* tab to review the authorization data. The green light indicates the authorizations were previously generated.

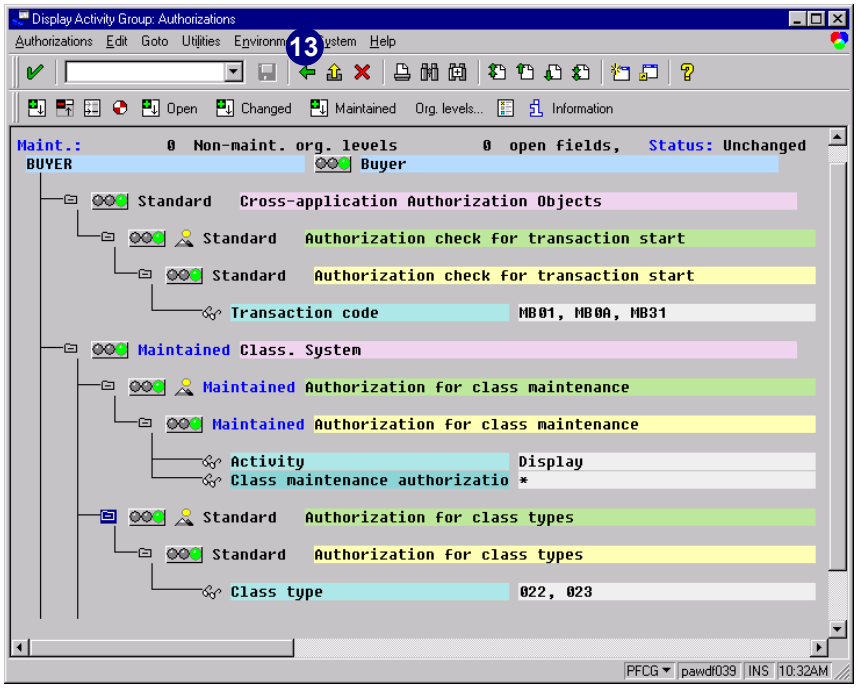


On this screen, you see general information on the authorization profile.

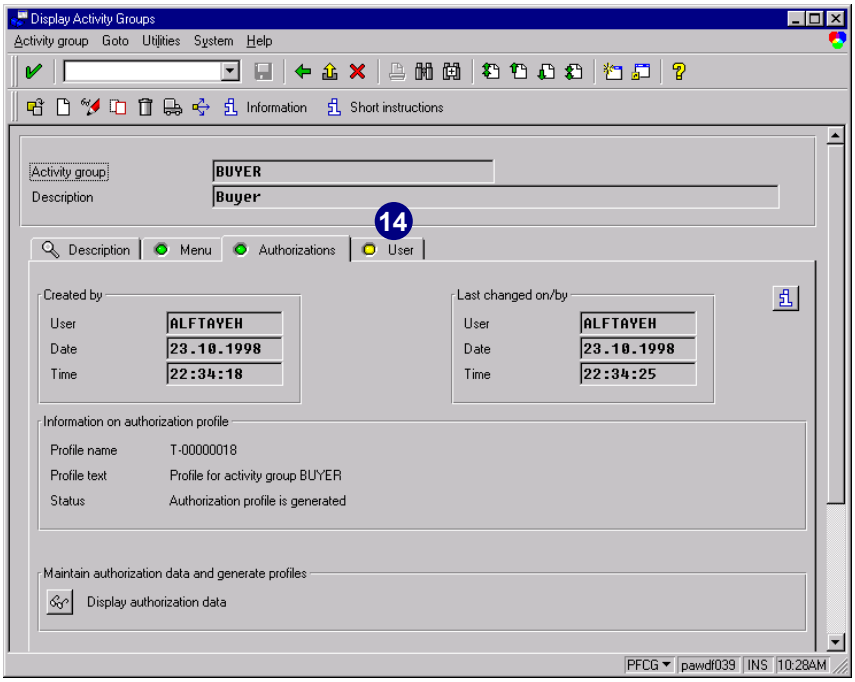
12. Choose *Display authorization data* to review the authorizations generated from the selection of transactions.



13. Choose *Back*.

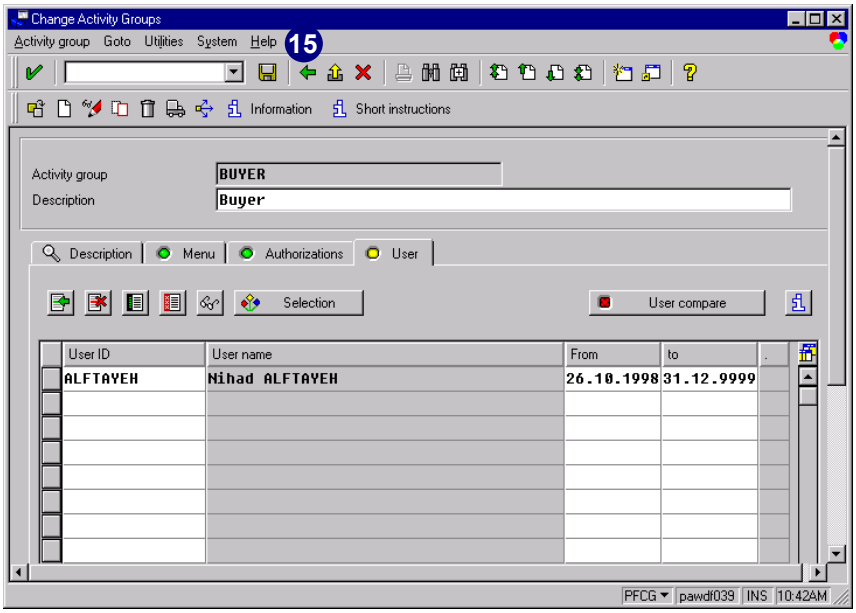


14. Choose the *User* tab to review assignments from this activity group to R/3 users.



The data for all assigned R/3 users for this activity group appear in the table.

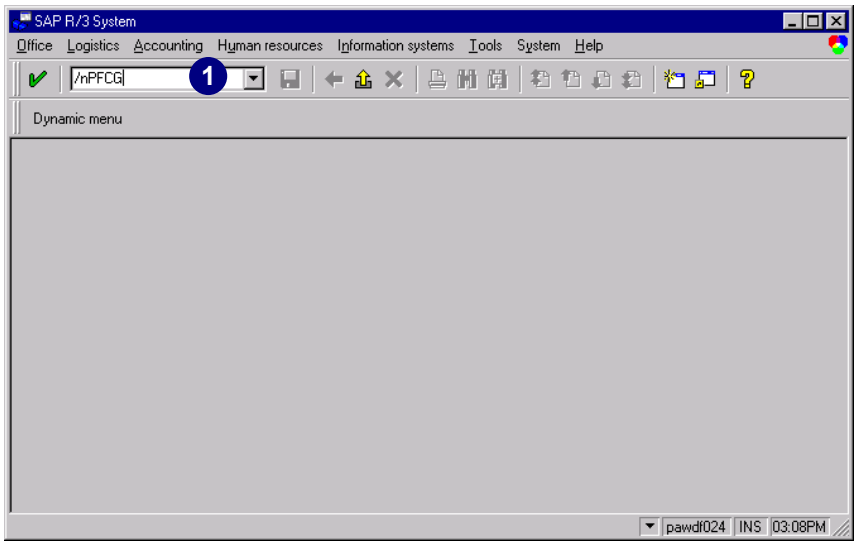
15. Choose *Back* twice to get to the initial screen.



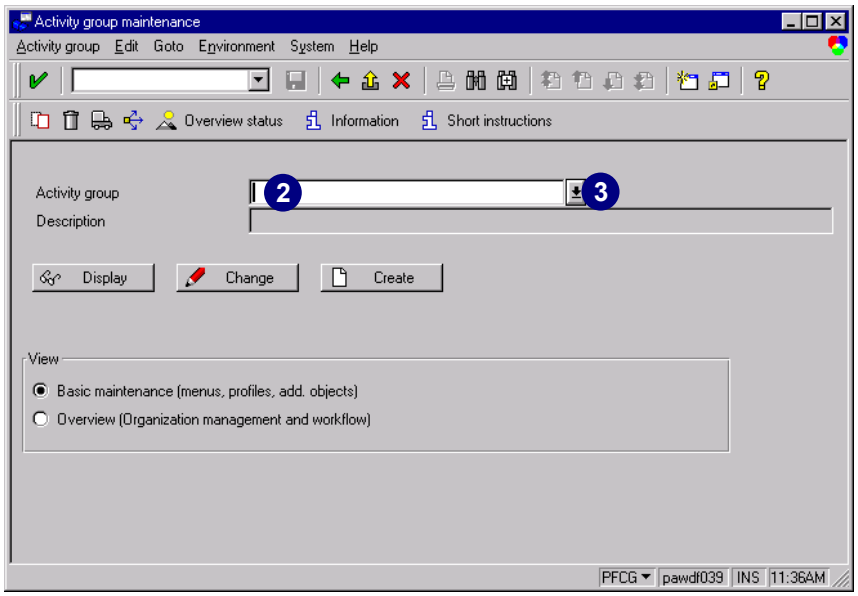
Changing Activity Groups

To edit an activity group's basic information or the activities assigned to it, you need to change the activity group.

1. In the *Command* field, enter transaction **PFCG** and choose *Enter* (or choose *Tools* → *Administration* → *User maintenance* → *Activity groups*).

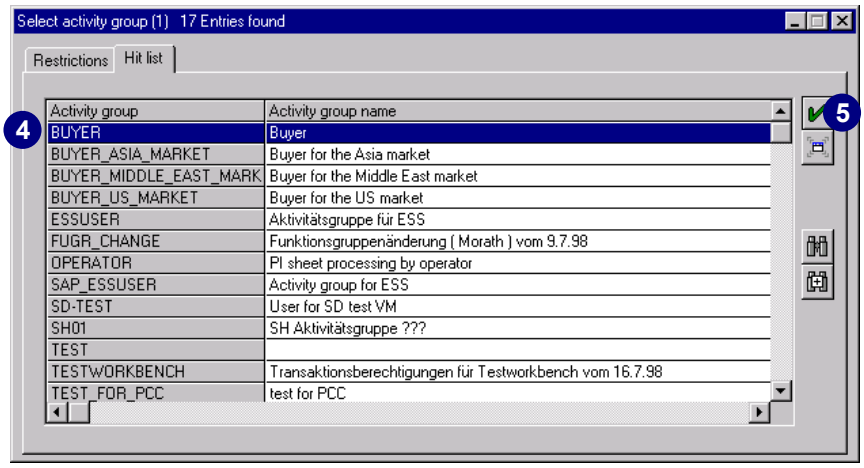


2. Position the cursor in the *Activity group* field.
3. Choose *possible entries*.

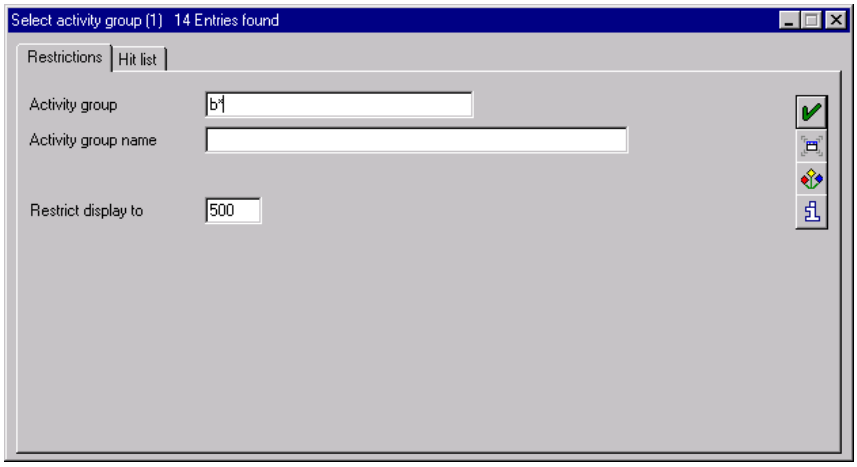


A *Hit list* appears.

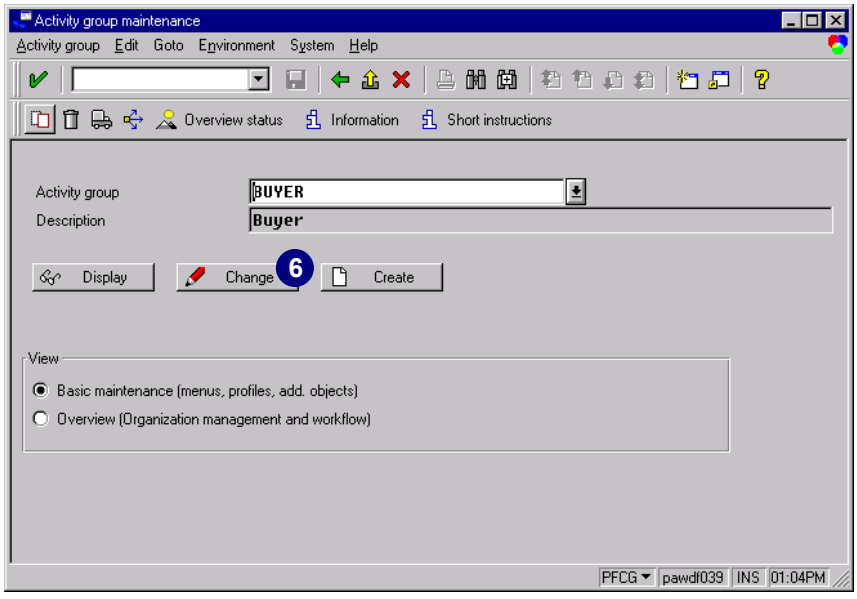
4. Select the activity group you want to change.
5. Choose *Copy*.



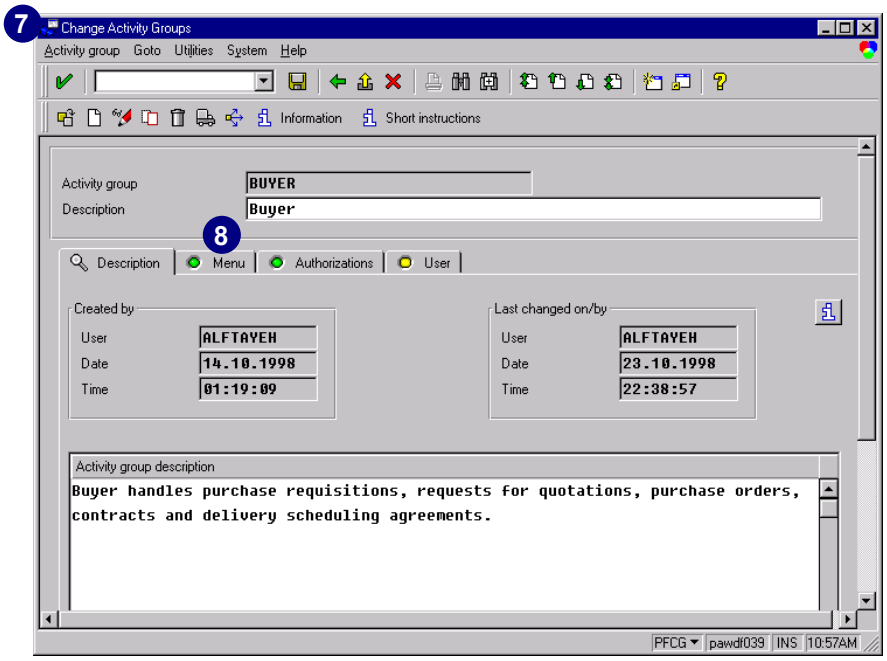
If the *Hit list* is too long, choose the *Restrictions* tab to narrow your search. Enter the first letters of the activity group you are looking for and choose *Start search*.



6. Choose *Change* to edit your activity group data.



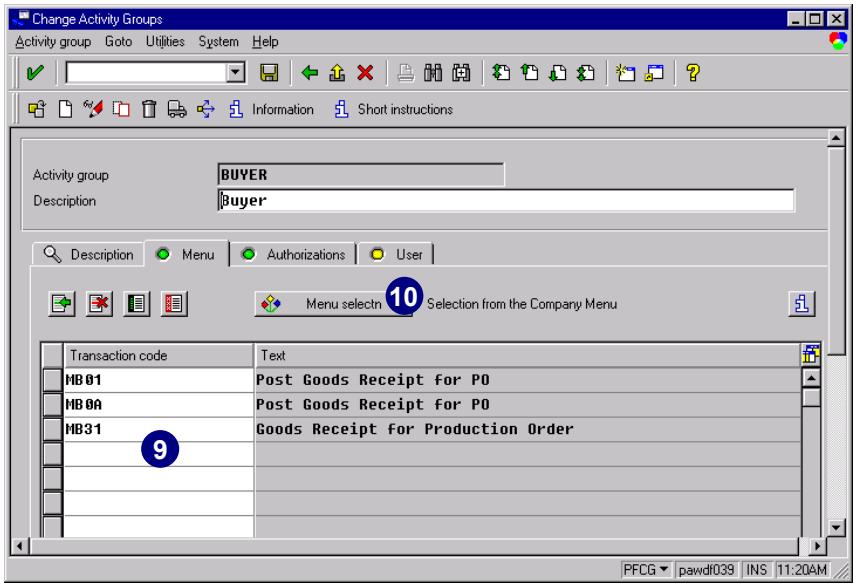
7. You are now in the *Change Activity Groups* mode.
8. Choose *Menu* to edit your transactions and reports selection for this activity group.



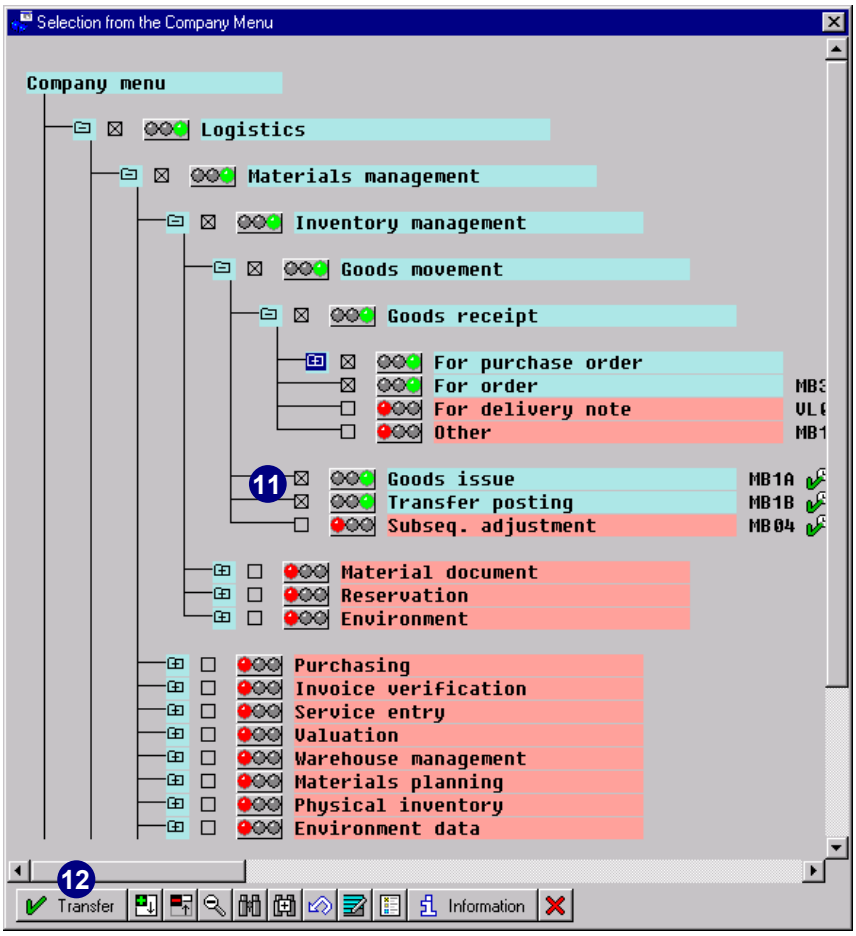
On this screen, you see the selected transactions and their descriptions.

You can add transactions directly by performing either step 9 or 10:

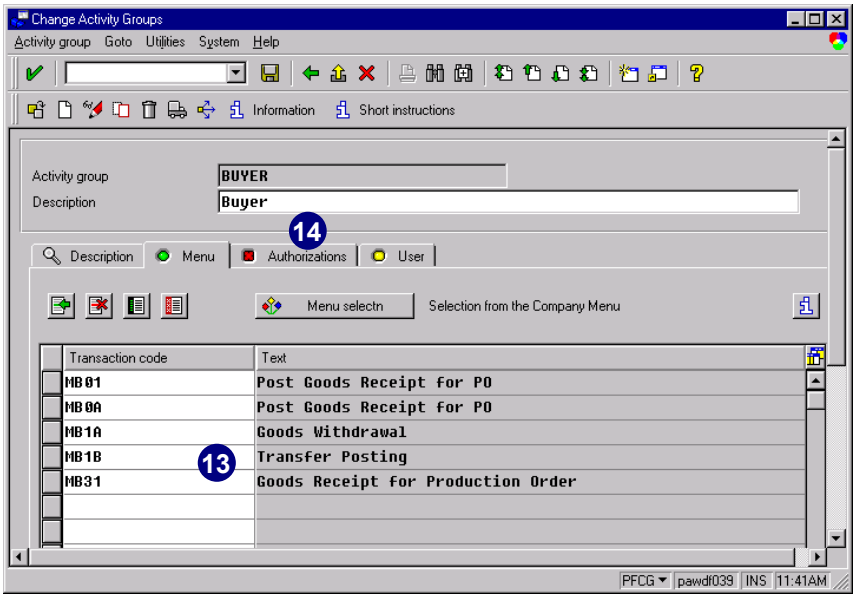
9. Enter the transaction code into the *Transaction Code* field.
10. Choose *Menu selectn* to edit the company menu structure.



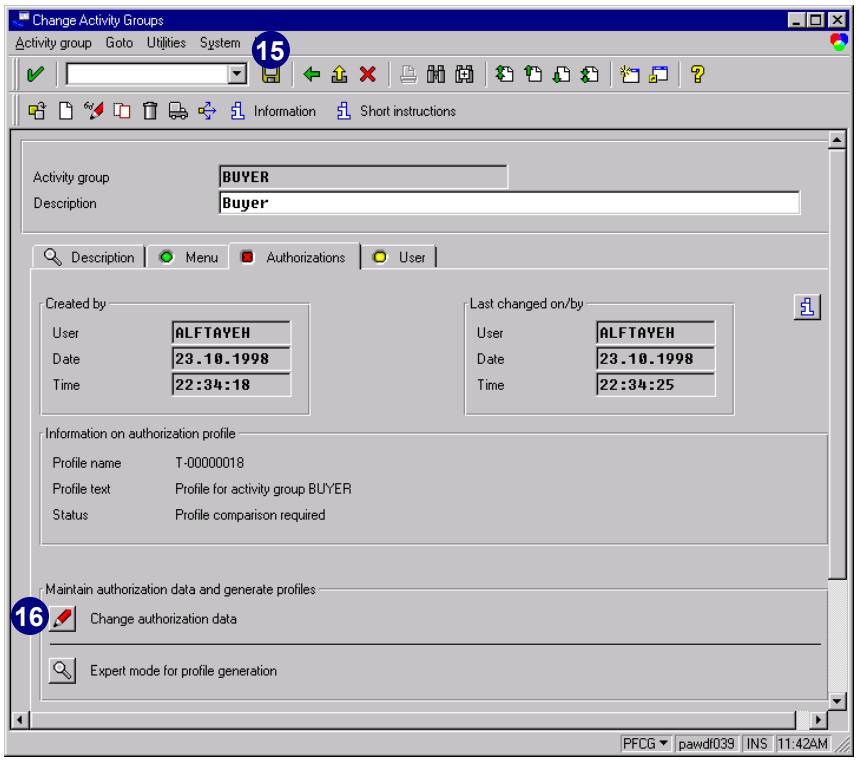
11. Select or deselect the transactions you want to add to your activity group from the *Company menu*.
12. Choose *Transfer* to transfer your changes into the activity group.



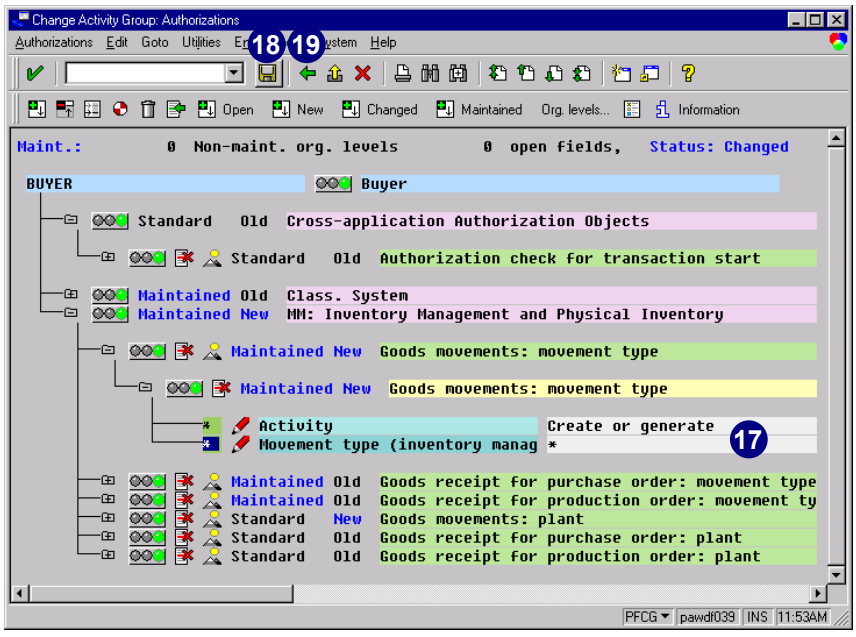
13. Your changes have been transfered and appear in the table.
14. Choose the *Authorizations* tab to edit the authorization data.



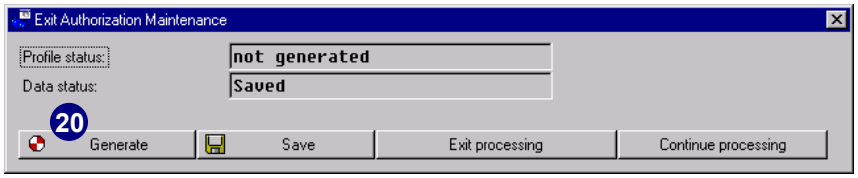
15. Choose *Save* to save your changes.
16. Choose *Change authorization data* to maintain the corresponding authorization field with the newly added authorization.



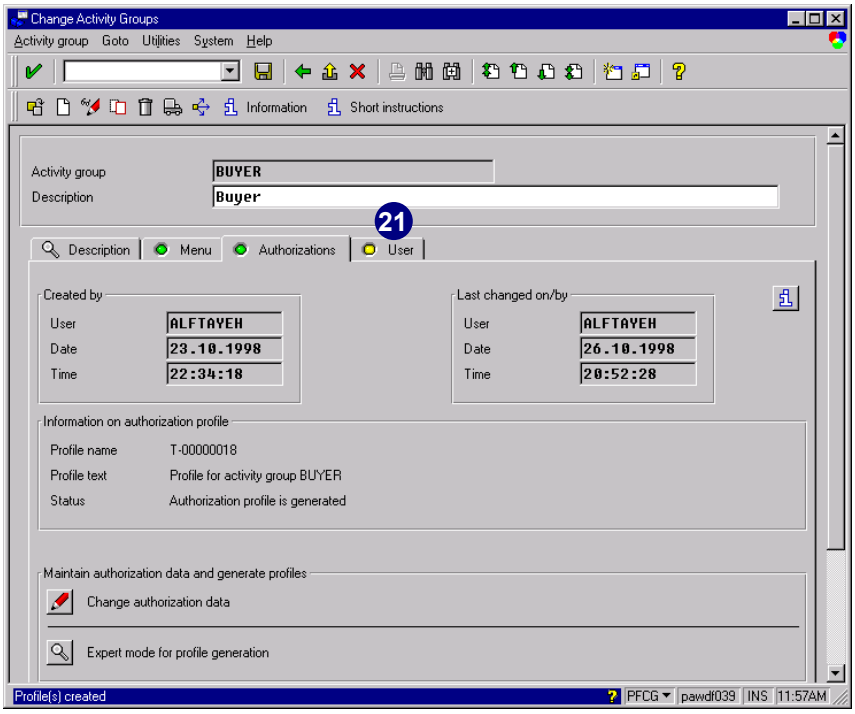
17. Enter the desired value for the authorization field.
18. Choose *Save* to secure your changes.
19. Choose *Back* to exit this screen.



20. Choose *Generate* to generate your changes.



21. Choose the *User* tab to edit and change any assignments from this activity group to R/3 users.

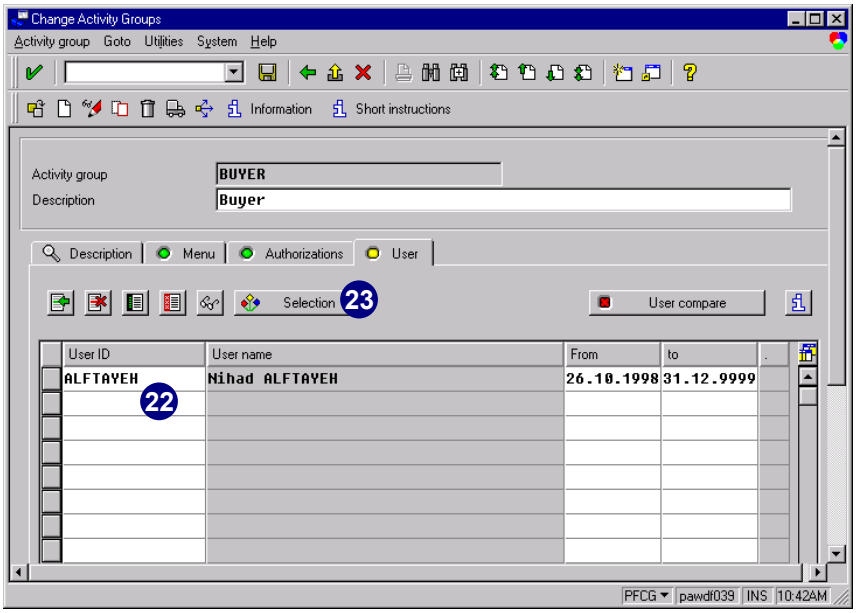


The data for all assigned R/3 users for this activity group appears in the table.

To add a user, perform either step 22 or 23:

22. Type their name directly into the *User ID* field.

23. Select the user from a *selection* list.



For detailed information on the user assignment see chapter 8 for more information.

Regenerating Authorization Profiles After Changes

When you change an activity group, you must regenerate its authorization profiles. Please see chapter 5 for more information.

Automatic User Assignment Update

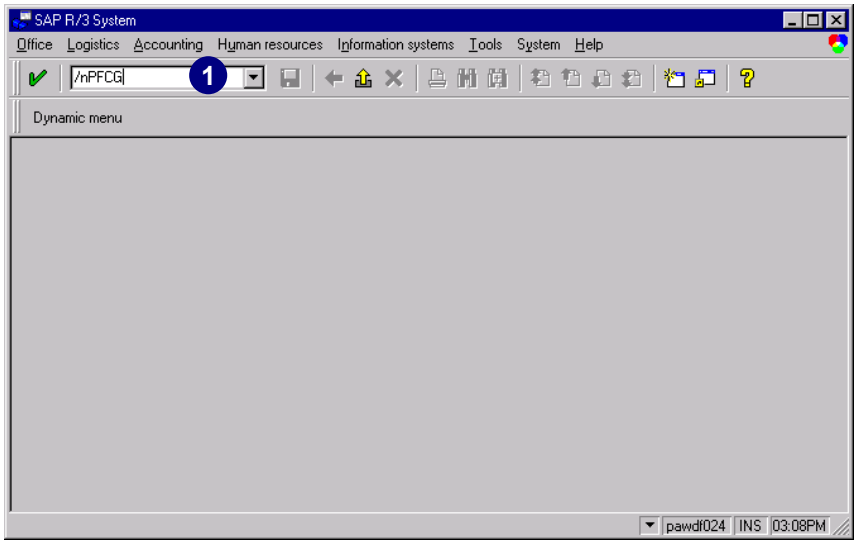
When you change an activity group that has already been assigned to users or PD objects, and a user compare has been done, do not update the assignment. Once you have regenerated the authorization profiles for this activity group, the user will automatically work with the latest generated authorization profiles after a new logon.

Deleting Activity Groups

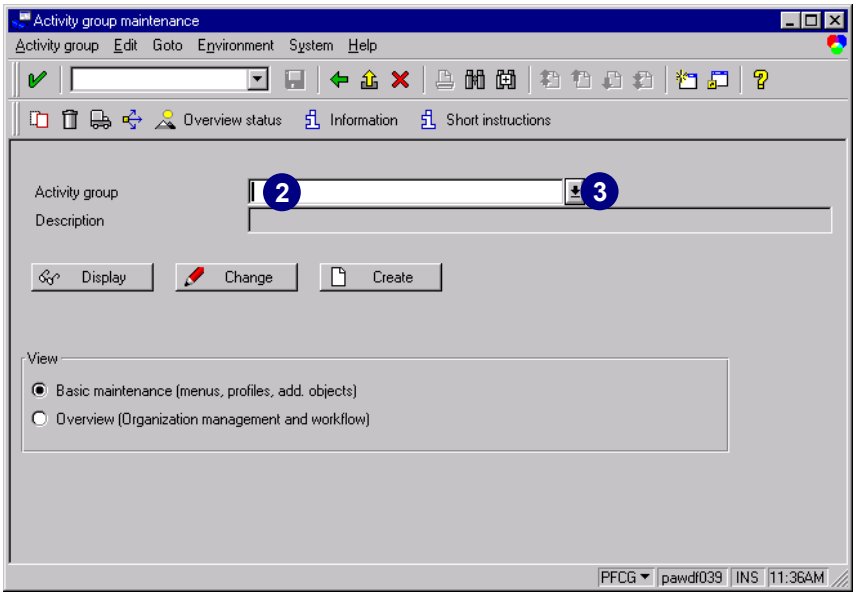
Delete activity groups when you no longer need them.

When you delete an activity group, the system automatically deletes any assignments existing between that activity group and R/3 users, positions, jobs, or organizational units.

1. In the *Command* field, enter transaction **PFCG** and choose *Enter* (or choose *Tools* → *Administration* → *User maintenance* → *Activity groups*).

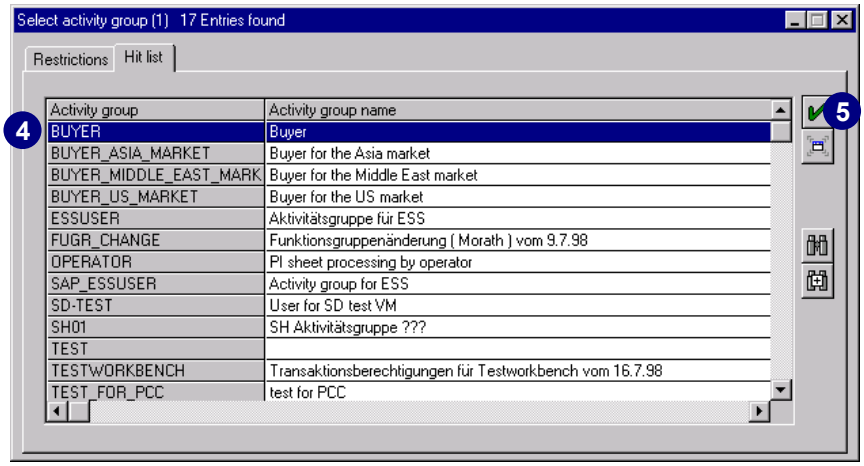


2. Position the cursor in the *Activity group* field.
3. Choose *possible entries*.

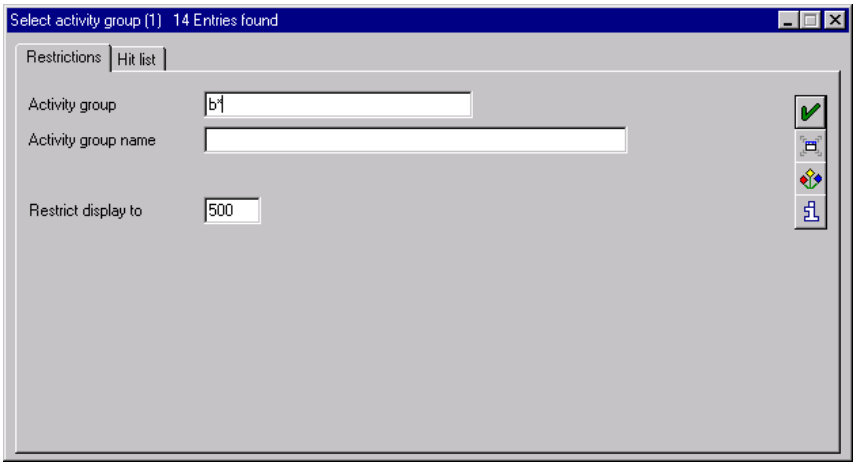


A *Hit list* appears.

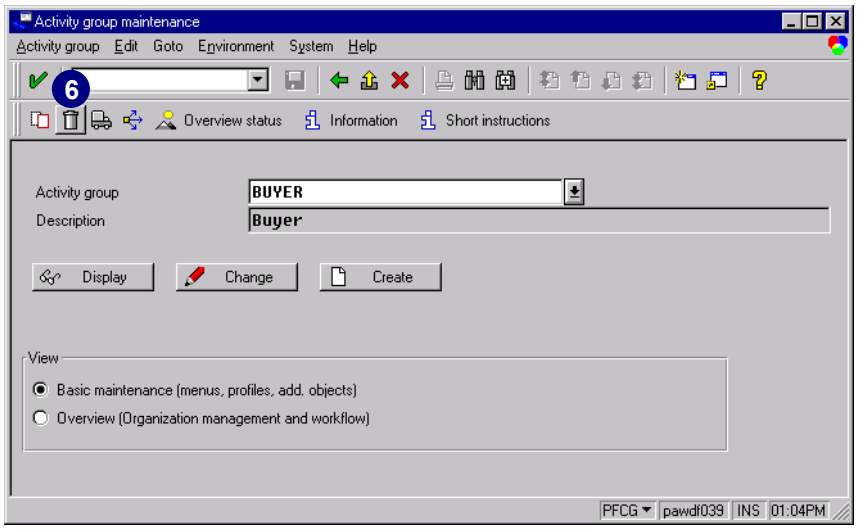
4. Select the activity group you want to delete.
5. Choose *Copy*.



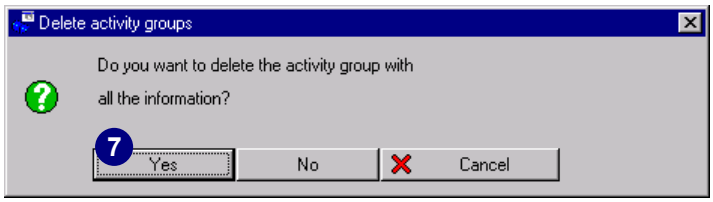
If the *Hit list* is too long, choose the *Restrictions* tab to narrow your search. Enter the first letters of the activity group you are looking for and choose *Start search*.



6. Choose *Delete* to delete the activity group.

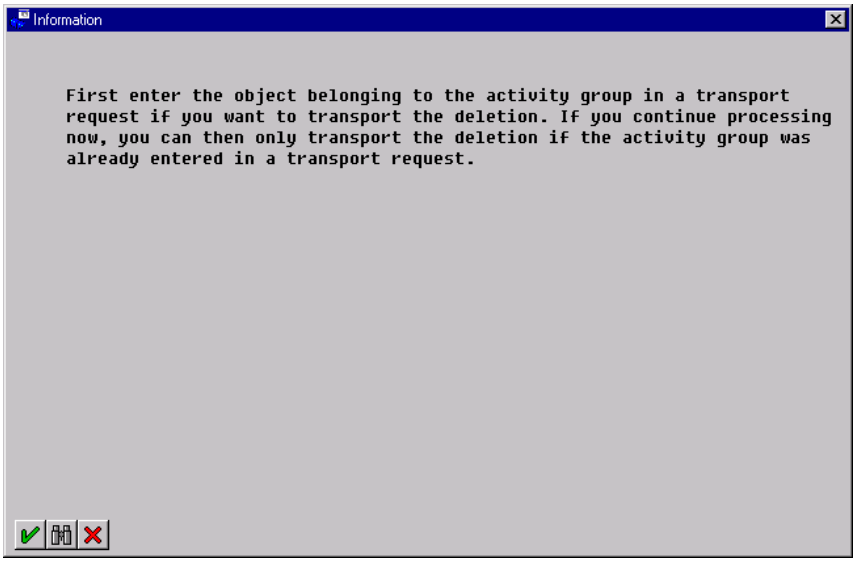


7. Choose *Yes* if this is the activity group you wish to delete.

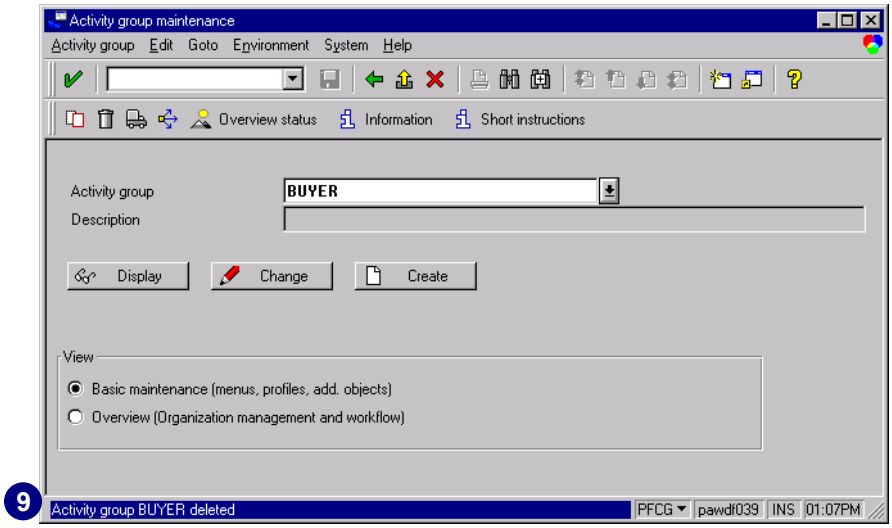


Verify that your activity group was actually entered in a transport request completed earlier, otherwise the deletion cannot be transported.

8. Choose *Enter*.



9. The chosen activity group and all the corresponding assignments have now been deleted.
The authorization profiles including the authorizations generated for this activity group are also deleted.



Important Information About Deleting

While deleting an activity group, the system automatically deletes the following:

- Assignments existing between this activity group and other objects
- Appropriate authorization profile(s) generated for this activity group
- Appropriate authorizations generated for this activity group

Transporting Activity Groups

Please see chapter 12 for information on how to transport activity groups.

Chapter 5: Generating and Maintaining Authorization Profiles

Contents

Overview

To generate an authorization profile, you must first create an activity group. (For more information on setting up activity groups, please see chapter 4.) Once you have defined an activity group, use the Profile Generator (PG) to automatically generate an authorization profile. Authorizations automatically generated for activity groups use SAP-supplied data, so that most fields are already filled with proposed values.

To generate an authorization profile:

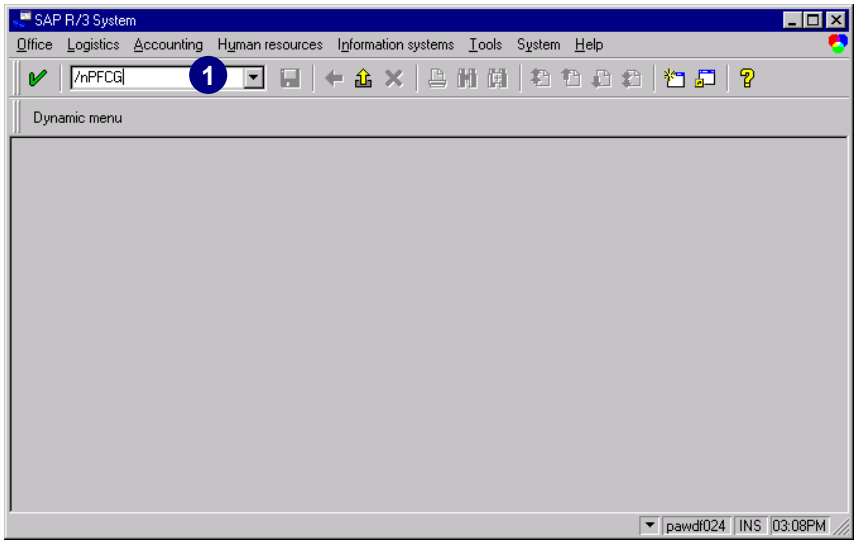
1. Start the generation process.
2. Maintain the organizational levels.
3. Postedit the authorizations and organizational levels.

Generating the Authorization Profiles

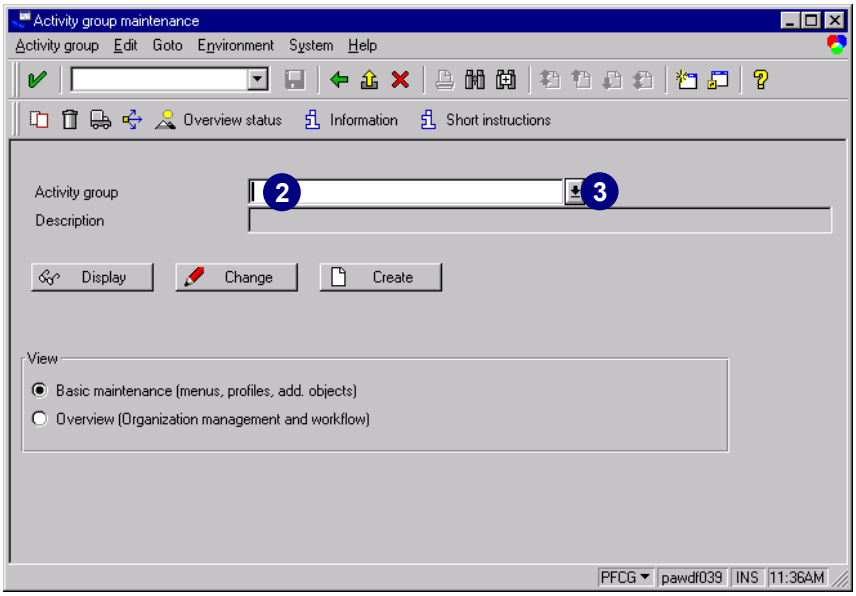
In this section, we assume the activity group has already been created and saved. In the next section, we will generate the authorization profiles for an activity group.

Starting the Generation Process

1. In the *Command* field, enter transaction **PFCG** and choose *Enter* (or choose *Tools* → *Administration* → *User* → *Activity groups*).

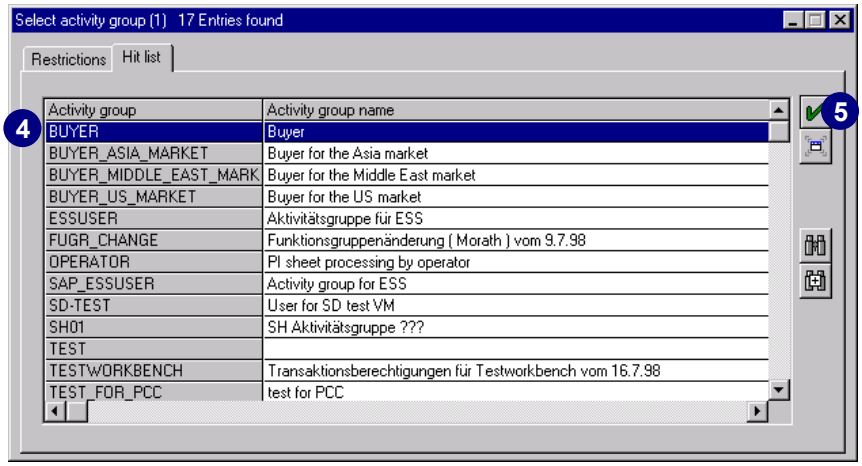


2. Position the cursor in the *Activity group* field.
3. Choose *possible entries*.

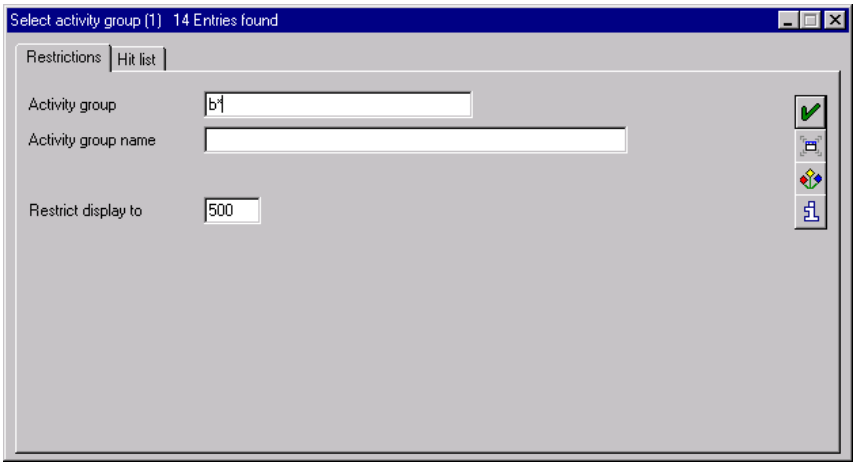


A *Hit list* appears.

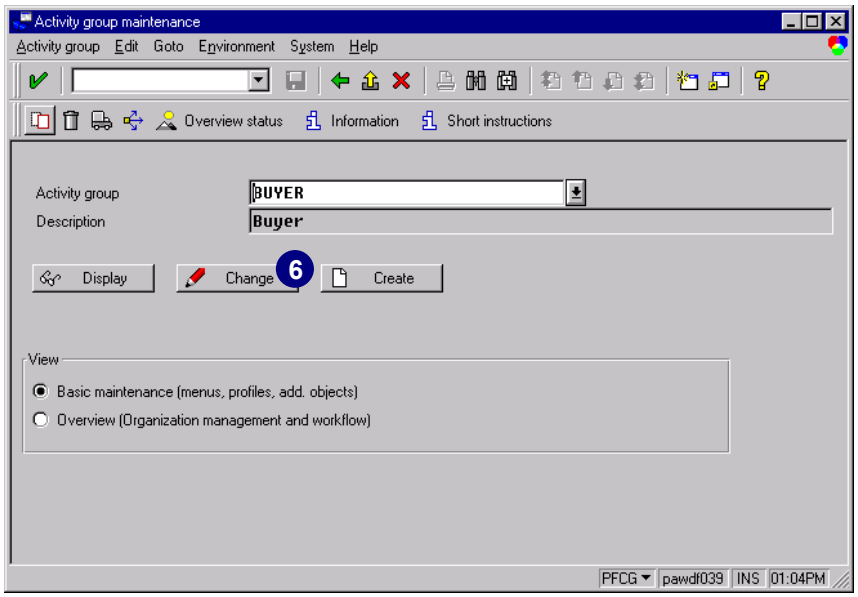
4. Select the activity group you want to edit.
5. Choose *Copy*.



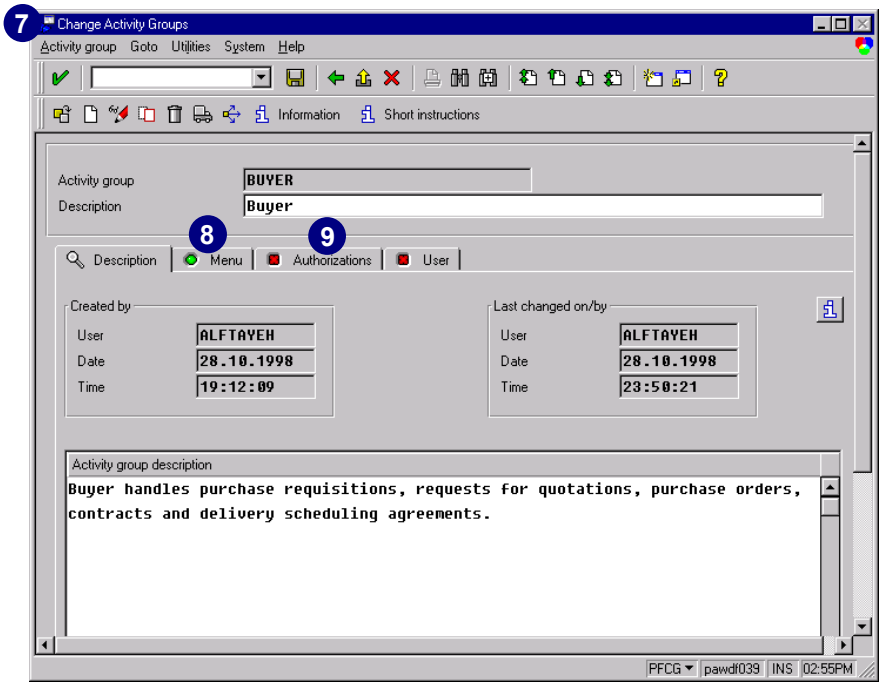
If the *Hit list* is too long, choose the *Restrictions* tab to narrow your search. Enter the first letters of the activity group you are looking for and choose *Start search*.



6. Choose *Change* to edit your activity group data.



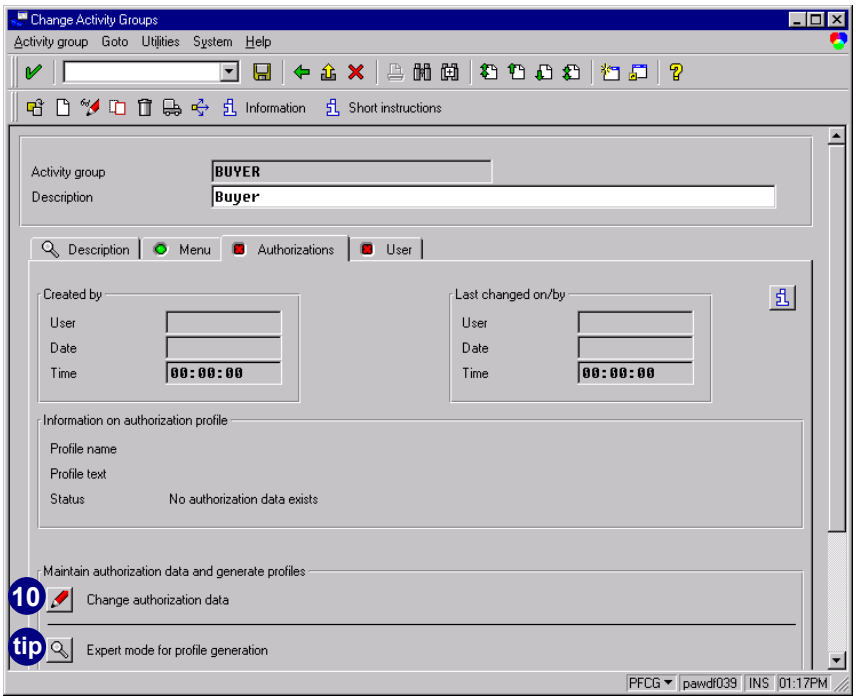
7. You are now in the *Change Activity Groups* mode.
8. The green light on the *Menu* tab indicates that you have already saved a menu selection for this activity group.
9. Choose the *Authorizations* tab to start the generation process.



To check the selected transactions, choose the *Menu* tab and verify your selection. You can also verify the menu structure by choosing the *Menu selectn* button.

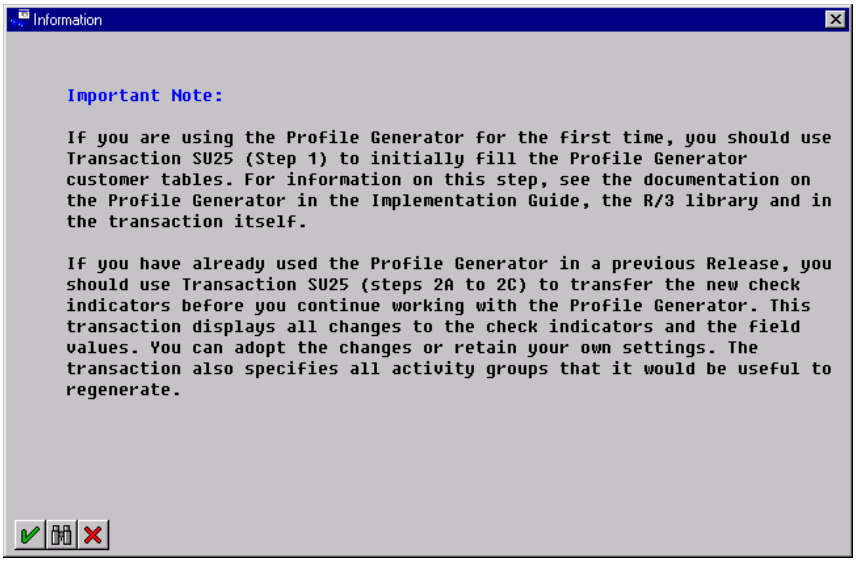
The red light on the *Authorizations* tab indicates that no authorization profiles have yet been generated for this activity group.

10. Choose *Change authorization data* to change and maintain the authorization data.



In *Expert mode for profile generation* you can select explicitly the option with which you want to maintain authorization values. This option is automatically set correctly in normal mode.

Should this information window pop up your customizing was not done succesfully and you would work with empty or old Profile Generator tables. Please complete or correct your customizing!



Maintaining Organizational Levels

1. The first time you choose the *Authorizations* tab, the *Define org. levels* dialog box appears.

   The system automatically identifies all open organizational levels fields needed to access the transactions from your activity group. You are prompted to maintain the organizational levels, which are SAP-defined authorization fields that refer to your company structure and occur in most authorizations.

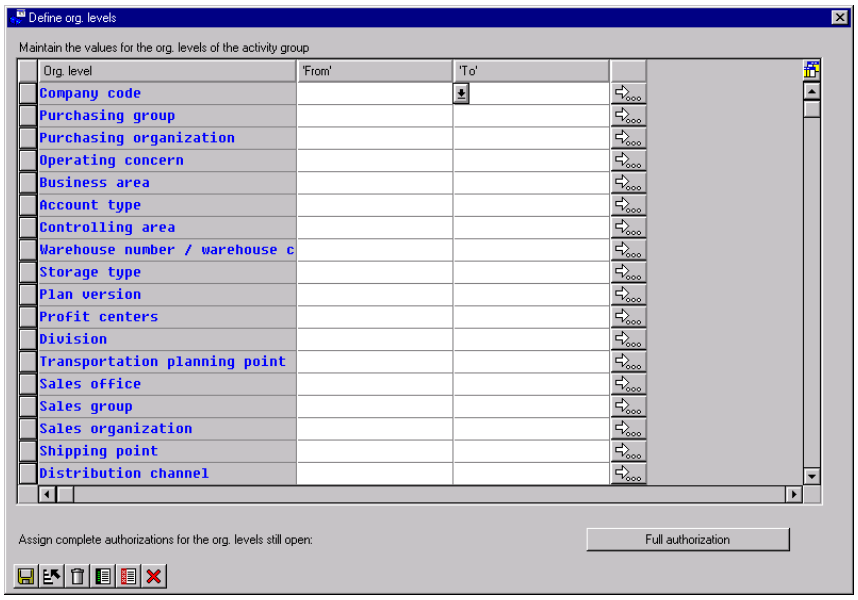
2. Position the cursor in the first '*From*' column.

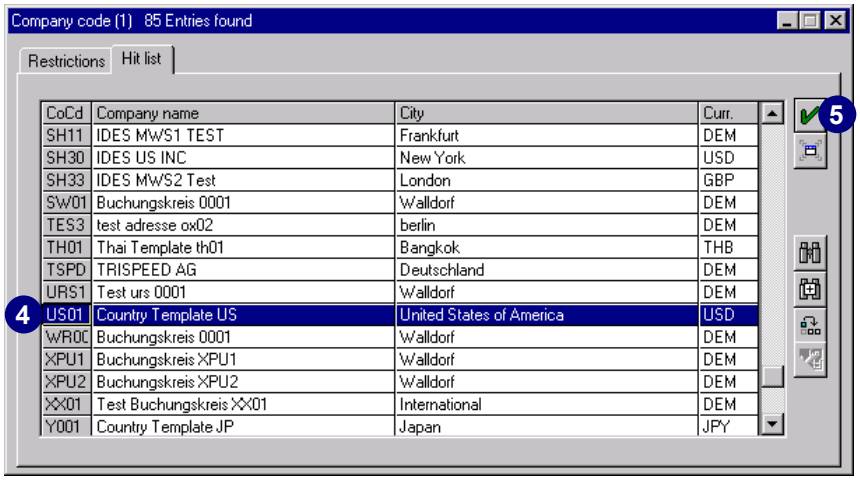
3. Choose *possible entries* for this field.

   A *Hit list* appears.

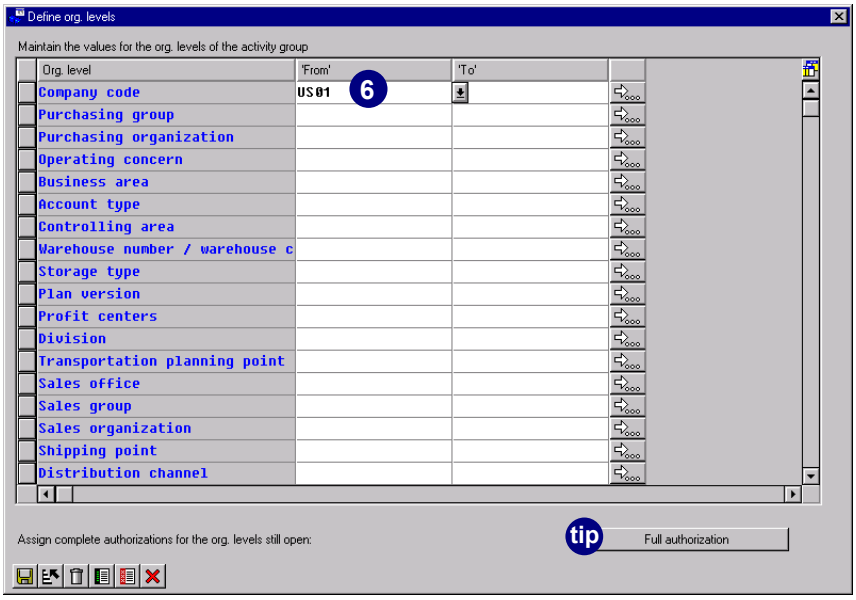
4. Select the entry you want to choose.

5. Choose *Copy*.





6. The value was transferred into the '*From*' column.
7. Repeat steps 1–6 for all other open fields.

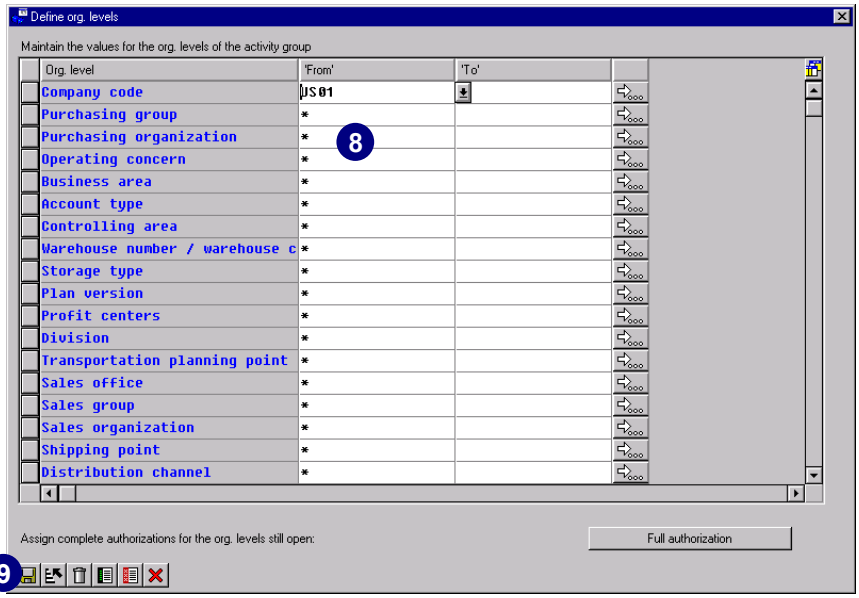


Choose the *Full authorization* button to fill the remaining open fields with an asterisk (*). The asterisk indicates complete access to any existing value for this field.

In this example, we chose *Full authorization*.

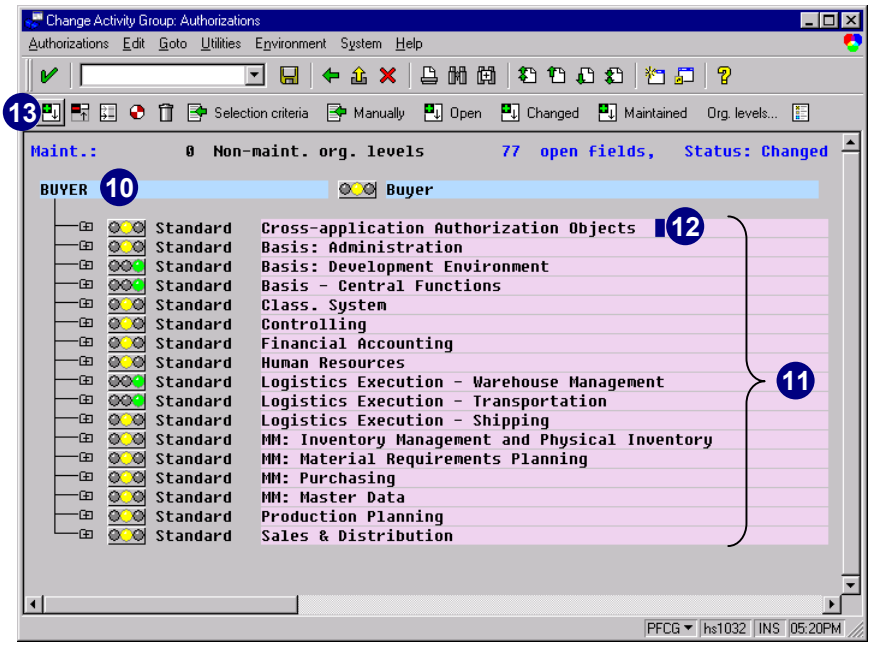
8. All open fields are now filled with asterisks (*).
9. Choose *Transfer*.

   Each *Org. level* field in the authorization is now filled with the values you entered for the corresponding organizational level.



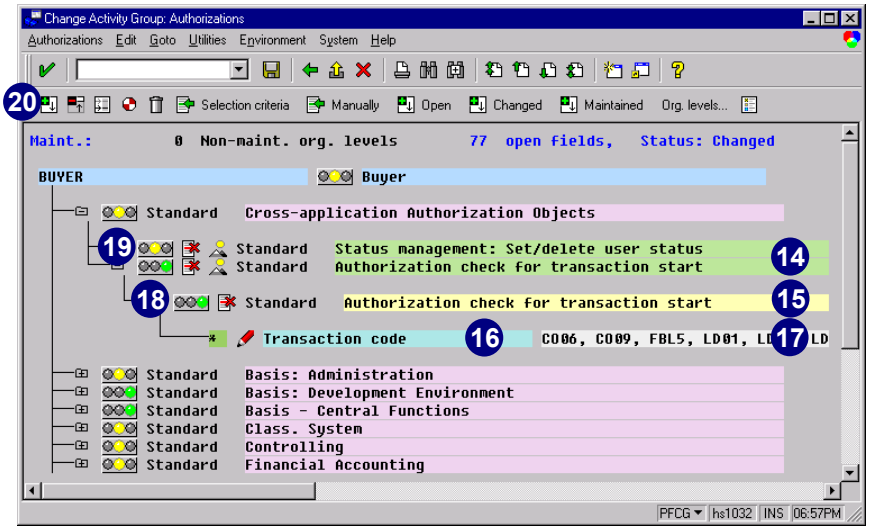
Company codes, business areas, and plants are examples of organizational levels. You can display and maintain a list of the existing levels with transaction *SUPO*.

10. The authorization data appears hierarchically. The activity group begins at the first level.
11. Underneath the activity group are the object classes of the relevant authorizations for this activity group.
12. Place the cursor in *Cross-application Authorization Objects*.
13. Choose *Expand* or click on the node at the beginning of the corresponding line.

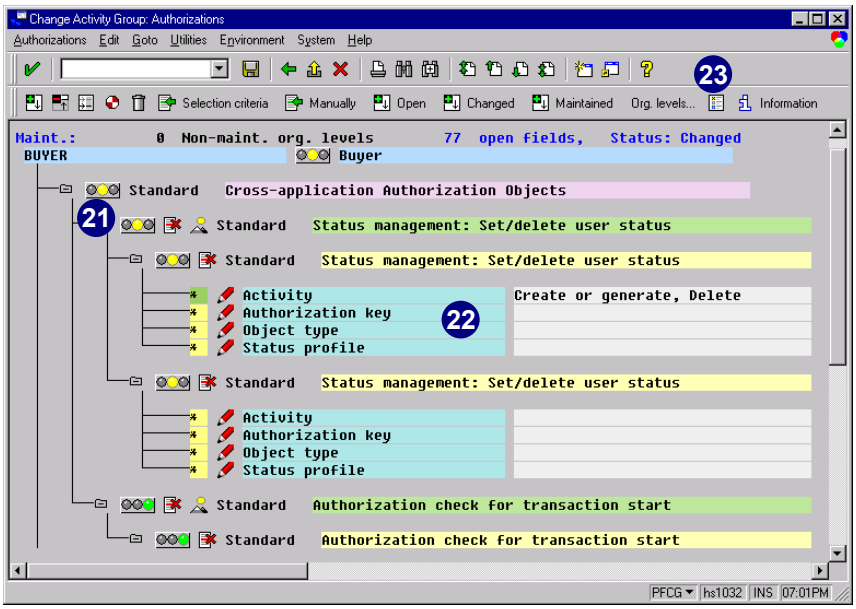


For a detailed explanation of the on-screen icons read *Elements and Symbols of the Hierarchy Display* on page 5–27.

14. The authorization object appears underneath the object class.
15. The authorization appears under the authorization object.
16. The authorization fields appear under the authorization.
17. To the right of the authorization fieldname is the field with the corresponding values. Most of the values are already filled with either SAP-defined values for the menu functions, or with the values you maintained for the organizational levels.
18. The green traffic light indicates that the authorization field values have been automatically maintained throughout R/3.
19. Position the cursor on any object class with a yellow traffic light.



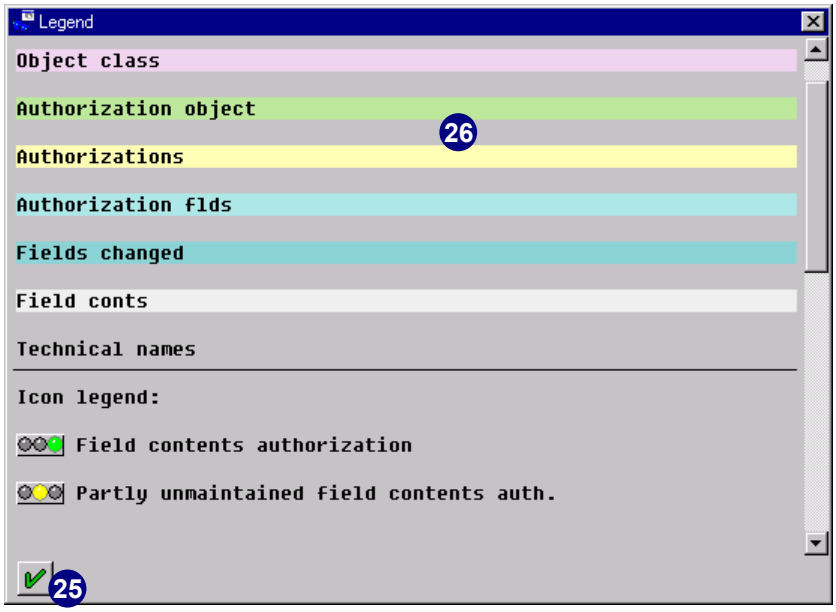
20. Choose *Expand*.
21. Open fields for authorizations that have not been maintained, where R/3 cannot automatically maintain values for you, will have yellow traffic lights.
22. In our example, there are some open fields for the authorization *Status management: Set/delete user status*.
23. To get a detailed explanation of the colors used, choose *Legend*.



24. On the *Legend* screen, you can see the colors, the icons, and their corresponding terms as they appear in the authorization procedure.

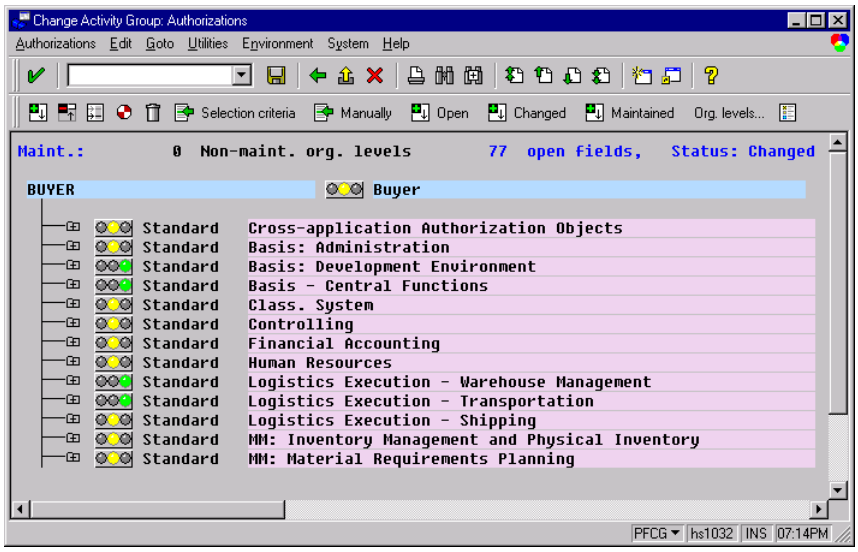
    Object class = purple
    Authorization object = green
    Authorization = yellow
    Authorization fields = light blue
    Fields changed = blue/green
    Fields conts = white

    Scroll down to display additional icons.
25. Choose *Continue*.



26. To generate the authorization profiles, all open authorization fields, indicated by a yellow or red traffic light, must be maintained with corresponding values.

    The next section describes two options for filling in the missing values for these authorization fields.



Postediting Authorizations and Organizational Levels

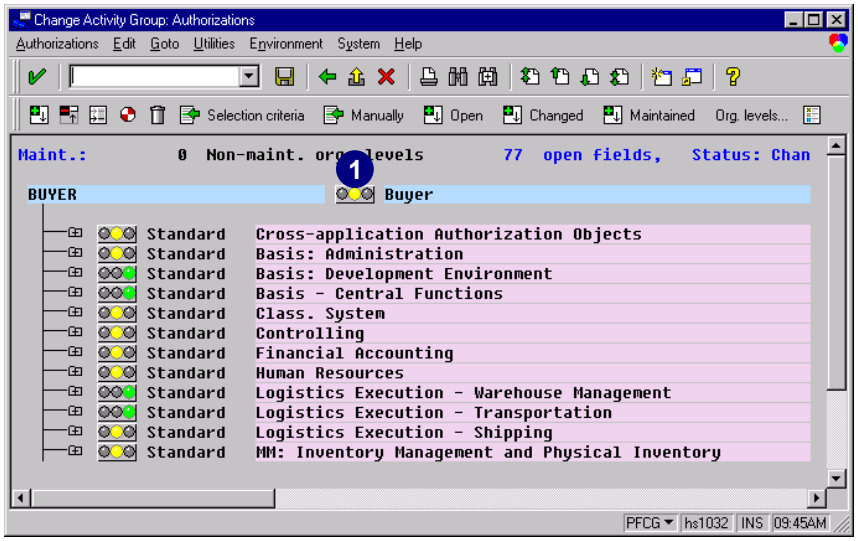
There are two options to generate authorization profiles. **Option A** is the faster solution; **option B** is not as fast, but is more thorough. These options are described in the following subsections.

Option A demonstrates how to quickly generate authorization profiles by assigning complete authorizations to all non-maintained authorization fields. You may return to the profiles later to place additional restrictions on them.

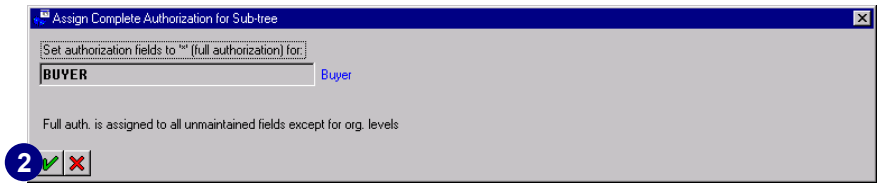
Option B (in the next section, page 5–13) restricts further activities in your activity group.

Option A

1. Click the yellow traffic light for the activity group.

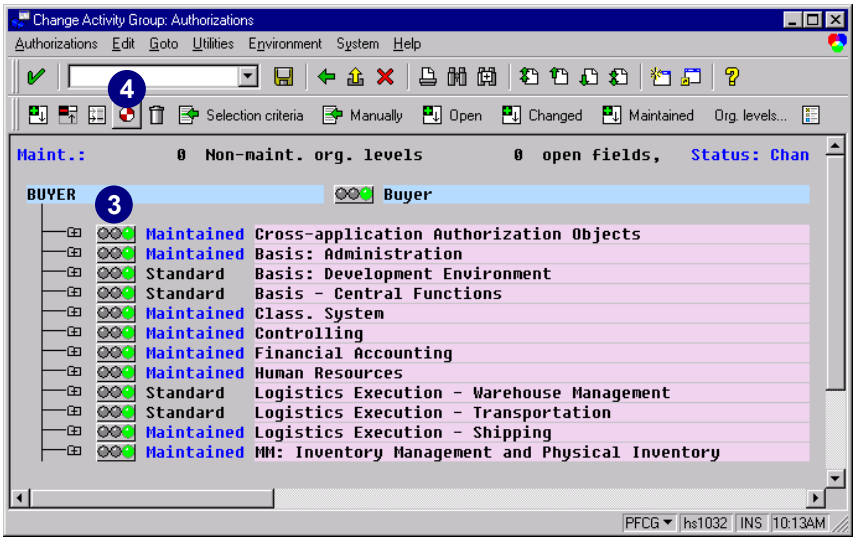


2. Choose *Enter* to confirm that you want to assign a full authorization (*) to all open authorization fields.



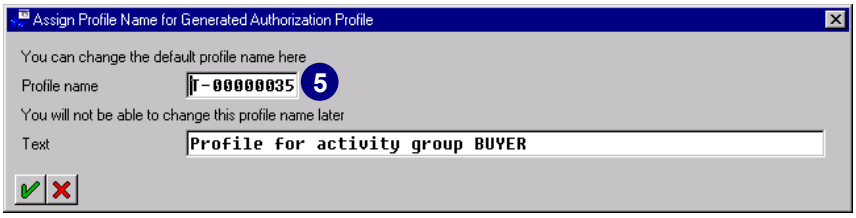
Full authorizations will be assigned to all unmaintained authorization fields of the current activity group that are indicated by a yellow traffic light, except for open organizational level fields, which are indicated by a red traffic light.
This can be done at every traffic light on every hierachy level.

3. Now, all of the yellow traffic lights change to green, and all open authorization fields are simultaneously filled with an asterisk (*).
4. Choose *Generate* to save and generate the authorization profiles.



5. The *Assign Profile Name for Generated Authorization Profile* dialog box appears. By default, the profile's name is *T-<internal number>*.

   The short *Profile name* cannot be changed later. However, the long *Text* for the profile can be changed at any time.



Naming Conventions for Authorization Profiles and Authorizations Generated with the Profile Generator

When you save your changes, you are prompted to enter a profile name. However, only the first 10 characters (the profile torso) can be freely assigned. The number of profiles generated depends on the number of authorizations in each activity group. A maximum of appr. 150 authorizations can fit into a profile. If there are more than 150 authorizations, an additional profile is generated. It has the same 10-character torso as the profile name, and the last two digits are used as a counter.

To avoid conflicts between customer-defined and SAP-supplied profiles, do not use a name that has an underscore (_) in the second position. SAP places no other restriction on naming authorization profiles (refer also to OSS note 16466). If your company has its own naming convention, you may overwrite proposed names.

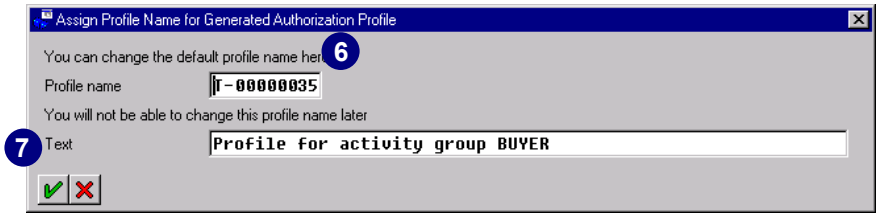
The authorization names are also derived from the profile torso. If more than one authorization is required for an object, the last two digits are counters.

Depending on the authorization profile name, the technical names for authorizations are then named as follows:

- Begin with a *T-*
- Comprise an internal number
- End with a two-digit number between *00* and *99*

Sample authorization name: T-5000001900

6. Rename the authorization *Profile name* with your company convention if necessary.
7. Choose *Execute*.



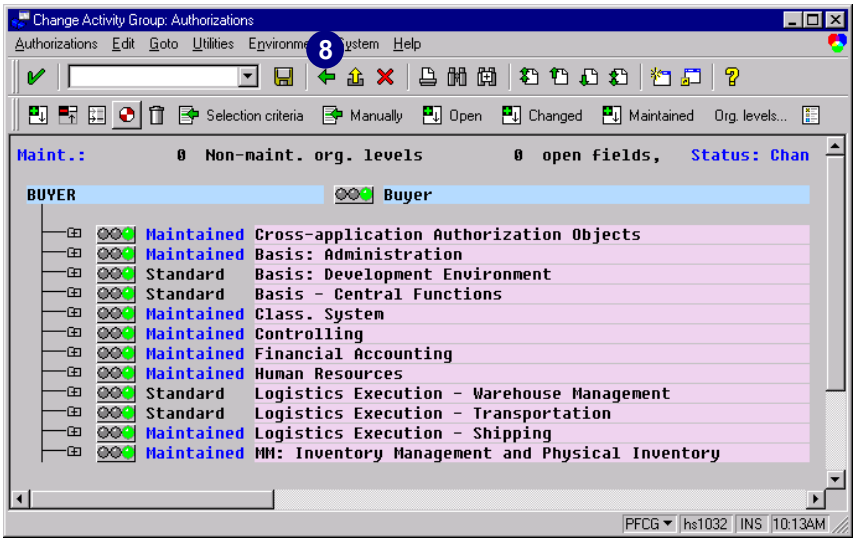
The authorization object *S_USER_PRO* is checked during authorization maintenance. This object is defined with the following fields: *Authorization profile* and *Activity*. In *Authorization profile*, enter the authorization profiles that authorization administrators will maintain or that user administrators can assign to their users. In *Activity*, you can limit what administrators are allowed to do.

Please note, if you want to set up an authorization administrator who can maintain only certain profiles, set up your own naming convention.

Congratulations. You have just generated the authorization profile.

8. To exit transaction *PFCG*, choose *Back* three times.

   To assign the activity group to an R/3 user or a position, please see chapter 7.

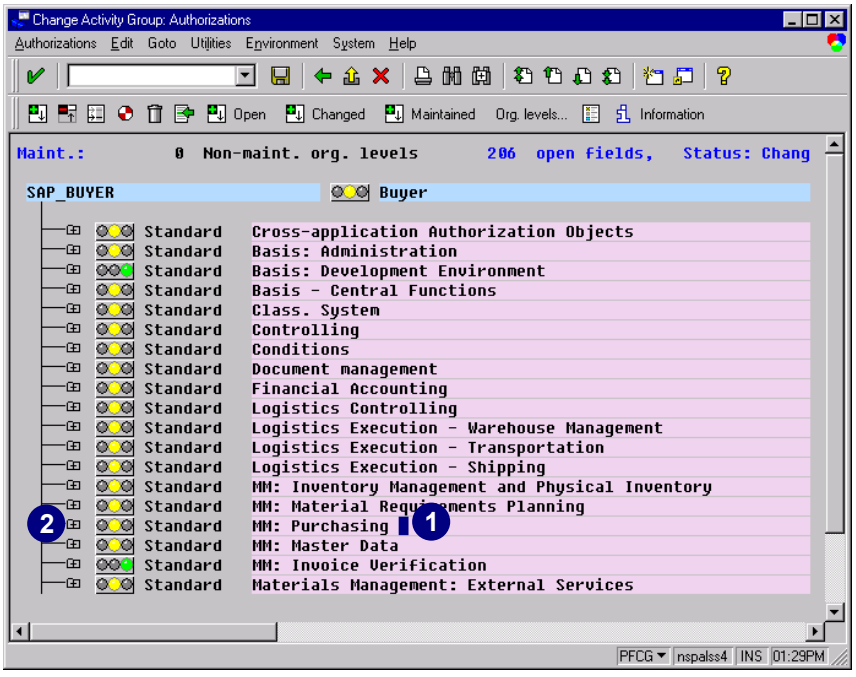


Option B

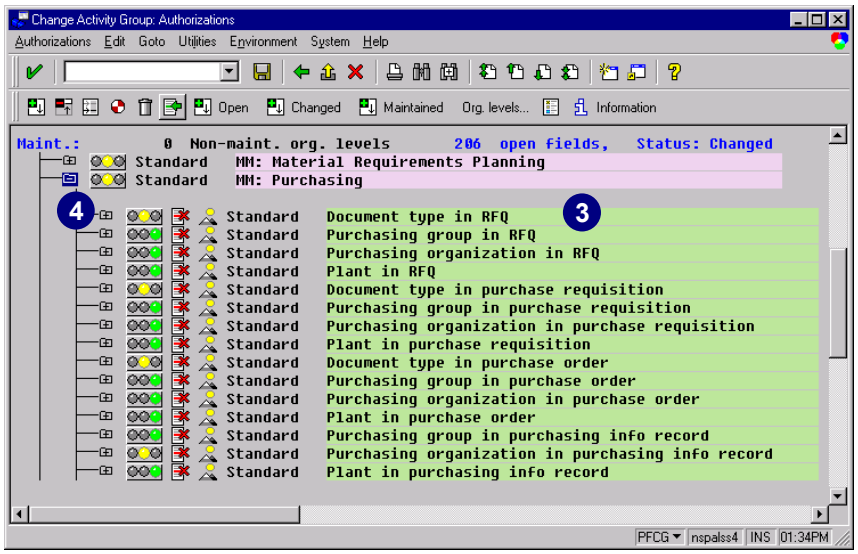
Option B demonstrates how to thoroughly generate the authorization profiles. Choose this option to restrict authorization profiles.

Please see *Elements and Symbols of the Hierarchy Display* on page 5–27 for a detailed explanation of the icons.

1. Position the cursor over an object class with a yellow traffic light (for example, *MM: Purchasing*).
2. Click the node at that beginning of the line to open the hierarchy.

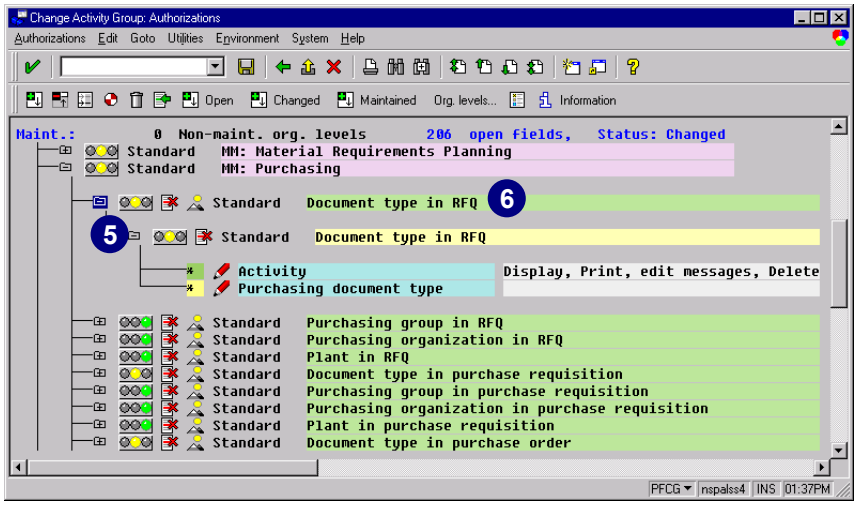


3. Under *MM: Purchasing*, notice the authorization objects for the authorization profile(s) you will create. These objects were automatically generated by the R/3 System.
4. In the list under *MM: Purchasing*, click the node of an authorization object with a yellow traffic light (for example, *Document type in RFQ*).

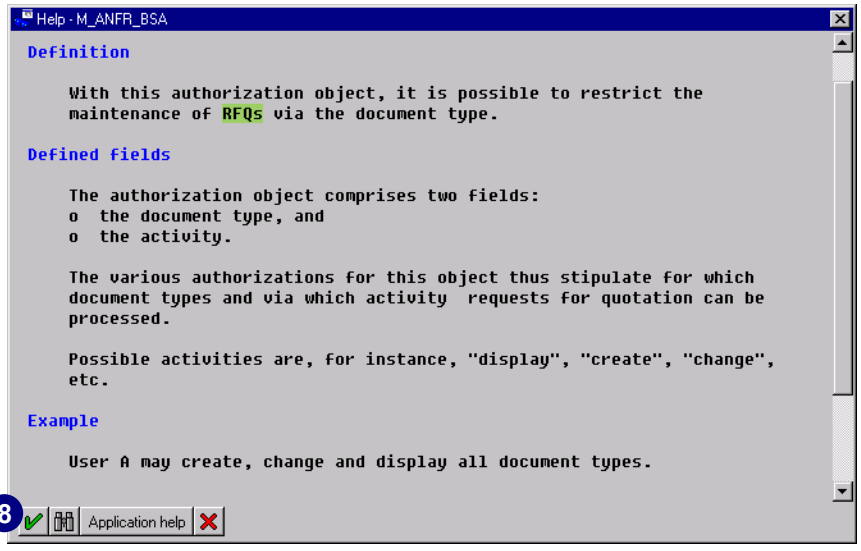


5. Under the authorization object are the existing authorizations (here just one).

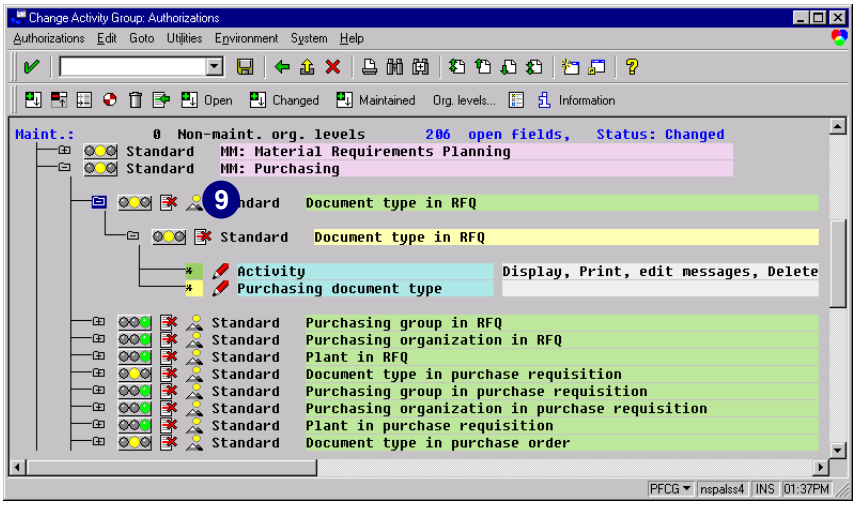
   First read the documentation for each authorization object with open authorization fields.
6. To view the documentation, double-click on the authorization object text.



7. Carefully read the entire document; you might have to scroll down.
8. When you have finished reading, choose *Continue*.

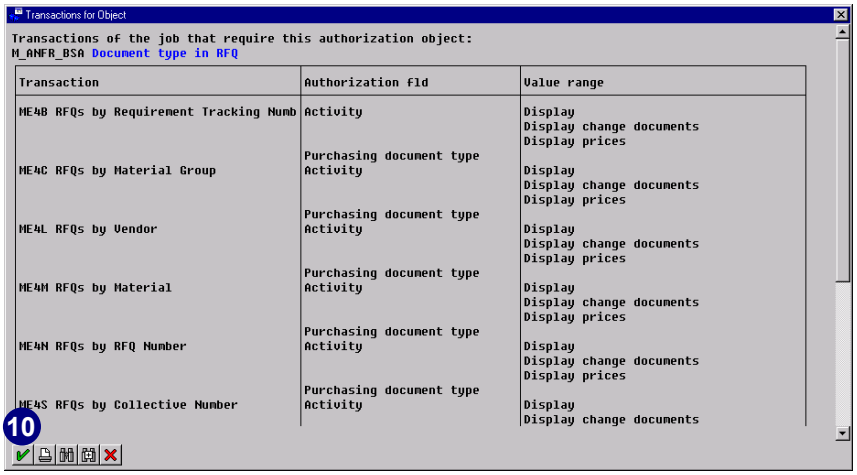


9. Choose the *Overview* icon to display all selected transactions that check this authorization object for the underlying activity group.

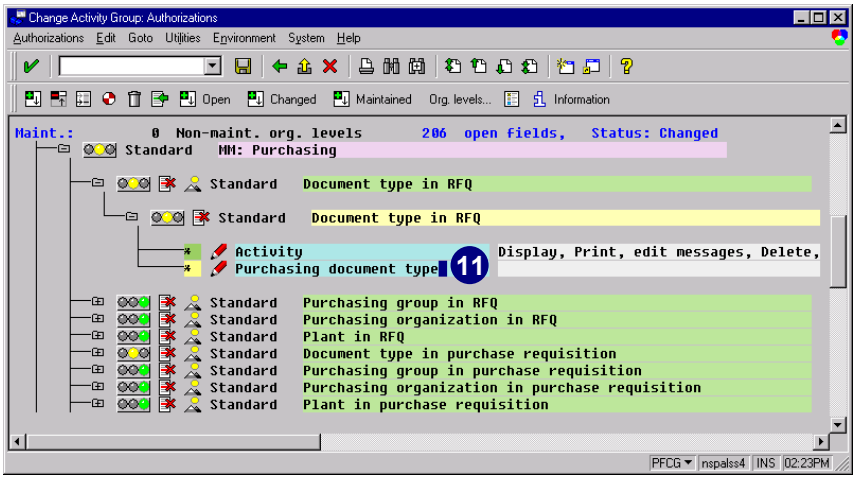


On the *Transactions for Object* screen, you see the transactions of the job that require this authorization object.

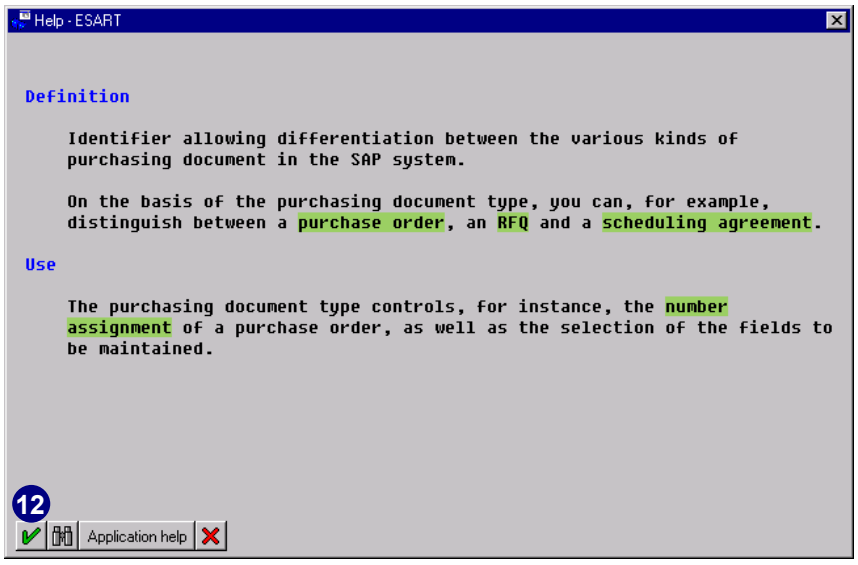
10. Choose *Continue*.



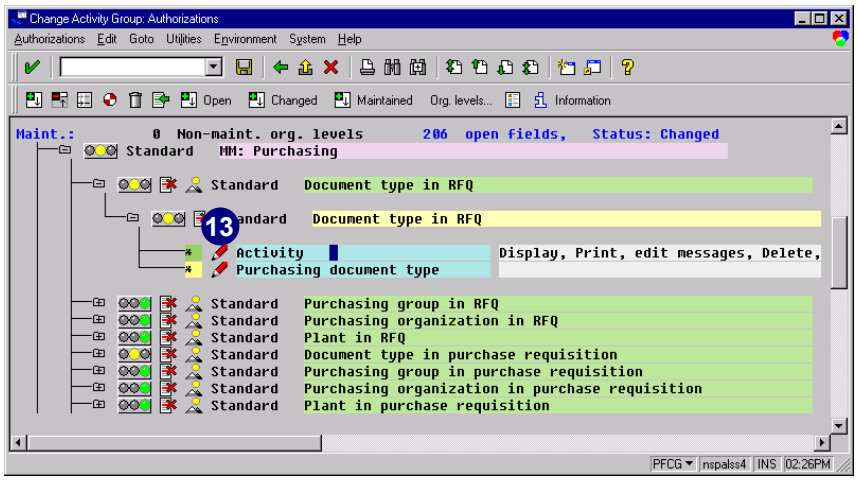
11. Double-click on the authorization field text to see its documentation (for example, *Purchasing document type*).



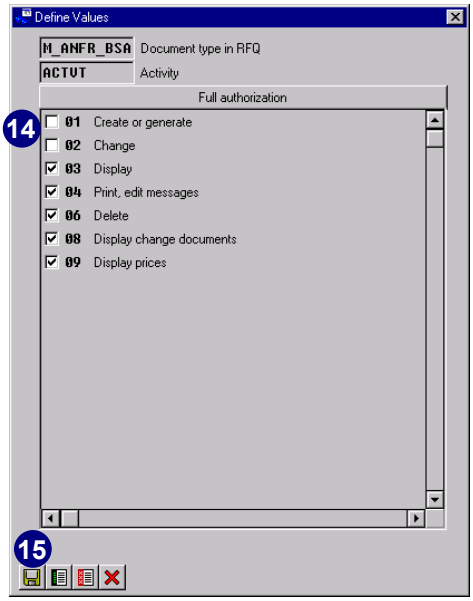
12. Choose *Continue*.



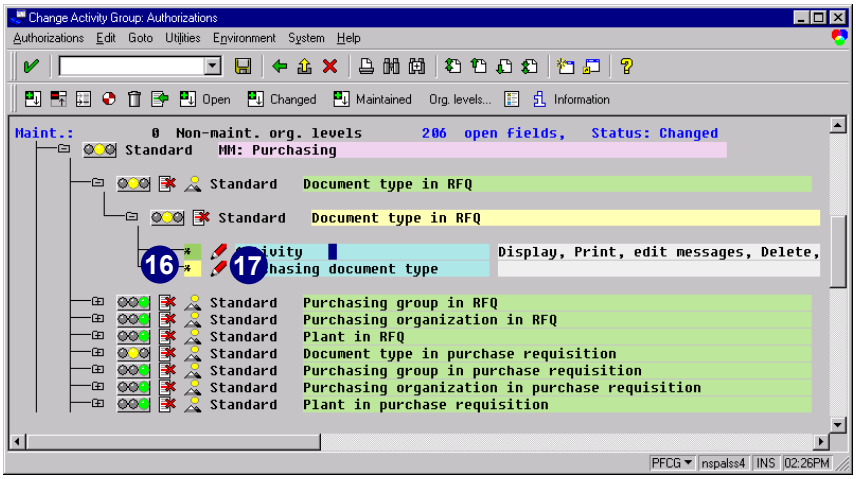
13. To check which values are automatically maintained by the R/3 System, choose *Change* for the activity authorization field (for example, *Activity*).



14. Based on your selection of transactions from the activity group, the *Define Values* dialog box displays the activities that were preselected by the R/3 System for this authorization field.
15. Choose *Transfer* to save your selection.



Now that you know everything about this authorization object and its fields, you can maintain the missing value for the open field.

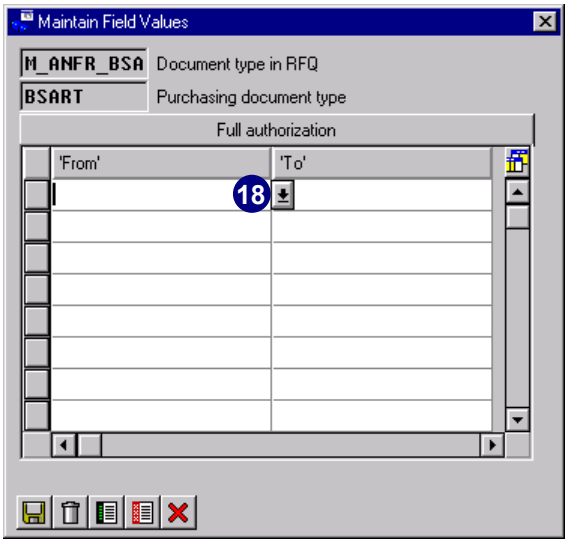


To maintain a missing value for an authorization field, you can either perform step 16 or 17:

16. To allow complete authorization for this field, click on the highlighted asterisk (*).
17. To maintain the field, choose *Change*.

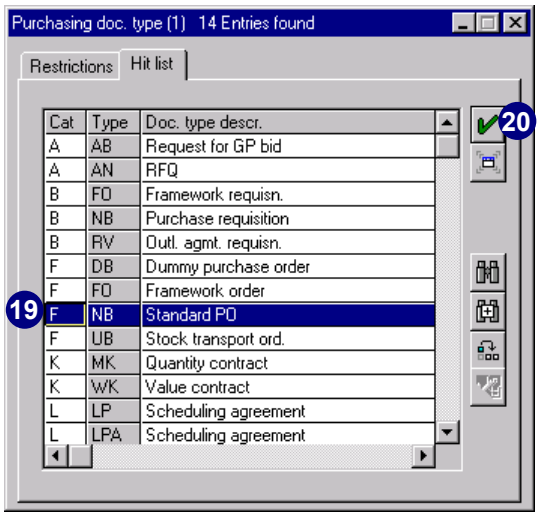
    In this example, we chose *Change*.

18. In the *Maintain Field Values* dialog box, choose *possible entries*.

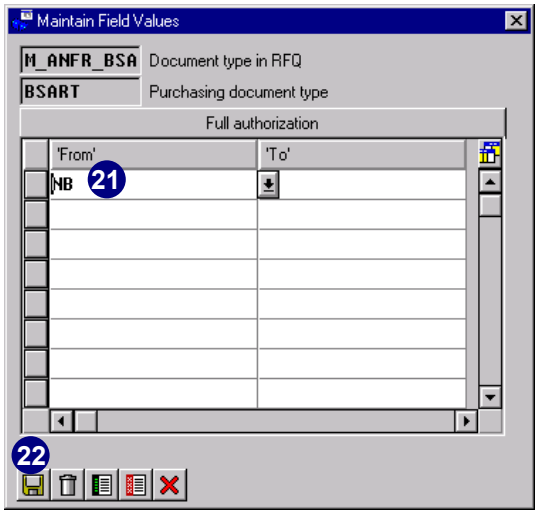


Rather than entering an interval, enter the necessary values in the *'From'* column.

19. Position the cursor and mark the desired entry in the value list.
20. Choose *Copy*.

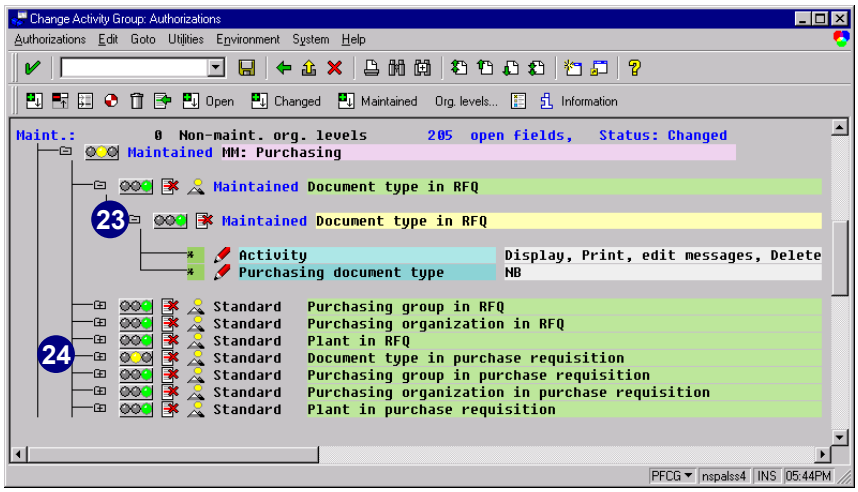


21. The selected value is automatically transferred to the correct field. (You may enter more single values or a value range.)
22. Choose *Transfer*.



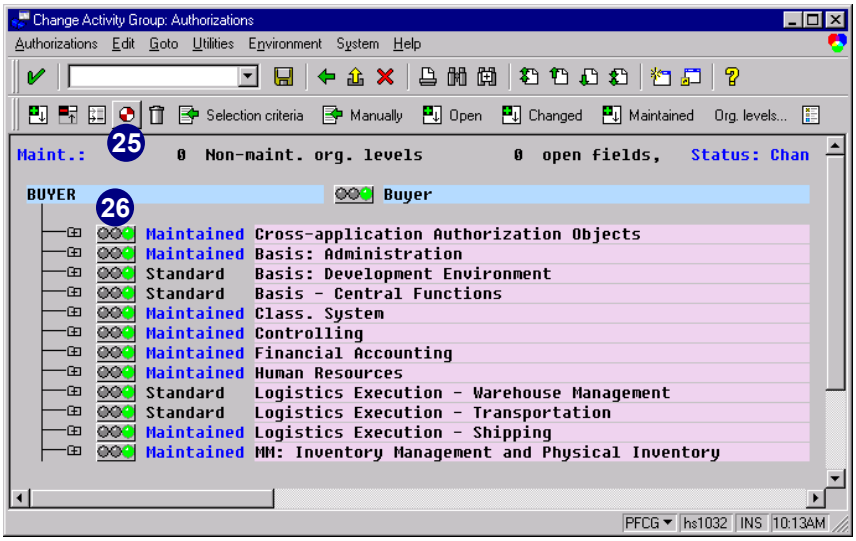
Rather than entering an interval, enter the necessary values in the *'From'* column. You can make additional entries in different rows.

23. After maintaining the missing value, the light for this authorization changes from yellow to green.
24. Check the tree for other missing values (yellow lights) in authorization fields and add values as necessary.



Remember to maintain each open authorization field with a suitable value. For some authorizations, enter a suitable value in *Authorization group*. If you are not sure of a suitable value, use the asterisk (*) to assign overall authorization for unmaintained fields. Remember that you can always change values later.

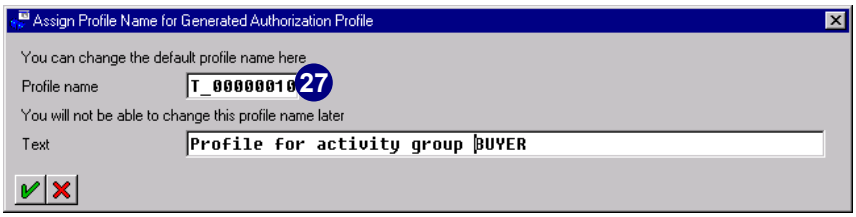
25. After maintaining the last open authorization field with the correct value, you should only see green lights in the tree.
26. Choose *Generate*.



The system then generates an authorization for each authorization in the tree and an authorization profile for the activity group that applies to the entire tree.

27. The *Assign Profile Name for Generated Authorization Profile* dialog box appears. The system suggests *T_<internal number>* as the default profile name.

    The short profile name cannot be changed later. However, the long text for the profile can be changed at any time.



Naming Conventions for Authorization Profiles and Authorizations Generated with the PG

When you save your changes, you are prompted to enter a profile name. However, only the first 10 characters (the profile torso) can be freely assigned. The number of profiles generated depends on the number of authorizations in each activity group. A maximum of approximately 150 authorizations can fit into a profile. If there are more than 150 authorizations, an additional profile is generated. It has the same 10-character torso as the profile name, and the last two digits are used as a counter.

To avoid conflicts between customer-defined and SAP-supplied profiles, do not use any name with an underscore (_) in the second position. SAP places no other restrictions on the naming of authorization profiles (refer also to OSS note *16466*). If your company has its own naming

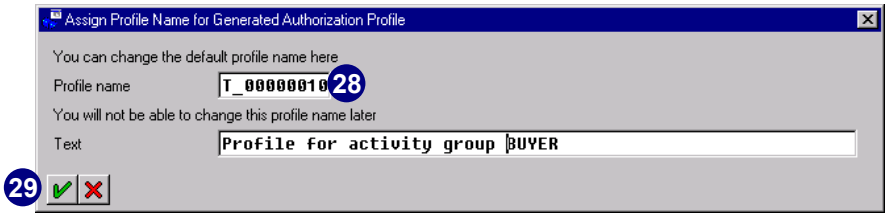
conventions, you may overwrite proposed names.

The names of the authorizations are also derived from the profile torso. The last two digits are used as a counter when more than one authorization is required for an object. Depending on the authorization profile name, the technical names for authorizations are then named as follows:

- Begin with a *T-*
- Comprise an internal number
- End with a two-digit number between *00* and *99*

Sample authorization name: T-5000001900.

28. Rename the authorization *Profile name* with your own naming convention.
29. Choose *Execute*.



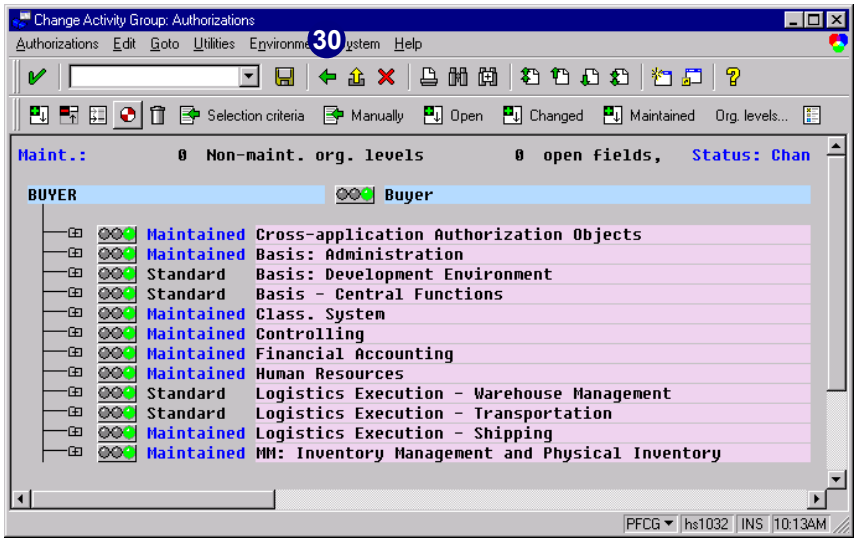
The authorization object *S_USER_PRO* is checked during authorization maintenance. The object is defined with the following fields: *Authorization profile* and *Activity*. In *Authorization profile*, enter the authorization profiles that an authorization administrator can maintain or that user administrators can assign to their users. In *Activity*, you can limit what the administrator is allowed to do.

If you want to set up an authorization administrator who can maintain only certain profiles, set up your own naming convention.

Congratulations. You have just generated the authorization profiles.

30. To exit transaction *PFCG*, choose *Back* three times, or to find out how many profiles were generated, continue with the next section.

    To assign the activity group to an R/3 user or a position now, please see chapter 7.



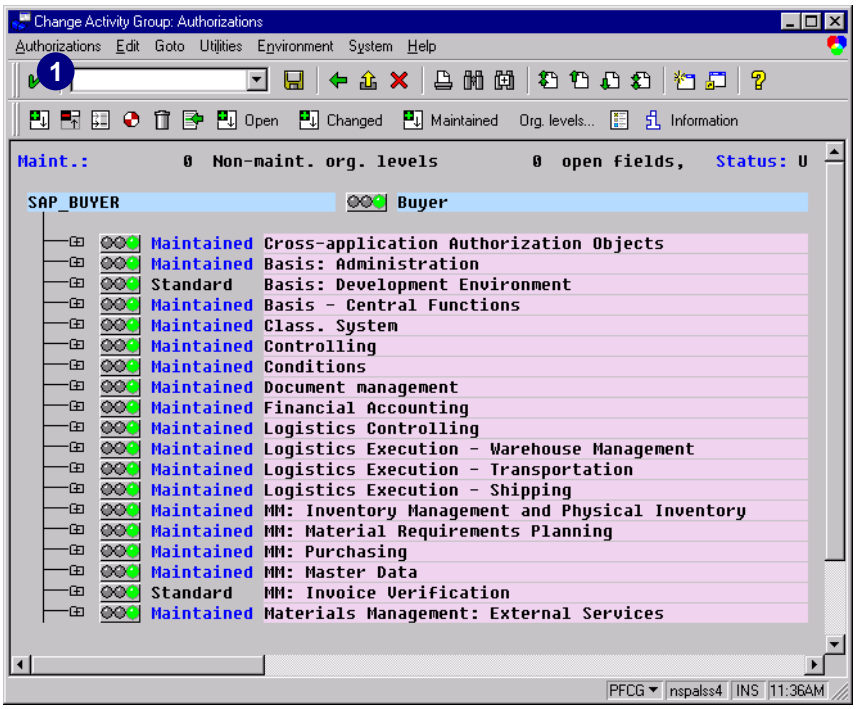
Displaying an Overview of Generated Profiles

After successfully generating the authorization profiles, to find out how many profiles were generated, you have to know the number of authorizations in each activity group. A maximum of approximately 150 authorizations fit into a profile. If there are more than 150 authorizations, an additional profile is generated. It has the same 10-character torso as the profile name, with the last two digits used as a counter.

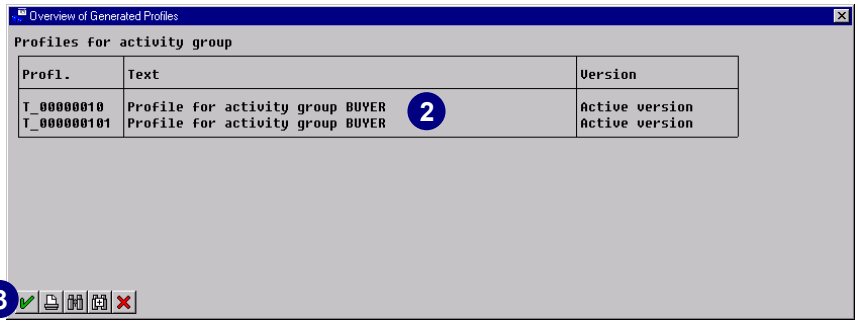
If an activity group is changed so that one profile becomes two or more, the additional profiles are automatically assigned to all the original profile's users. The user master of this user is automatically updated.

Start from the *Change Activity Group: Authorizations* screen in transaction *PFCG*.

1. Choose *Authorizations* → *Profile overview*.

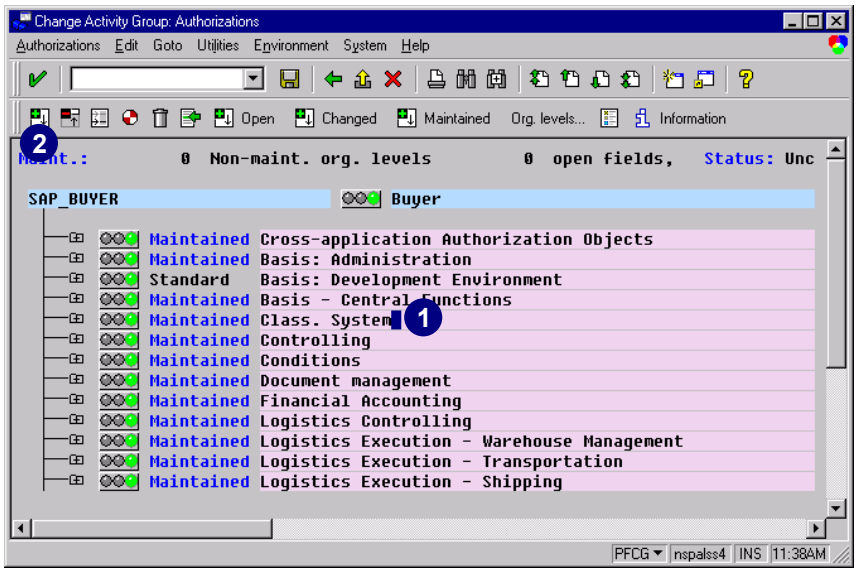


2. If the generated authorization profiles are already active, the dialog box provides an overview of their current status.
3. Choose *Continue*.

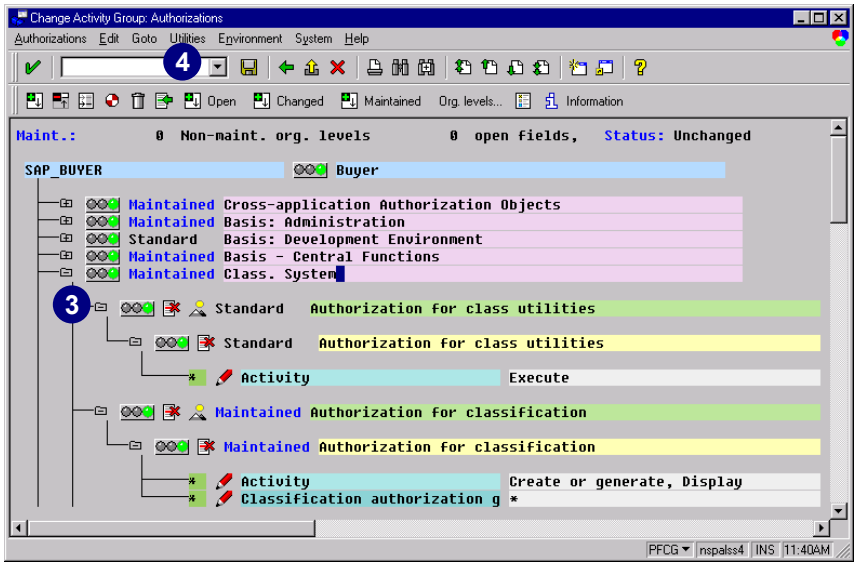


Displaying the Technical Names in the Tree List

1. Place the cursor on any object class entry in the tree (for example, *Class. System*).
2. Choose *Expand* or click the node at the beginning of the line.

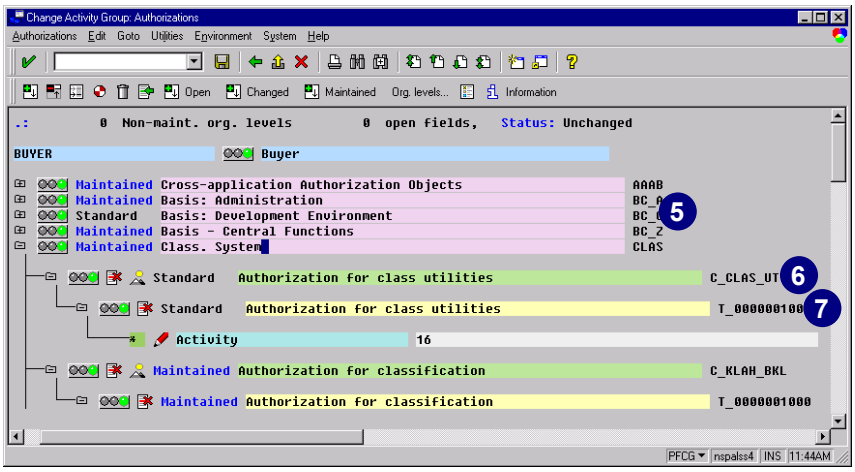


3. All the authorizations under the selected object class are now displayed.
4. To turn the technical names on, choose *Utilities* → *Technical names on*. To turn the technical names off, choose *Utilities* → *Technical names off*.



The names represent the:

5. Technical name of the object class
6. Technical name of the authorization object
7. Technical name of the authorization



Regenerating Authorization Profiles After Making Changes

When an activity group is changed, for example after you add another transaction in the menu, regenerate its authorization profiles with transaction *PFCG*. For the following example, we assume that you have saved changes to an activity group as described in chapter 4.

When you change an activity group, the status on the tab *Authorizations* indicates whether a profile is current or not. If the display shows a red or yellow light, the profile is not current. The status text on the screen explains why the profile is not current.

- Red light and text *Profile comparison required*

  The menu has been changed since the profile was last generated. Therefore the profile is not current and the authorization profiles needs to be regenerated. You may also have to maintain the authorization field values.

- Yellow light

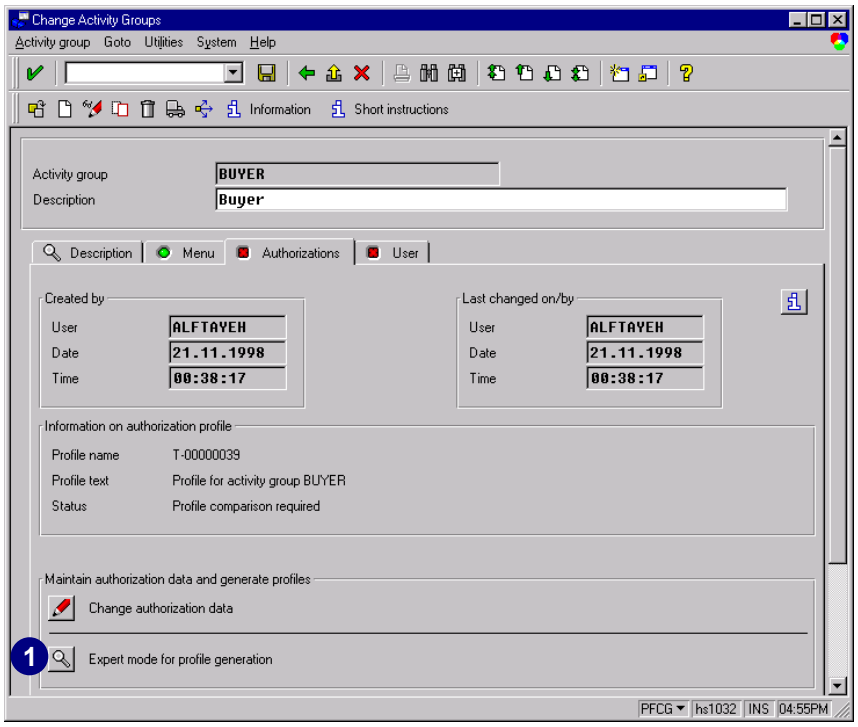
  The profile has been changed and saved since it was last generated and the profile is not current anymore and the authorization profile needs to be regenerated.

- If you are unsure whether an authorization profiles should be regenerated:

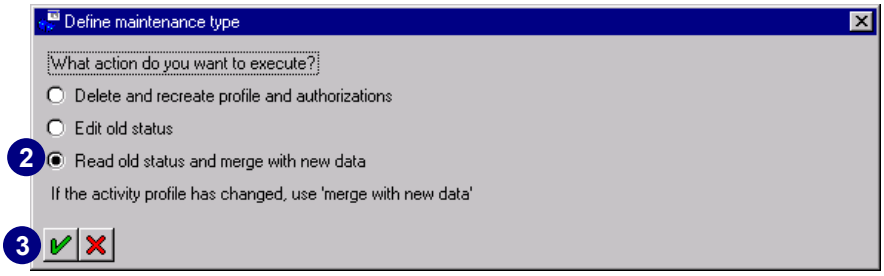
  1. Run transaction **SUPC**.
  2. Choose *Also act. grps to be adjusted.*
  3. Choose *Execute*.

The system generates a list of all activity groups with existing authorization data in the system. Activity groups in red need to be regenerated after post-maintaining any open authorization fields. Select one of these activity groups and choose *Maintain profile*. From **SUPC**, call transaction **PFCG**, and proceed as described below.

1. To regenerate the authorization profiles, choose *Expert mode for profile generation*.



2. Select *Read old status and merge with new data*.
3. Choose *Execute*.



Options on the *Define maintenance type* screen are described as follows:

- *Delete and recreate profile and authorizations*

  All authorizations are recreated. Values that have previously been maintained, changed, or entered manually are lost. Only the maintained values for organizational levels remain.

- *Edit old status*

  You can edit the authorization profile you previously maintained with its old values. It is not worth editing if the assignment of transactions to activity groups has changed.

- *Read old status and merge with new data* (default after a change in the menu)

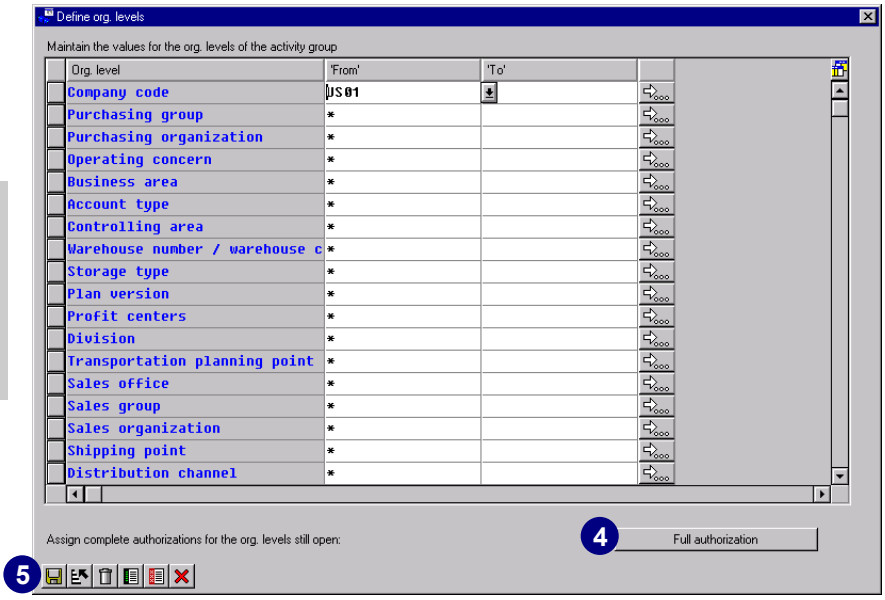
  The Profile Generator compares the old and the current data from the activity group. This choice is the best option if the activity group has changed. Unchanged data is marked as *Old*, new data as *New*.

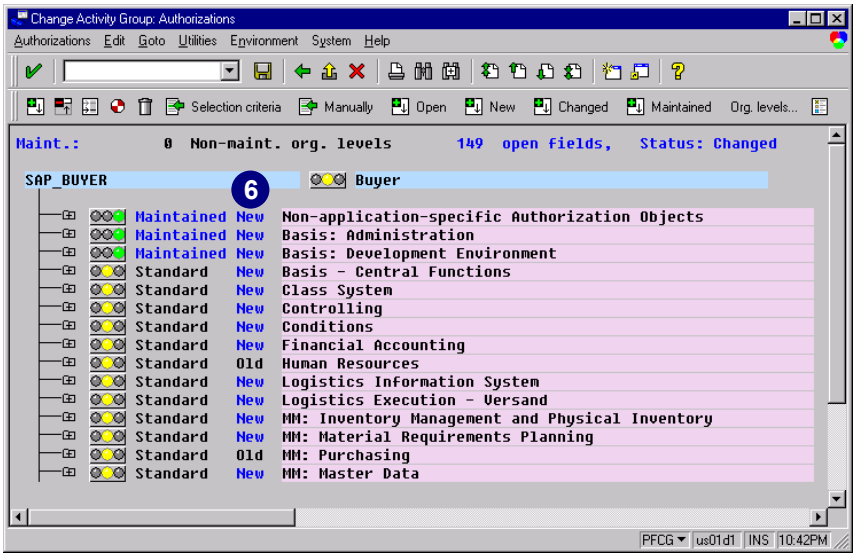
In the activity group *Buyer*, we added a few transactions to the previous selection. The previously maintained organizational levels are kept. When new organizational levels are added, they must be maintained.

4. Fill in the right information in the '*From*' field, or choose *Full authorization* for a complete authorization.
5. Choose *Transfer*.
6. As you can see, old authorizations are marked as *Old*, and new authorizations as *New*.

   To maintain all of the open authorization fields, please see *Generating the Authorization Profiles* on page 5–2.

   Before postmaintaining the open authorization fields, please read the information in the *Caution* textbox on the following page.

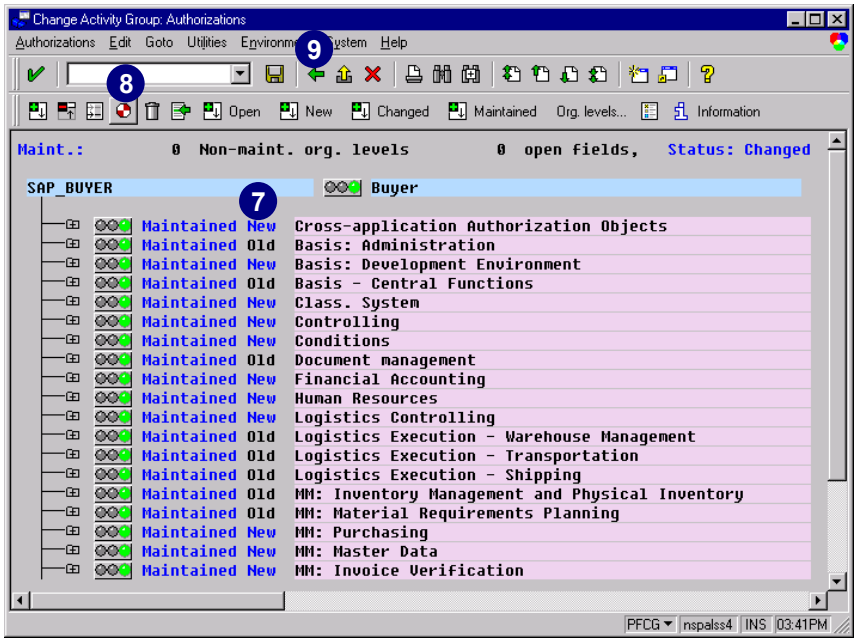




Please Keep the Following in Mind when Making the Post-Change Comparison:

- Previously maintained organizational levels are kept. If new organizational levels are added, you must maintain these levels.
- If authorizations within an authorization object have changed, you always need to execute the comparison manually. You must decide whether to keep the old modified data or whether to use the current data. Delete or maintain the authorizations you no longer require.
- Maintained authorizations are configured with the values you maintained for them. For example, for authorization group *0001*, certain activities (*Insert*, *Change*, and *Display*) and maintained authorizations for the activity group transactions are required (you maintained the value for authorization group). Change the activity group so that the following activities arise: *Change, Display,* and *Delete*. The value *0001* is copied for the authorization group for *Change* and *Display* (these activities were already maintained). The *Insert* option disappears. For the *Delete* activity, maintain the authorization group again, since this group was not maintained in the old profile's status.
- Wherever the *New* attribute appears, check if the new authorizations make sense (you can compare them manually with the old values).
- Manually entered authorizations are not deleted.
- The values for the authorization object *S_TCODE* are always automatically filled with the current transaction from the activity group, but have the attribute *Old*.

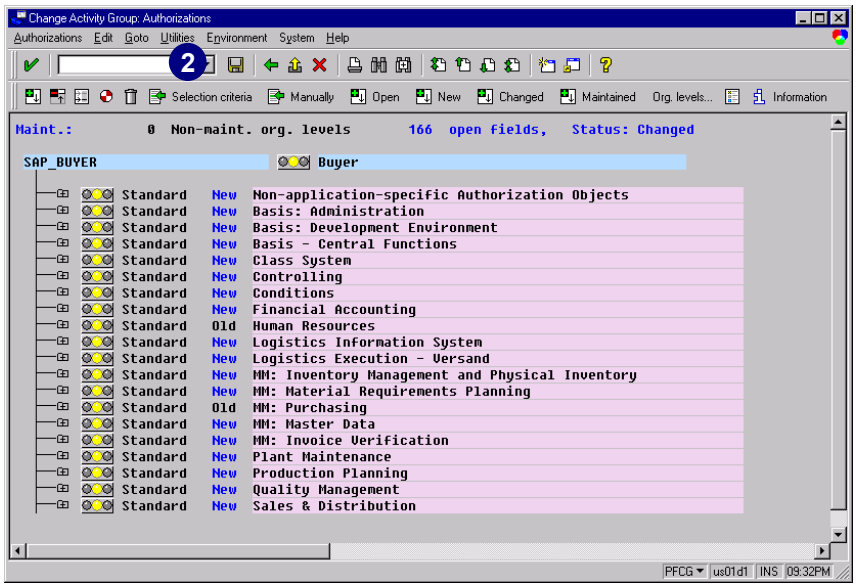
7. When you only see green lights in the tree, there are no more open authorization fields to maintain.
8. Choose *Generate* and the system will regenerate the existing authorization profiles.
9. You have finished regenerating the authorization profiles. Choose *Back* to get to the main screen.



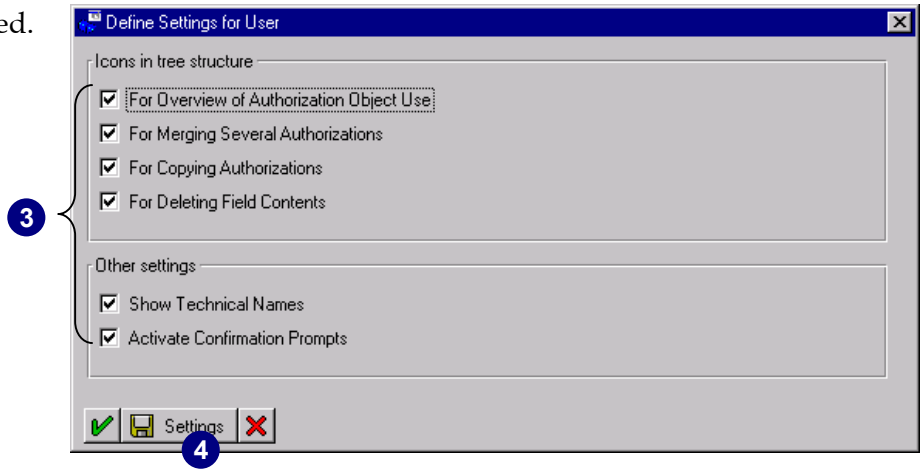
Elements and Symbols of the Hierarchy Display

In this section, we discuss all the graphical elements in the *Change Activity Group: Authorizations* window and how to work with them.

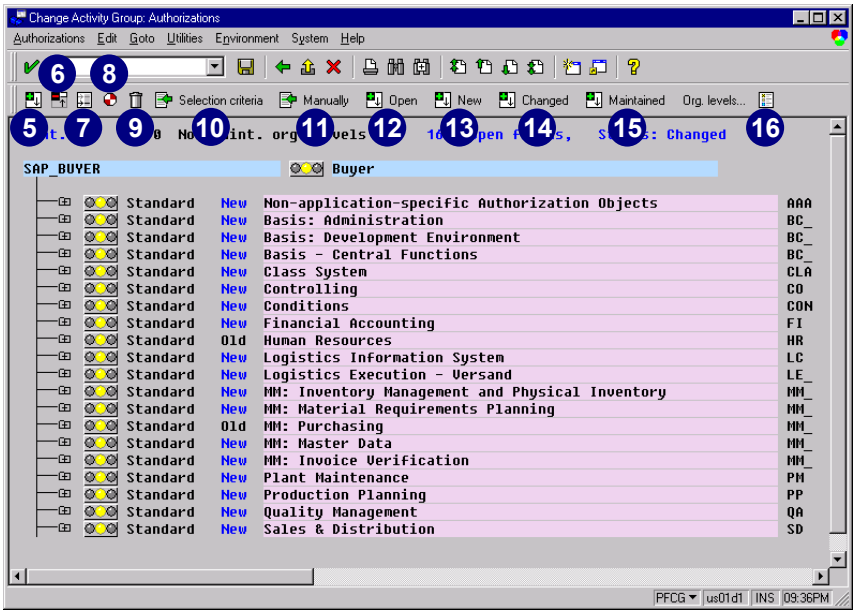
1. Open the *Change Activity Group: Authorizations* window.
2. Choose *Utilities* → *Settings*.



3. Make sure all options are selected.
4. Choose *Save Settings*.



Icons in the Standard Toolbar



5.  Expands the marked tree.

6.  Collapses the marked tree.

7.  Positions a selected line at the top of the list display.

8.  Generates the authorizations and the authorization profiles.

9.  Deletes all authorizations flagged as *Inactive* (see *Icons in the Hierarchy* on page 5–31).

10.  Manually inserts authorizations to an authorization object.

    See chapter 6 for more details.

11.  Manually inserts a new authorization object class.

12.  Displays all authorizations with open fields.

13.  Is visible only after you change an activity group and would like to update the authorization profile(s).

    Please see the section *Regenerating Authorization Profiles after Making Changes* on page 5–23.

14.  Expands object classes to display all authorizations modified manually after the authorization values were already maintained by the PG.

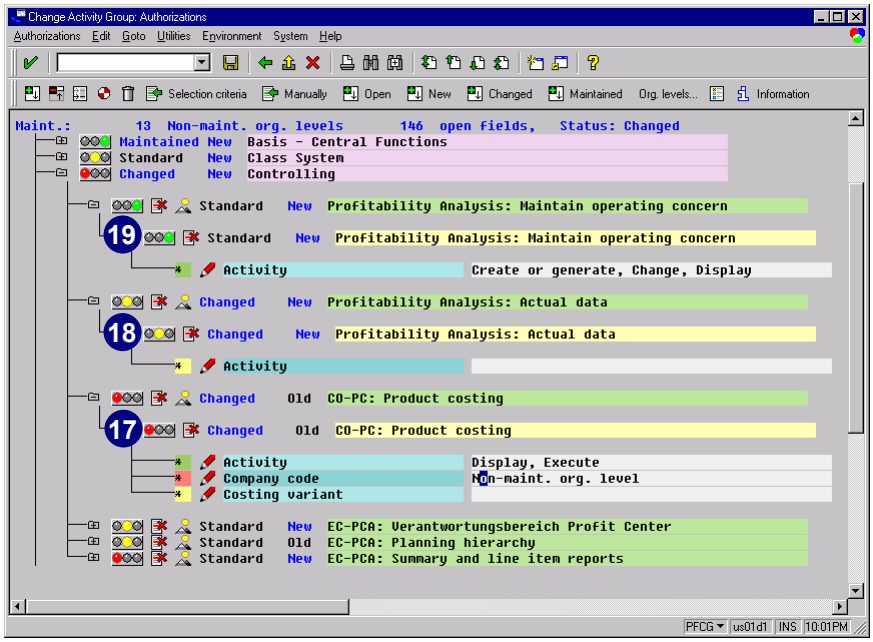
15. 

Expands object class to display all authorizations where you have post-maintained open field values.

16.  Displays the legend for colors and icons.

The Traffic Lights

The traffic lights indicate whether the values for the authorization fields have been maintained.



17. 

Red means that you have not yet maintained the organizational levels.

Click the red traffic light icon to assign complete authorization (*) to all of the open authorization fields (except for organizational levels) under this hierarchy.

18. 

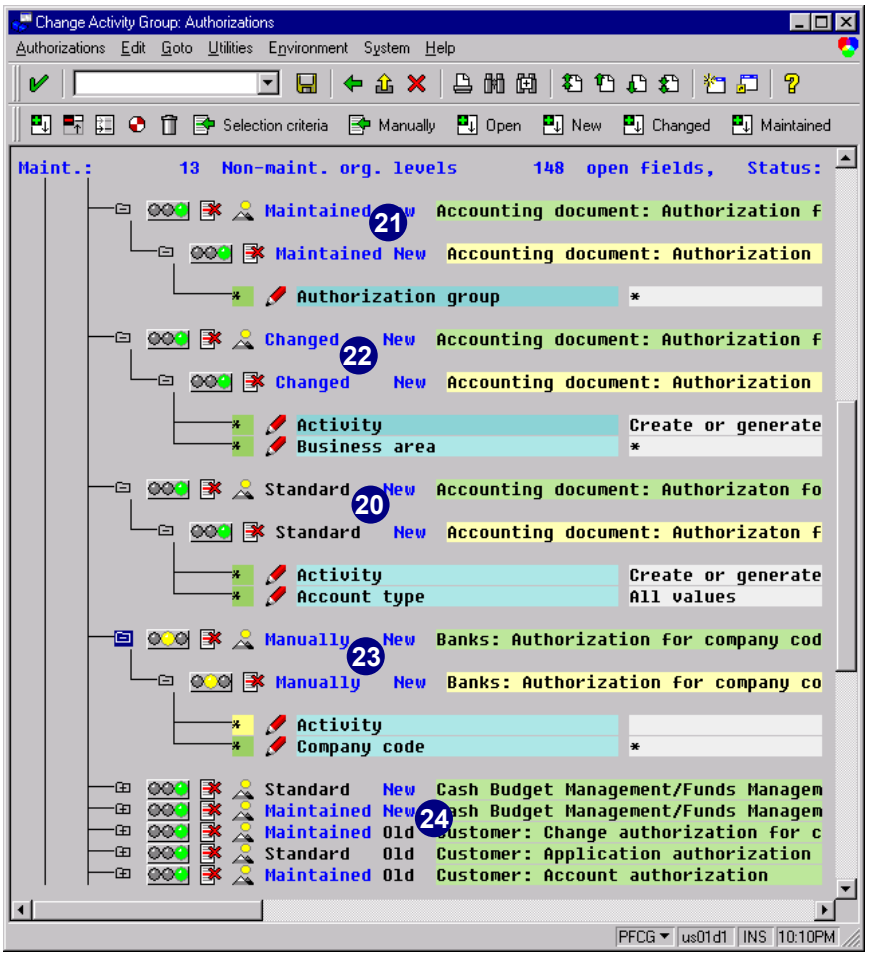
Yellow means that you have open authorization fields that are not organizational levels and have not been assigned any values.

Click the yellow traffic light icon to assign complete authorization (*) to all of the open authorization fields (except organizational levels) under this hierarchy.

19. 

Green means that the authorization fields have all been maintained.

Status Text for Authorizations



20. **Standard**

    In the subordinate hierarchy, all of the field values are unchanged and remain as delivered by SAP.

21. **Maintained**

    The subordinate hierarchy contains at least one field that was delivered blank by SAP and was subsequently maintained with your own value.

22. **Changed**

    The subordinate hierarchy contains a field that you changed after first maintaining it with an SAP-provided value. Even if you change a previously global organizational level, the status changes to *Modified* (unless you use the *Org. levels…* button).

23. **Manually**

    The subordinate hierarchy contains at least one authorization that you added with the *Insert manually (Selection criteria)* function.

24. **New** **Old**

    These attributes appear next to the other *Status text for authorization* after you changed an activity group and would like to update the authorization profiles. Please refer to the section *Regenerating Authorization Profiles After Making Changes* earlier in this chapter for additional information.

Icons in the Hierarchy


Choose this icon to:

25. **At the Authorization object level:**
Flag all authorizations underneath as `Inactive`.
Inactive authorization objects are ignored when profiles are generated.

26. **At the Authorization level:**
Flag only this authorization as `Inactive`.
Inactive authorizations are ignored when profiles are generated.

27. 
Choose this icon to reactivate a previously inactivated authorization.

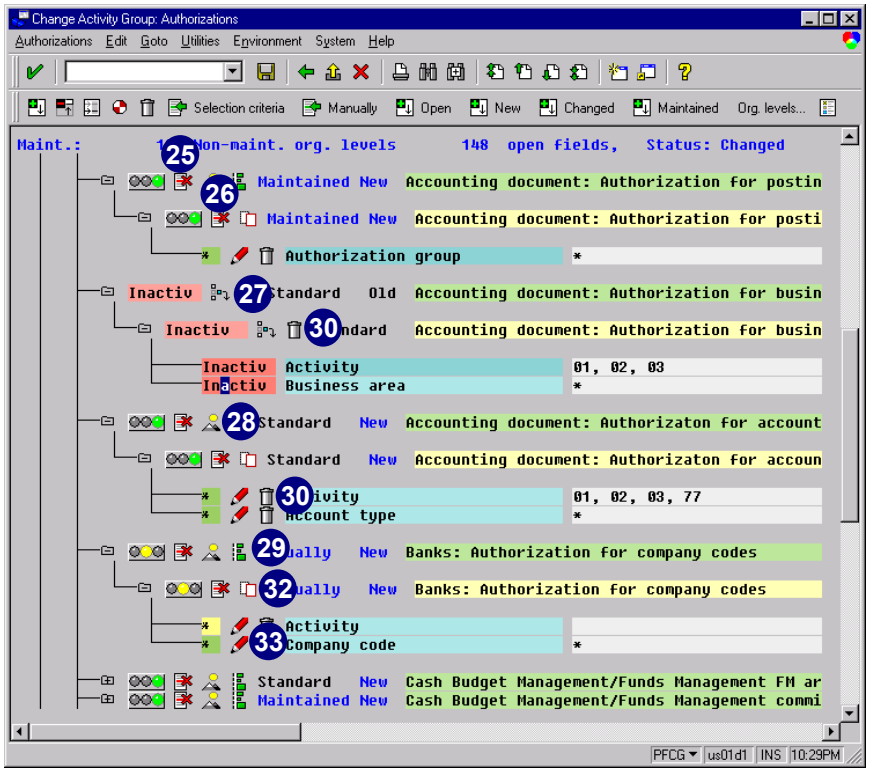
28. 
Choose this icon to display all the selected transactions that require this authorization object for the underlying activity group.

29. 
Choose this icon to summarize and merge authorizations for this authorization object. This step reduces the number of authorizations for the object.


Choose this icon to:

30. **At the Authorization field level:**
Delete the authorization field values and change the status of the authorization field.

31. **At the Authorization level:**
Delete the authorization only if it was previously deactivated.



32.  Choose this icon to copy the corresponding authorization.

33.  Choose this icon to maintain the field values for the corresponding selected authorization field.

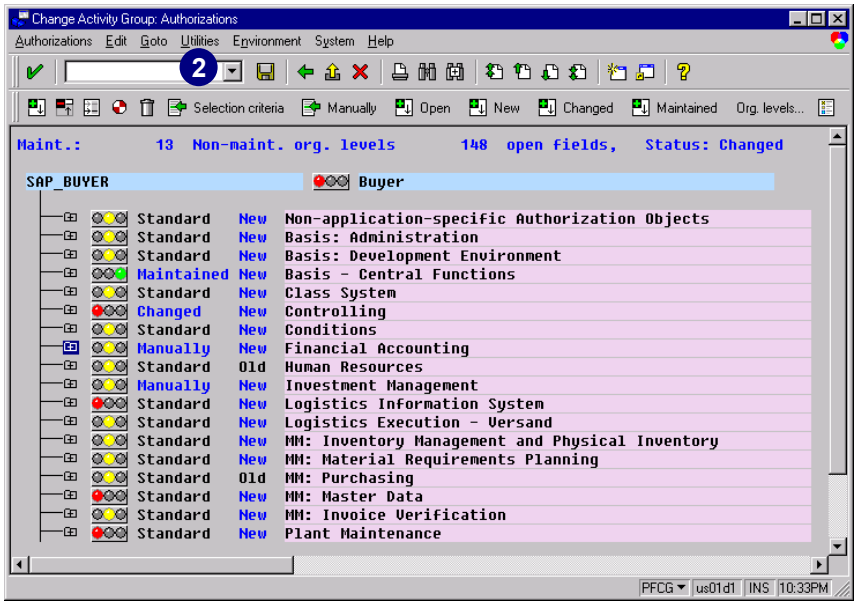
Using Utilities

There are two options to alter the automatically generated authorizations. These options are found in transaction *PFCG,* under the *Utilities* menu in the *Change Activity Group: Authorizations* screen.

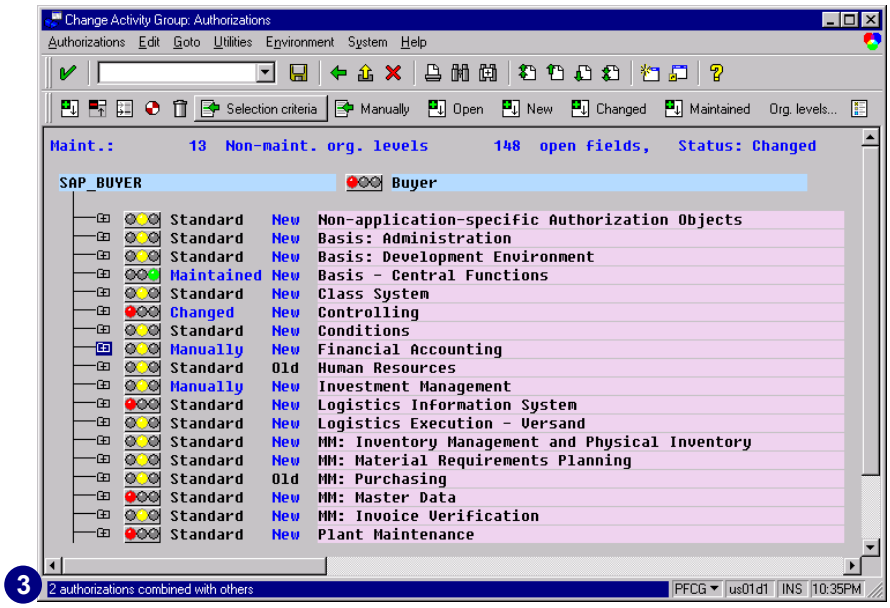
Merge Authorizations

If there are authorizations with identical authorization field content for an authorization object, the system automatically summarizes these authorizations. This step may result in fewer authorizations for an authorization object.

1. Start from the *Change Activity Group: Authorizations* screen in transaction *PFCG*.
2. Choose *Utilities* → *Merge authorizations*.



3. The system then automatically summarizes all possible authorizations and the result appears in the status bar.



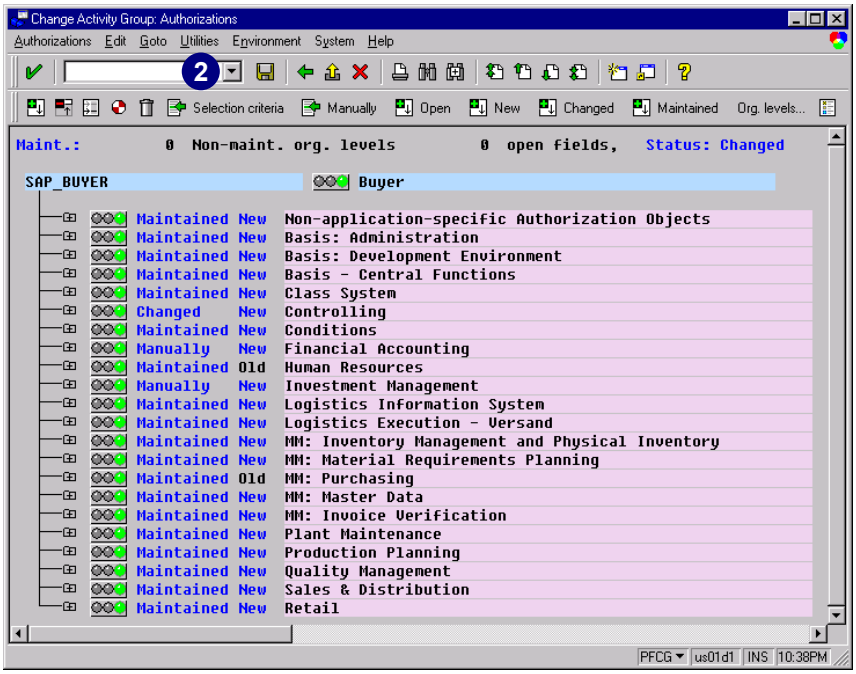
Reorganizing Technical Names of Authorizations

The technical name of an authorization within an authorization object is the name of the activity group and a two-digit number between 00 and 99.

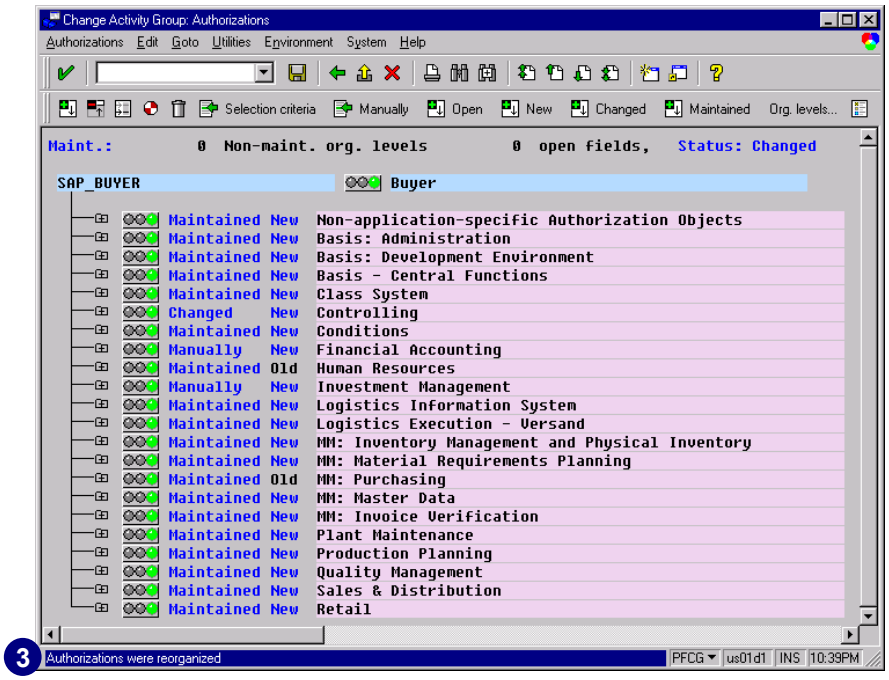
T-<internal number>nn, example: *T-5002995604*

If the authorization profiles changed as a result of changes in the appropriate activity group, reorganize the numbers to avoid number assignment problems. The following procedure restarts the number assignment from 00. Whenever you generate a new authorization profile, this reorganization is automatically taken into account.

1. Start from the *Change Activity Group: Authorization* screen.
2. Choose *Utilities* → *Reorganize*.



3. The system automatically reorganizes the final digits of the authorization's technical names and the result appears in the status bar (for example, *Authorizations were reorganized*).

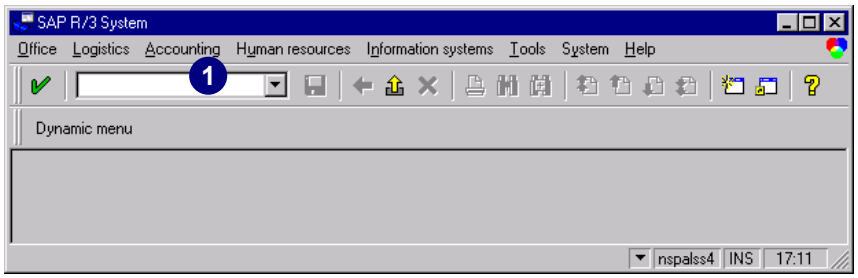


Customizing Authorizations

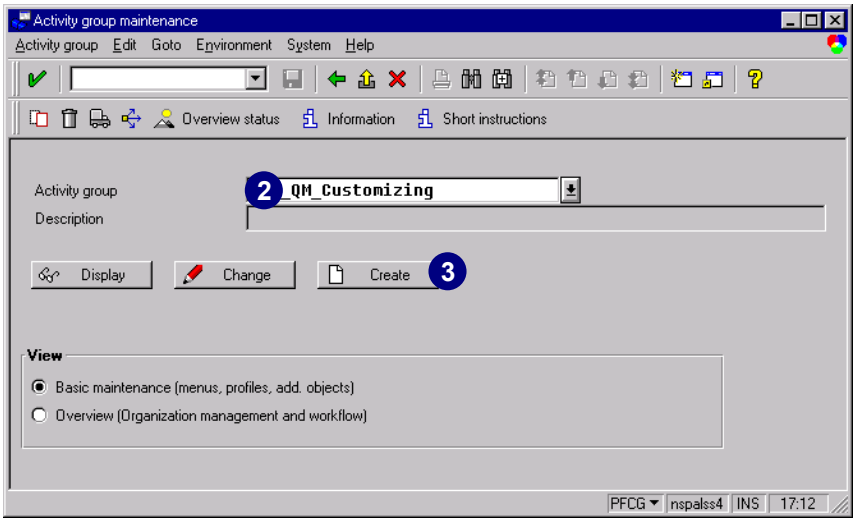
You can assign projects or views of the Implementation Guide (IMG) projects to an activity group. The aim of this assignment is to generate authorizations for and assign users to specific IMG activities. When you generate profiles, this also generates the authorization necessary to execute all activities in the assigned IMG projects or project views.

Assigning IMG Projects or Project Views to Activity Groups

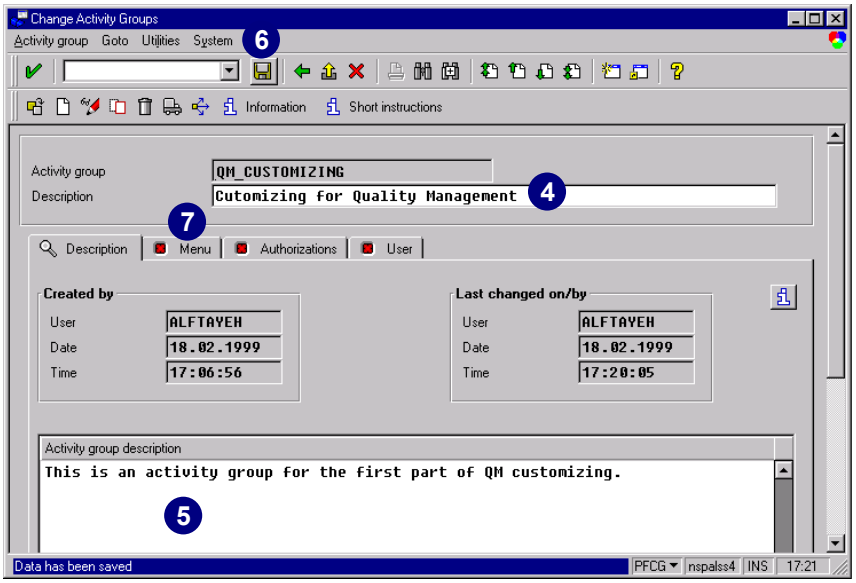
1. In the *Command* field, enter transaction **PFCG** and choose *Enter* (or choose *Tools* → *Administration* → *User maintenance* → *Activity groups*).



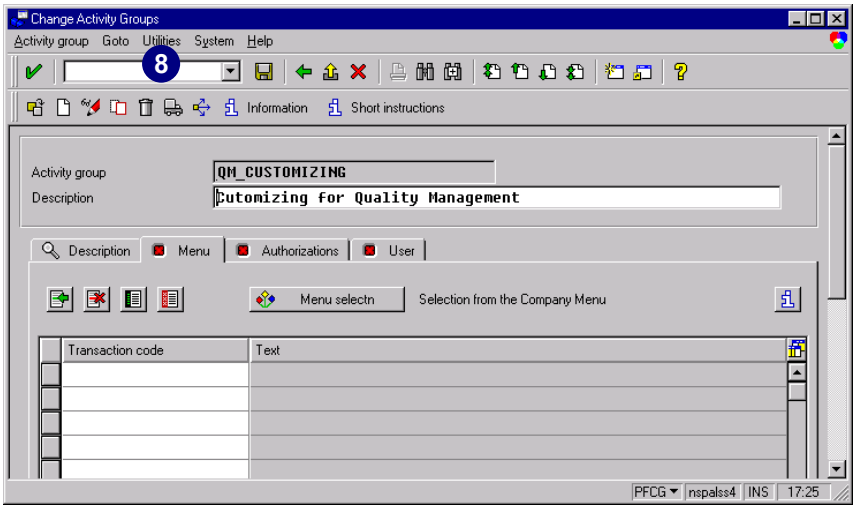
2. In the *Activity group* field, enter a name that describes your activity group the best.
3. Choose *Create*.



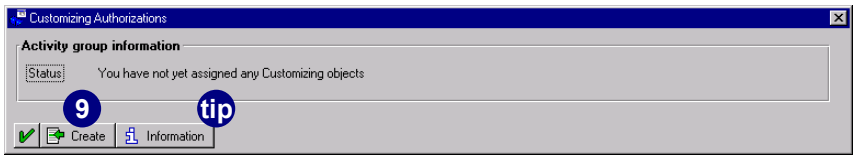
4. Enter a short description for your cutomizing activity group in the *description field*.
5. Optional you can enter a long text for the activity group.
6. Choose *Save*.
7. Choose the *Menu* tab.



8. Choose *Utilities* → *Cutomizing auth.*

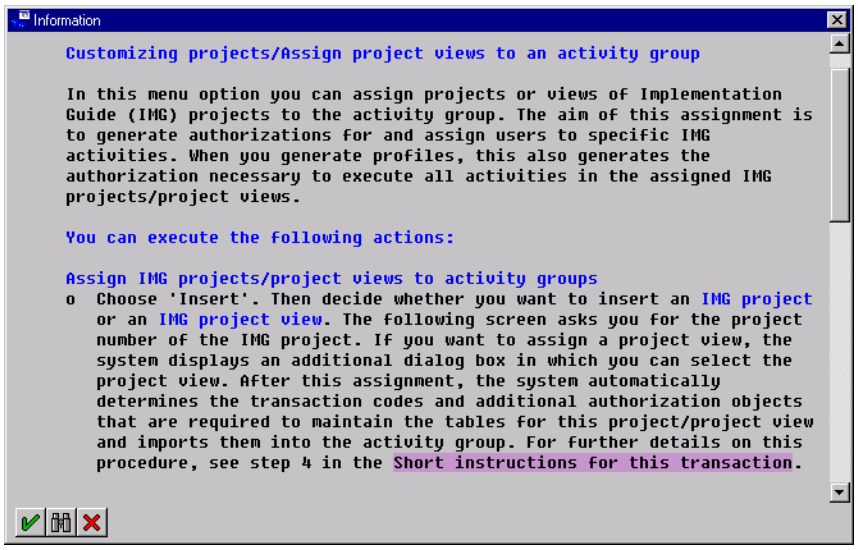


The system notifies that there are no customizing objects assigned to the activity group.



9. Choose *Create* to assign a customizing project or a customizing view to the activity group.

To get a online information on how to assign customizing projects/views to the activity group choose *Information*.

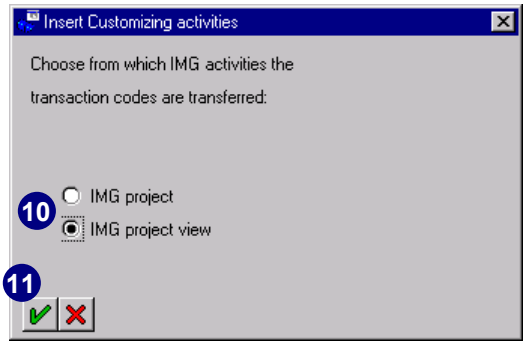


10. Choose *IMG project* or *IMG project view*.

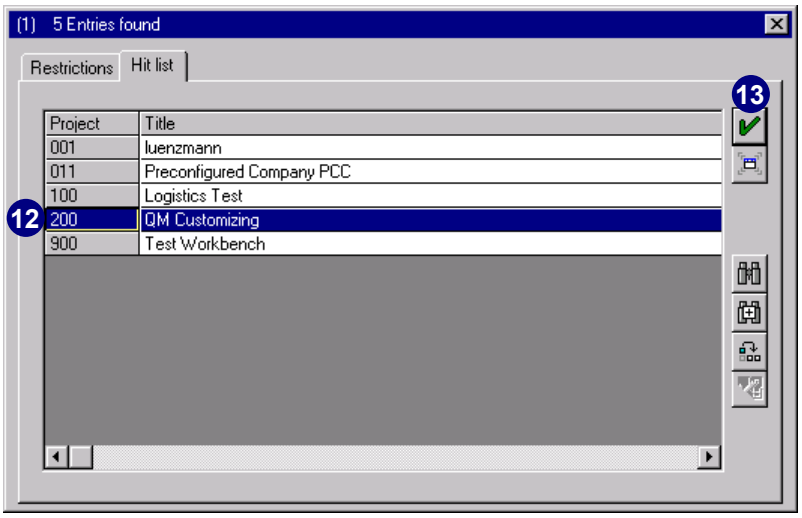
    If you select *IMG project view* you need to select the appropriate view on a later screen too.

    We chose *IMG project* view as an example.

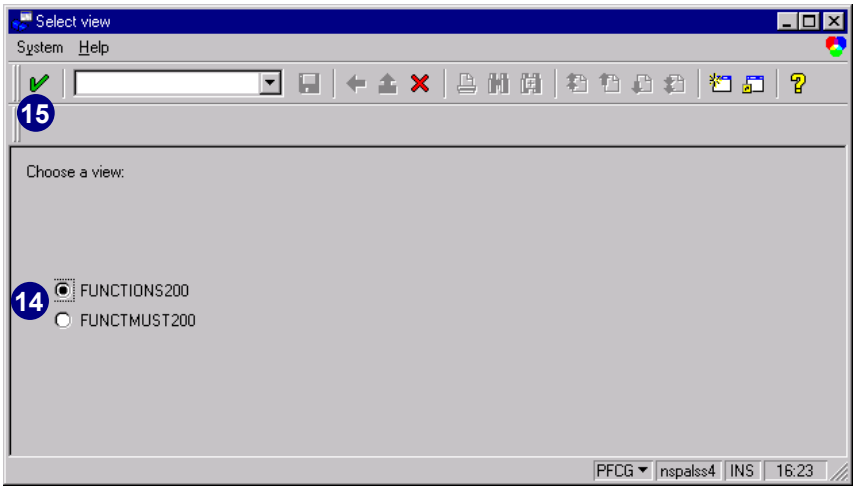
11. Choose *Continue*.



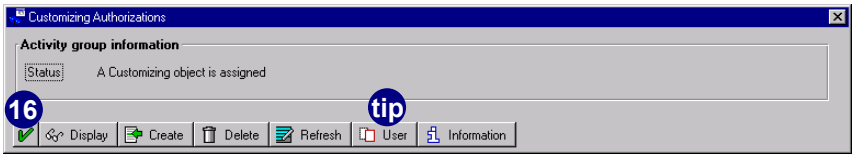
12. Choose a project.
13. Choose *Copy*.



14. Choose a Customizing view.
15. Choose *Continue*.



16. Choose *Continue*.



Transfer users from IMG projects.

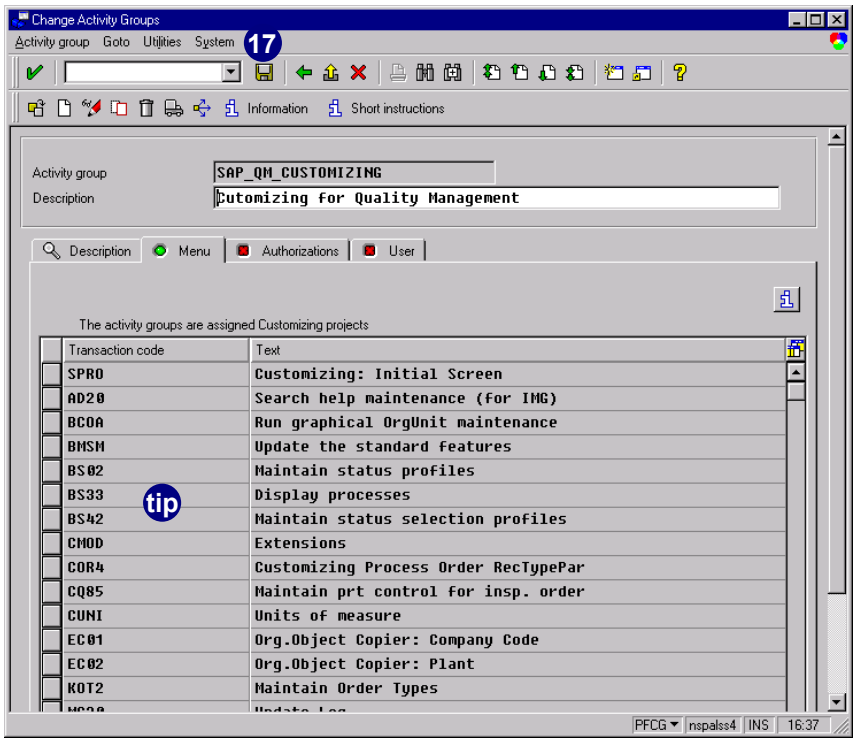
If you have assigned users (resources) to IMG projects in the project administration, you can transfer these to the activity group. To do this, choose *User*. This copies the users from the assigned project.

Note that you must call this function again each time you make changes in the IMG project administration.

The system automatically determined the transaction codes and additional authorization objects that were required to maintain the tables for this IMG project and project view, and imported them into the activity group.

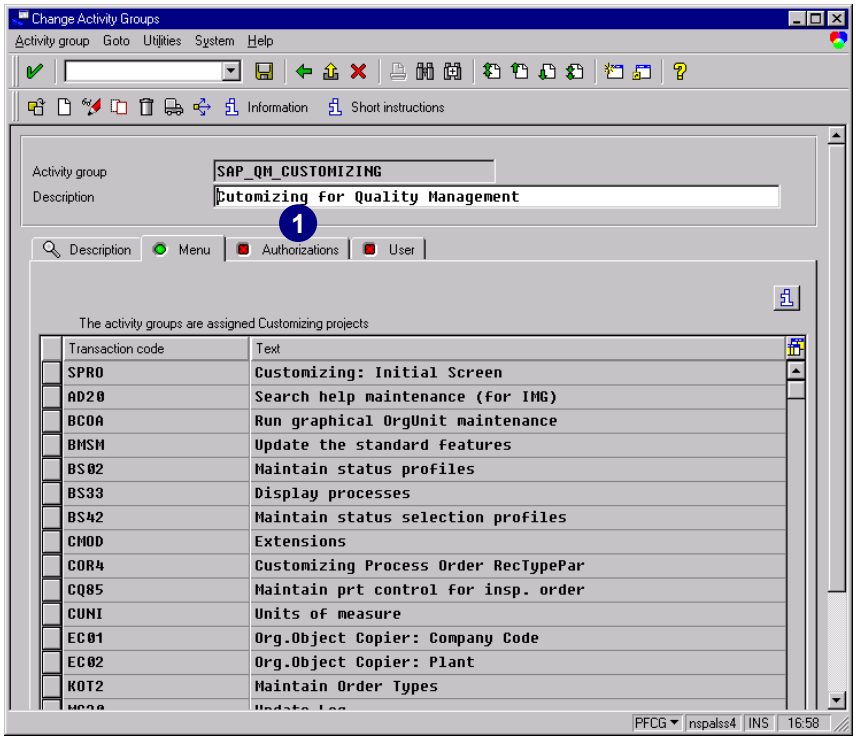
17. Choose *Save*.

You cannot manually assign any transactions to this activity group nor can you select any from the menu tree. Note that the screen changed gray and the buttons for inserting transactions and for the menu tree vanished.

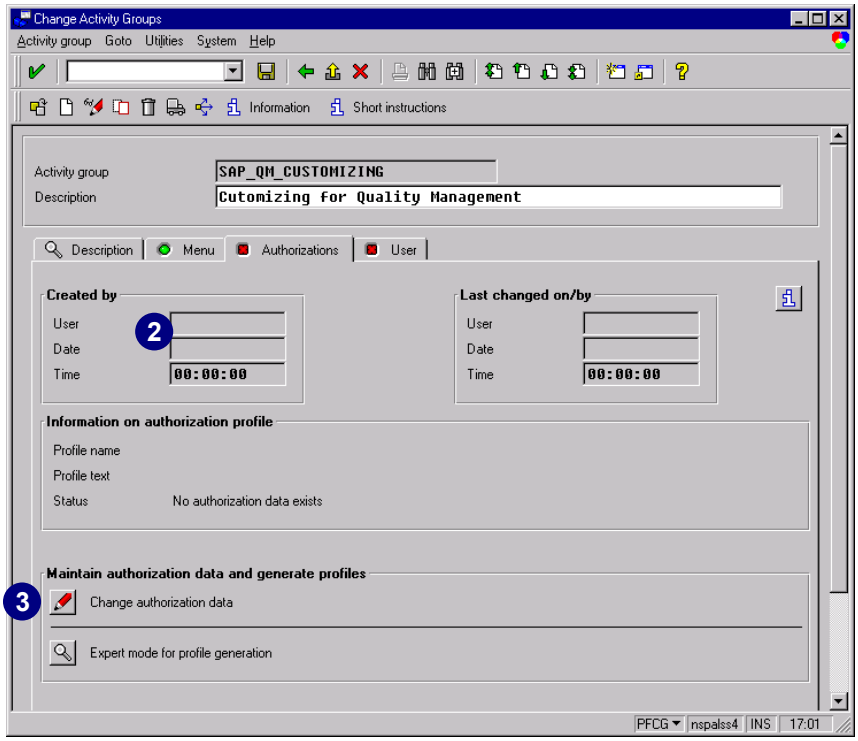


Maintaining and Updating Customizing Authorizations

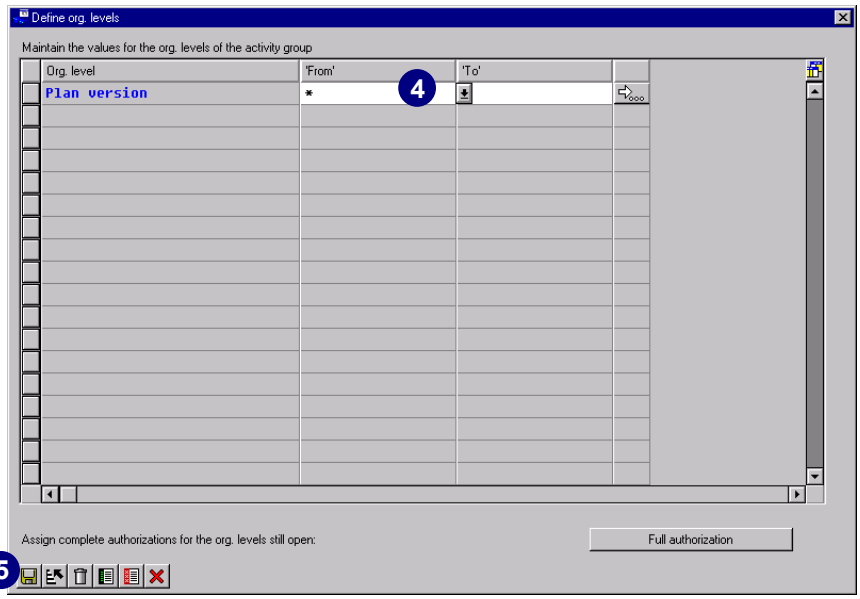
1. On the *Change Activity Group* screen for your customizing authorizations, choose the *Authorizations* tab.



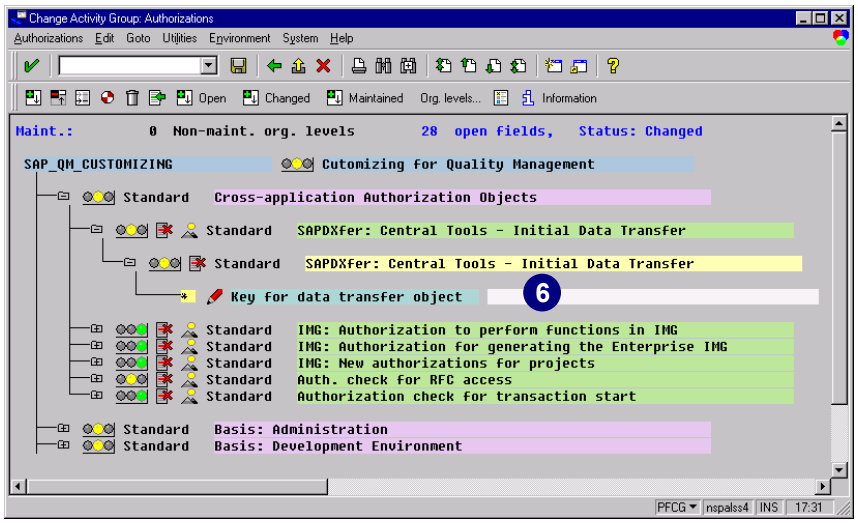
2. The first time you enter authorization data to a customizing activity group the fields are empty as shown.
3. Choose *Change authorization data.*



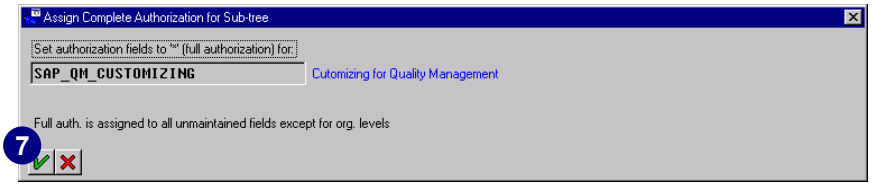
4. Enter the appropriate *Plan version* for the organizational level. We selected *Full authorization*. (In our example, the system requests the *Plan version;* the system could request a different *Org. level*, or nothing at all).
5. Choose *Transfer.*



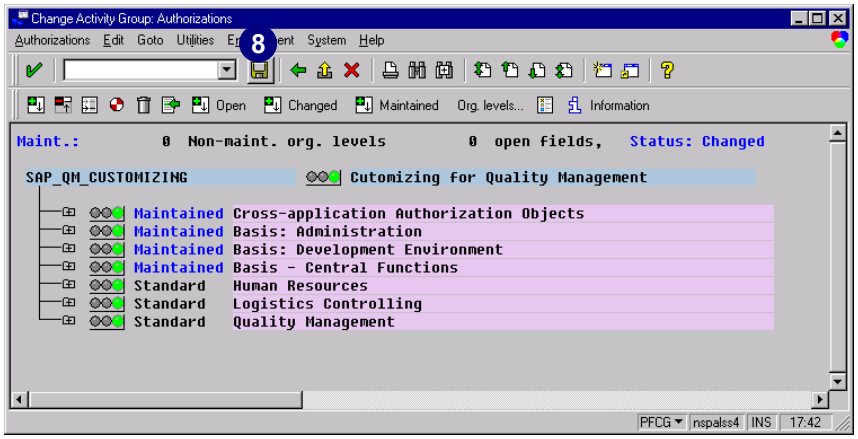
6. To maintain the authorization data and an explanation of all icons see *Postediting Authorizations and Organizational Levels* in this chapter on page 5–10. (In our example, we chose full authorization by double-clicking on the upper most yellow traffic light.)



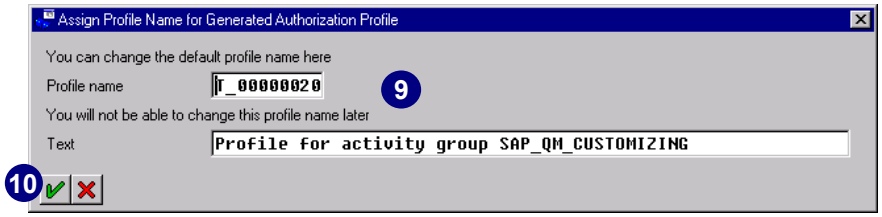
7. Choose *Execute*.



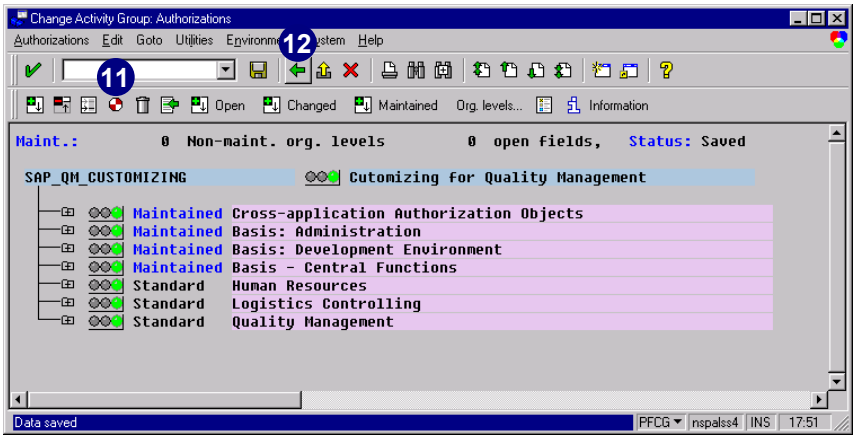
8. Choose *Save*.



9. You can change the *Profile name*.
10. Choose *Execute*.

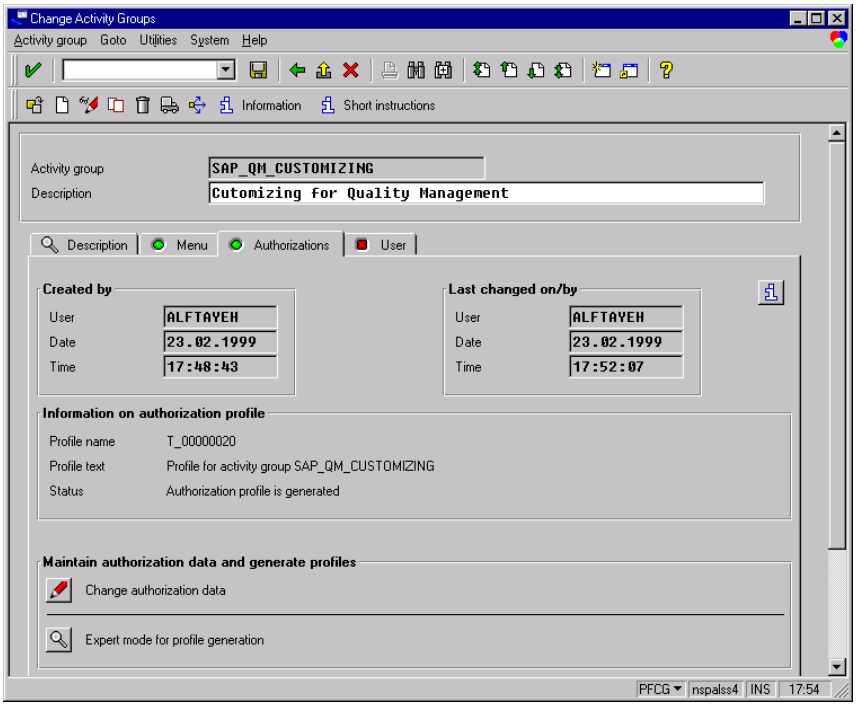


11. Choose *Generate*.
12. Choose *Back*.



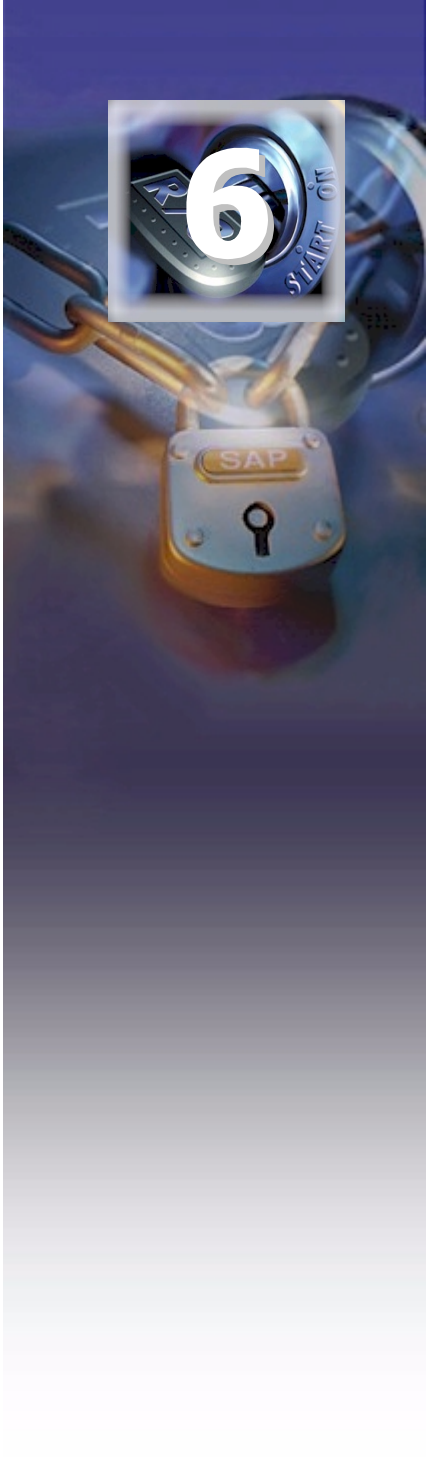
You have now created a customizing activity group and assigned authorization data to it.

If you have not assigned users to the customizing project or you have not transfered those users to the activity group, you still need to do so. Please see chapter 8 on how to assign users.



If the company menu or the IMG project have changed, you should regenerate the authorization data for this activity group. The first step is to choose *Refresh*. This action recalculates the transaction codes. You must then regenerate the authorization profiles for the activity group.

To assign users to the customizing activity group, you can transfer the users that are already assigned to the customizing project or project view and you can also assign any other user to this customizing activity group. See chapter 8, the section *Transferring Users from an IMG Project to an Activity Group* for details.



Chapter 6: Special Cases

Contents

Overview

In this chapter, we introduce a few special Profile Generator (PG) situations that may arise during the security implementation of your project. Please read this chapter before addressing problems which may arise in relation to the PG.

Manually Postmaintaining Authorizations

Although the PG generates authorization profiles, it may be necessary to manually include an authorization or adjust a field value. This process of maintaining the profile generator's suggested authorizations as derived from the transactions selected for an activity group is called **postmaintaining authorizations**. The following is a list of different situations where it may be necessary to manually include authorizations:

- Even though the PG assigned a particular profile, the user is mistakenly unauthorized to use the corresponding transaction and receives the error message: "You are not authorized…"

  By calling transaction *SU53*, the user can see the last authorization check that failed. Please see chapter 13 to learn how to use transaction *SU53*. If an authorization object is checked within the corresponding transaction and the respective authorization is not correctly entered in the generated profile, using transaction *SU24*, you can change the check indicator for this particular authorization object in the appropriate transaction. Please see chapter 2**,** *Reducing the Scope of Authority Checks in R/3 (SU24)* to learn how to use transaction *SU24*.
- The generated profile does not assign any general rights to the user.

  Basic authorizations are so general, it is not worth including them in each individual transaction. The system does not check whether an authorization is needed for an existing transaction, but new authorizations are included without checking for existing ones. Although this sounds unusual, this method greatly improves system performance. The system provides the functionality to summarize authorizations for the same authorization object.
- Transaction *SU53* is protected by the object *S_TCODE* and cannot be selected from the company menu tree in *PFCG*.

  We recommend including the appropriate authorizations for transaction *SU53* in each authorization profile. These authorizations guarantee that, if users get the error message "You are not authorized…," "No authorization for…" or any message regarding an authorization problem, the help desk can more easily assist them.
- Most, but not all reports are not yet completely supported by the PG.
- Manual postmaintenance may be necessary in the parameter and variant transactions and during the upgrade.

- Adding authorizations in a profile that you created in accordance with the conventional transactions *SU02* and *SU03*.

Manually Including Authorizations

You may insert missing authorizations:

- Manually
- From a template
- From a profile
- By inserting complete authorizations

To assign general authorizations, choose one of the following options:

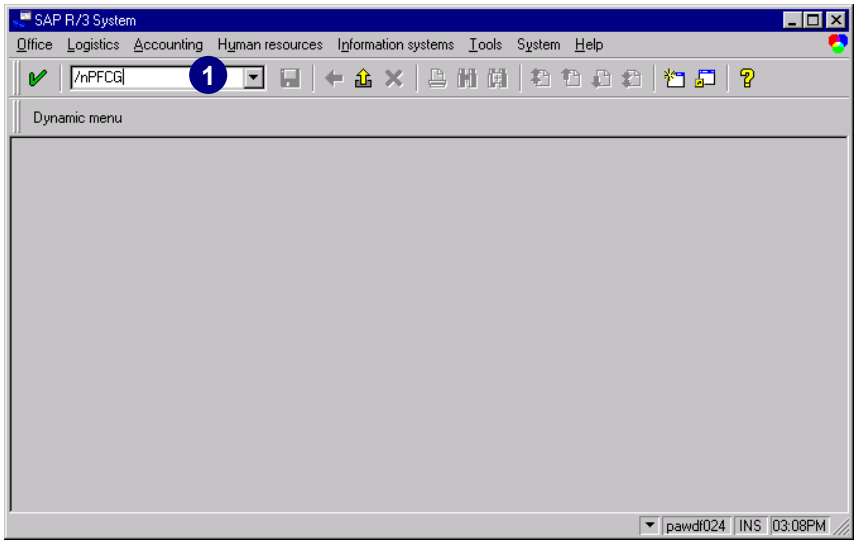
- Create a separate activity group containing only general authorizations (such as printing), and assign this activity group to all users. (This method works best if users will print from any or all printers; a generic printing authorization can be assigned.) Generate the authorization profiles for these activity groups and assign them to the users.
- Include the required objects in the activity group by using SAP templates or your own templates and by maintaining any missing field entries. (This method works best if users will be assigned to particular printers.)

Manually Inserting Authorizations

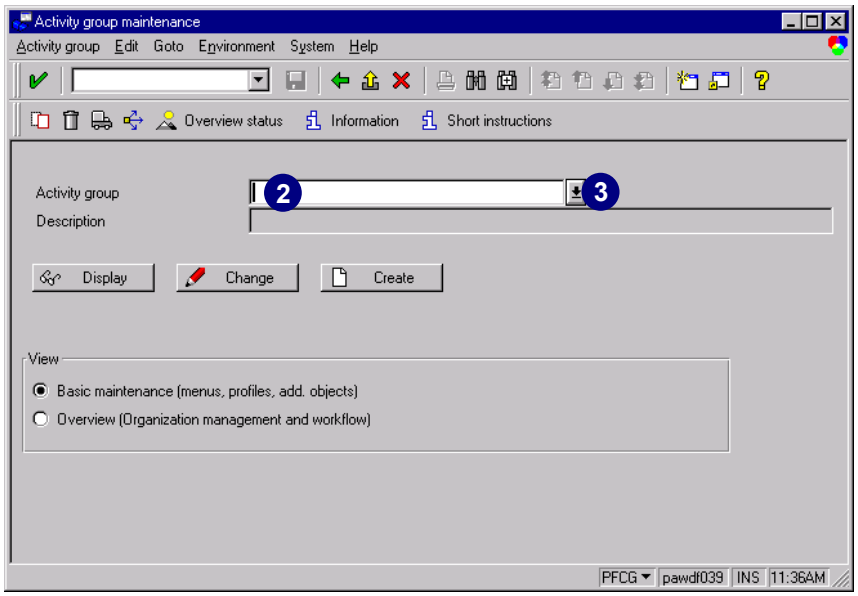
By calling up transaction *SU53*, you can clarify an authorization check your transaction is missing. *SU53* is only one of the manners to determine missing authorizations. Sometimes, traces are more useful because they are much more accurate and complete, especially when dealing with HR authorization problems. Identify the authorization object and the missing authorization field values. Then manually insert the missing authorization.

To manually insert authorizations:

1. In the *Command* field, enter transaction **PFCG** and choose *Enter* (or choose *Tools* → *Administration* → *User maintenance* → *Activity groups*).

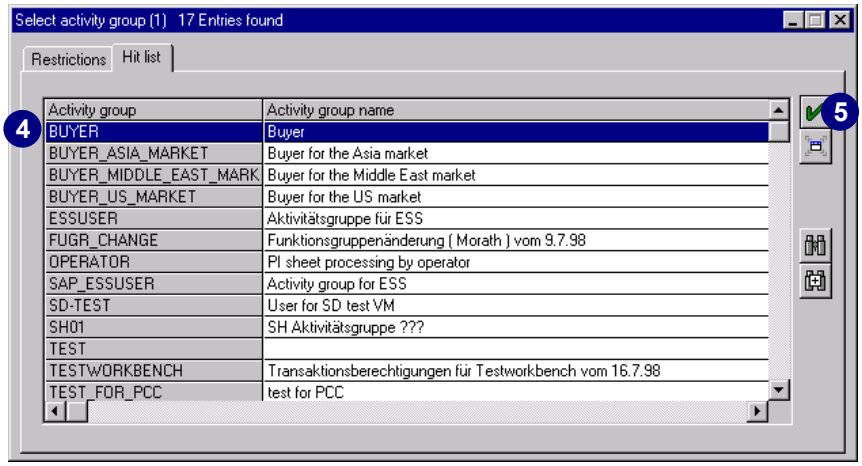


2. Place the cursor in the *Activity group* field.
3. Choose *possible entries*.

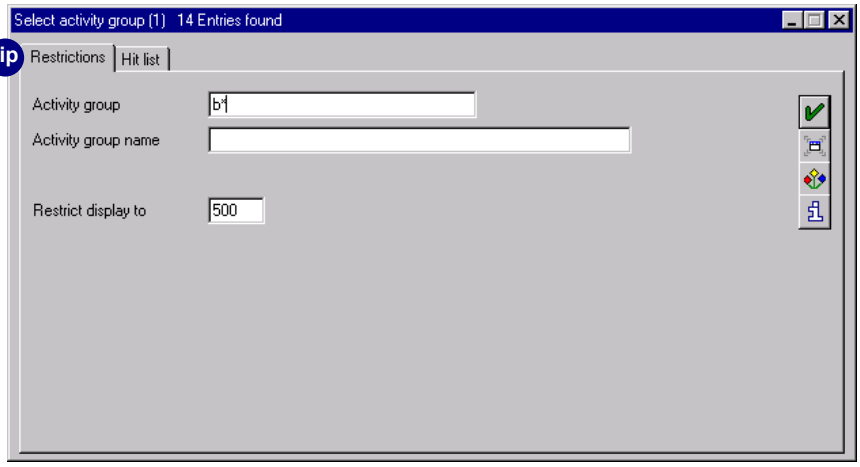


A *Hit list* appears.

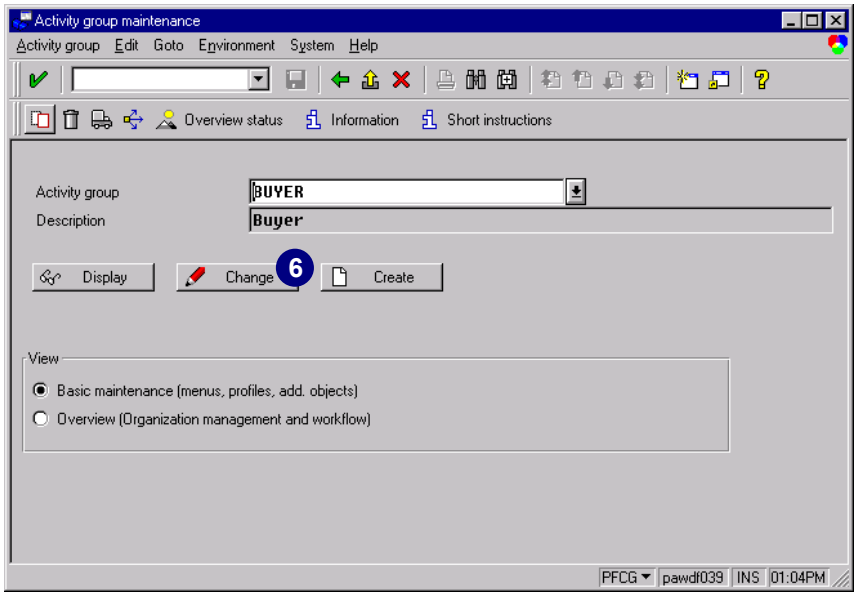
4. Select the activity group you wish to edit.
5. Choose *Copy*.



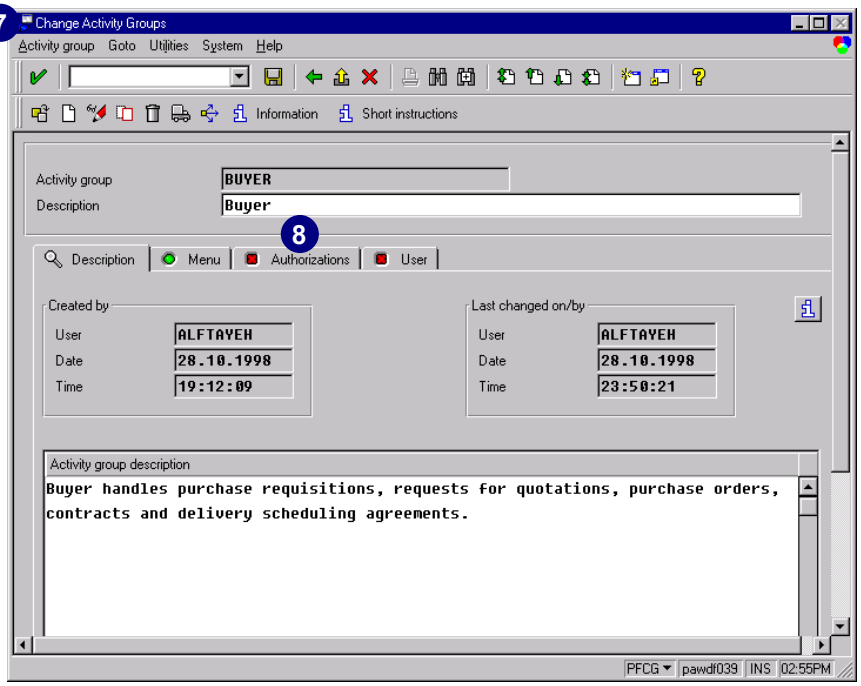
If the *Hit list* is too long, choose the *Restrictions* tab to narrow your search. Enter the first letters of the activity group you are looking for and choose *Start search*.



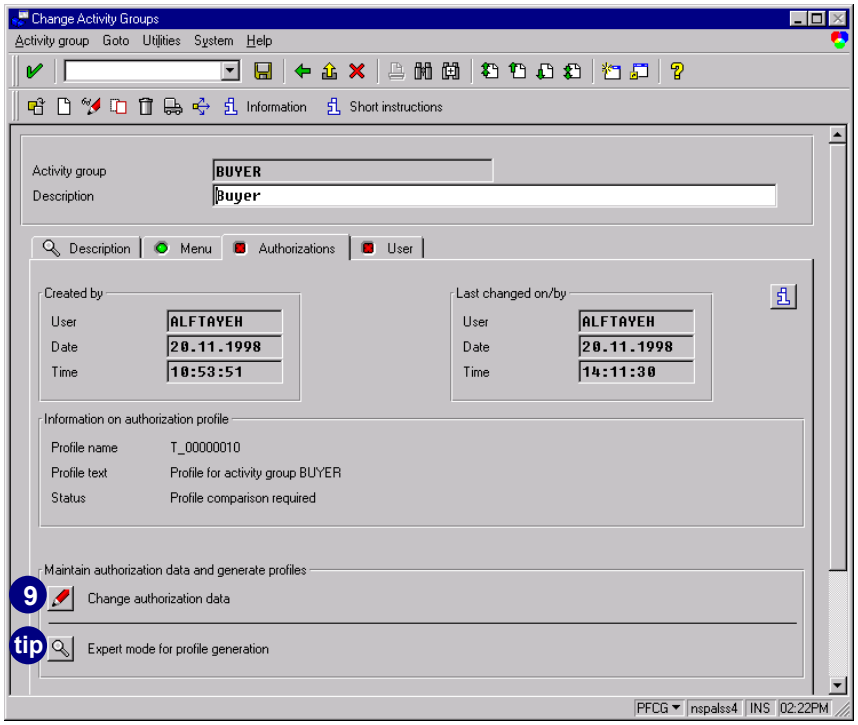
6. Choose *Change* to edit your activity group data.



7. The *Change Activity Groups* screen appears.
8. Choose the *Authorizations* tab.



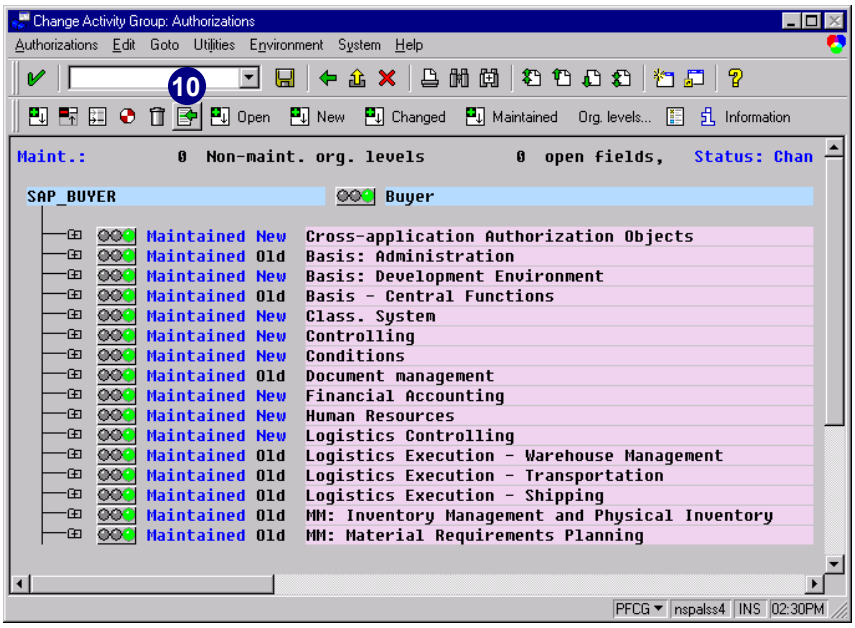
9. Choose *Change authorization data* to change and maintain the authorization data.



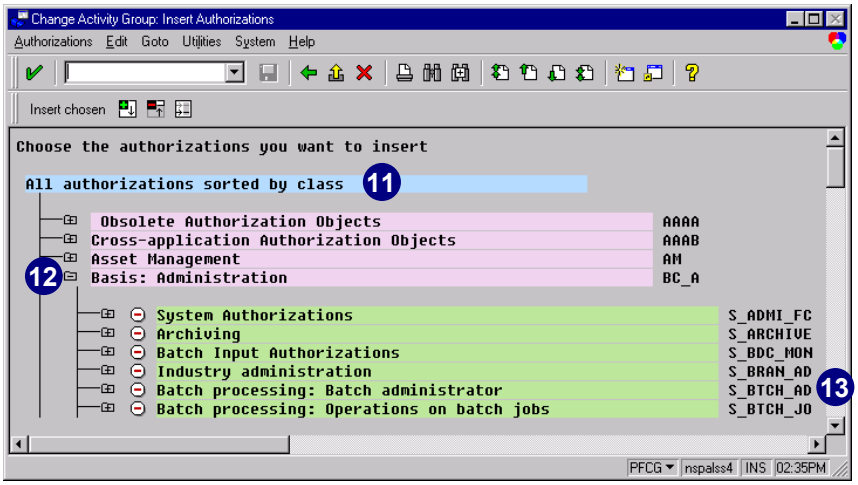
In *Expert mode for profile generation* you can select explicitly the option with which you want to maintain the authorization values. This option is automatically set correctly in normal mode.

On this screen we can see the already included authorization classes for this activity group.

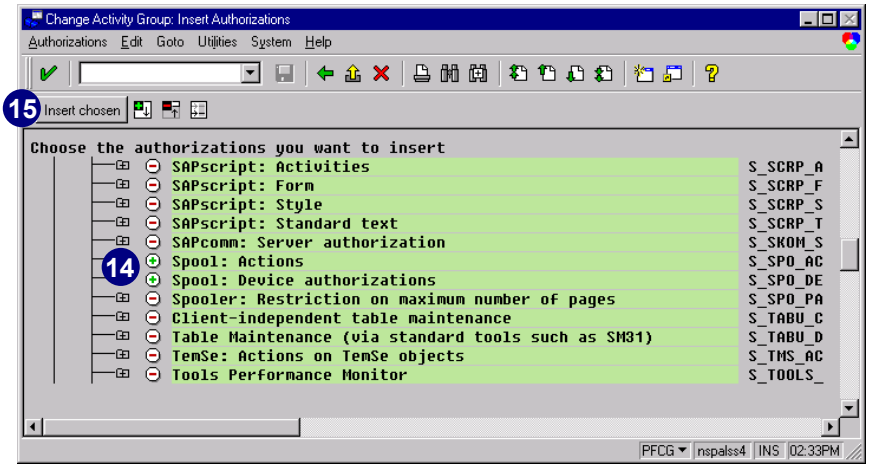
10. Choose *Insert manually* (or choose *Edit* → *Insert auth* → *Insert manually*).



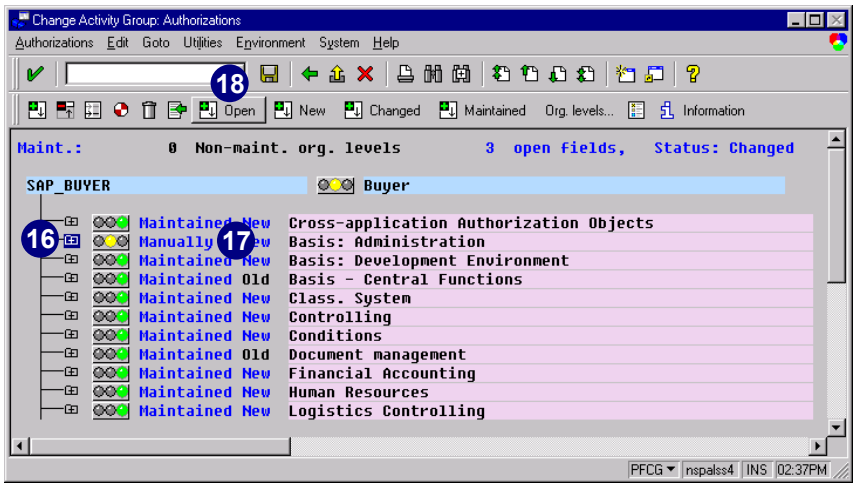
11. A new screen appears with all the authorization object classes appear from which you can choose.
12. Expand the object class *Basis: Administration* to choose the authorization objects for printing.
13. Scroll down until you see the authorization objects for *spool*.

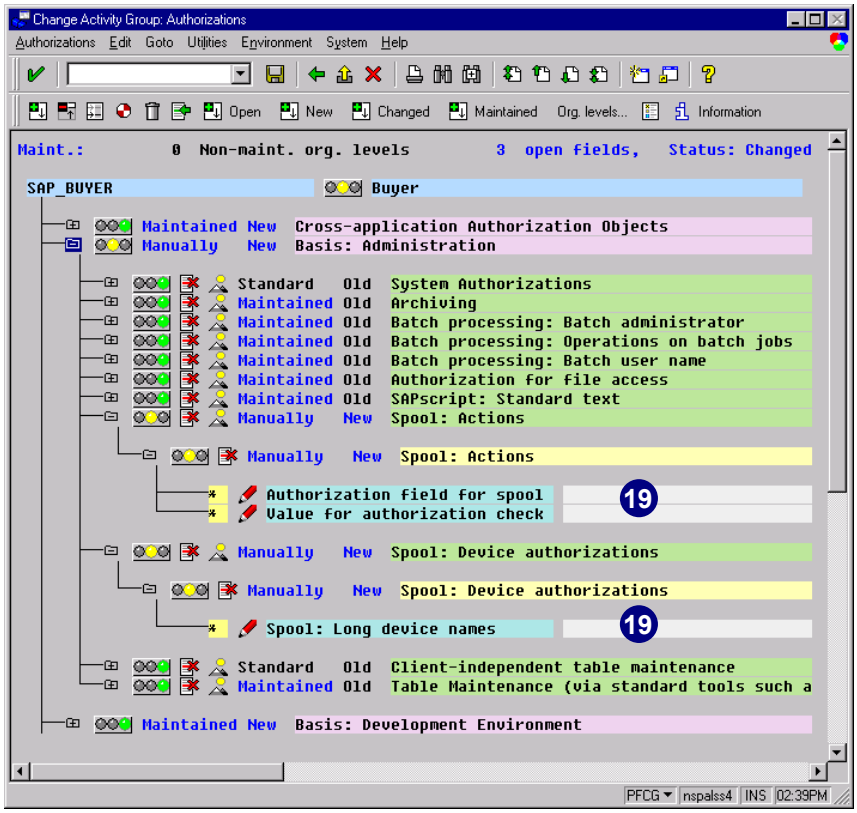


14. Click the circled red minuses (-) both for *Spool: Actions* and *Spool: Device authorizations* to select them. The circled green pluses (+) indicate that the objects have been selected.
15. Choose *Insert chosen*.



16. The two selected authorization objects are transferred back to the authorization classes for the specific AG, and the system creates a new authorization for each authorization object. However, as the yellow light indicates, no authorization field values are maintained yet.
17. You can also see that the status now reads *Manually*, which means that you have manually inserted authorizations underneath this object class.
18. Choose *Open* to display all open authorization fields.
19. Maintain the appropriate values for these open authorization fields and regenerate the authorization profiles.





Inserting Authorizations from a Template

Generated profiles do not automatically grant any general rights to:

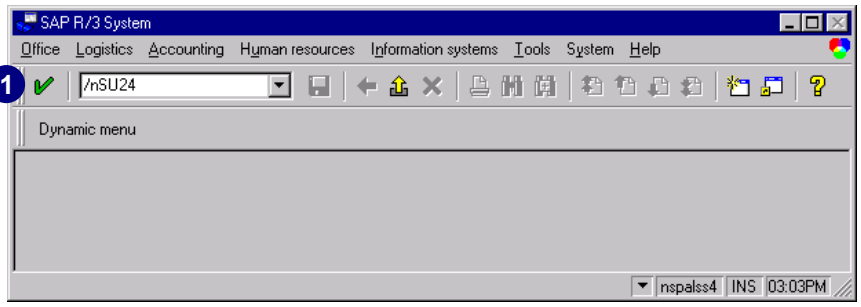
- Print
- Log on to Online Service System
- Use transaction **SU53**
- *Debug (view only)*

To assign general authorizations, choose one of the following options:

- Create a separate activity group with only general authorizations (such as printing), and assign this activity group to all users. (This method works best if users will print from any or all printers; a generic printing authorization can be assigned.) Generate the authorization profiles for these activity groups and assign them to the users.
- Include the required objects in the activity group by using SAP templates or your own templates and by maintaining any missing field entries. (This method is best if users will be assigned to particular printers.)

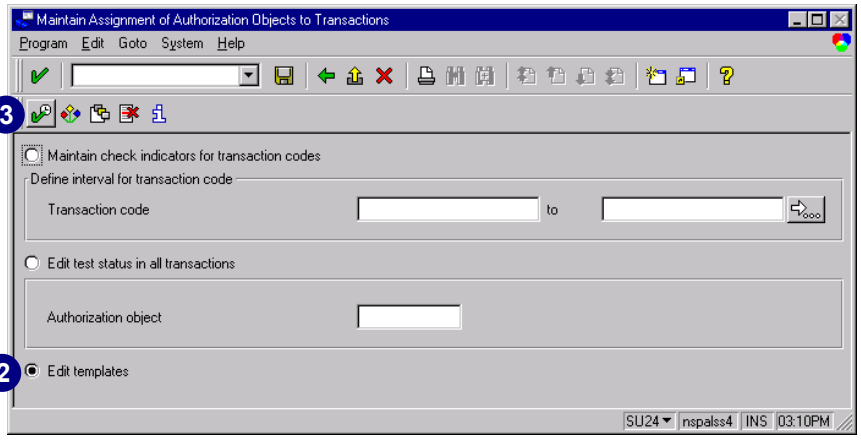
We will create a new template with transaction **SU24** and insert this template into an existing activity group.

1. In the *Command* field, enter transaction **SU24** and choose *Enter*.



You can also call transaction *SU24* from transaction *PFCG*. From the *Change Activity Group: Authorizations* screen, choose *Environment* → *Maintain templates*.

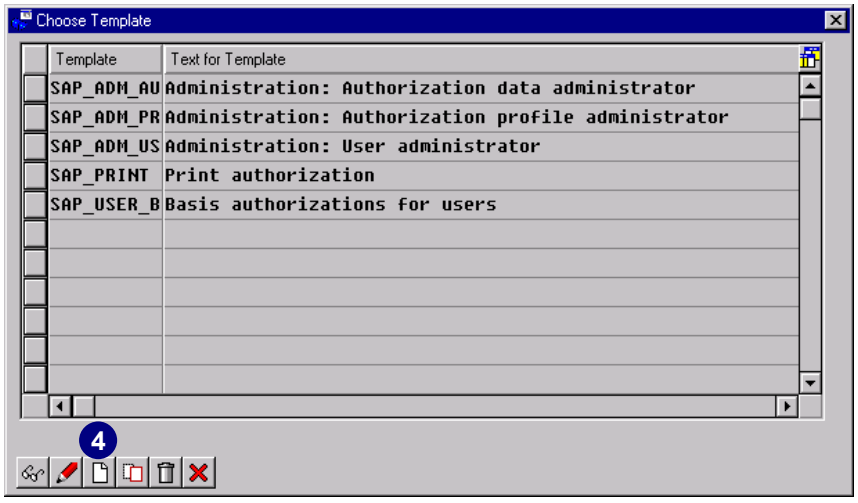
2. Select *Edit templates*.
3. Choose *Execute*.



A popup window appears showing a list of existing templates. All of the SAP-delivered templates begin with *SAP*.

You can either create your own templates or copy and alter the SAP templates.

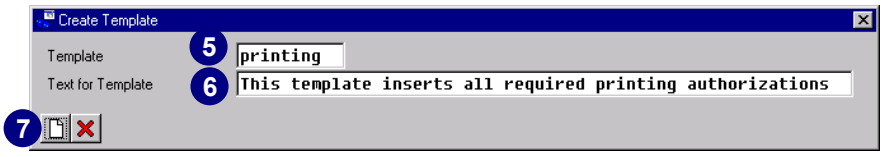
4. Choose *Create* to create your new template.

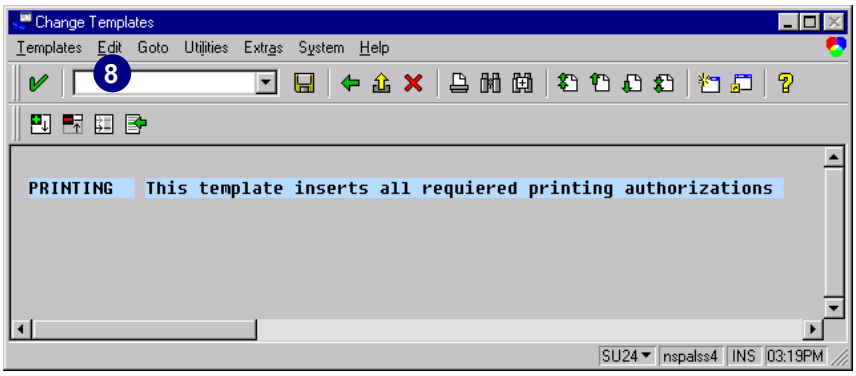


To avoid conflicts between customer-defined templates and the SAP-supplied templates, do not use template names (for your own templates) that begin with *S* or *J*. All other characters are possible. For additional information, please refer to Online Service System note *16466* and look for transport object *R3TR SUSP*.

Template changes are not passed on when you compare activity groups. That is, if you change a template that you already inserted into an activity group, there is no indicator in the activity group to show that the inserted template has changed.

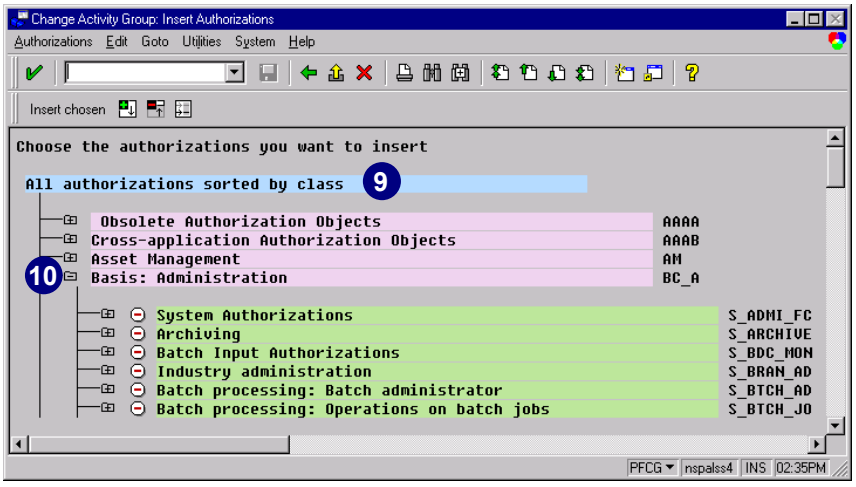
5. Enter the name for your new template in the *Template* field.
6. Enter descriptive text for the template in *Text for Template*.
7. Choose *Create*.
8. Choose *Edit* → *Insert auth.* → *Insert manually*.



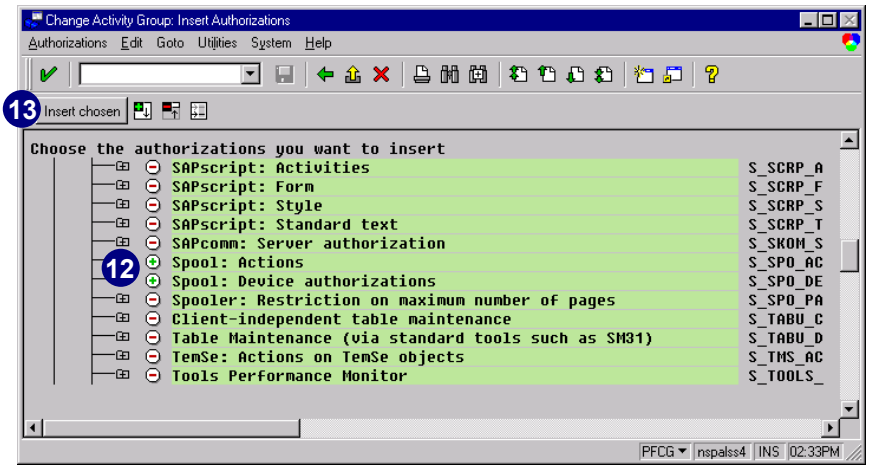


To create a new template, manually insert and complete the authorizations from existing profiles or other existing templates.

9. A new screen appears which shows all the authorization object classes.
10. Expand the object class *Basis: Administration* to choose the authorization objects for printing.
11. Scroll down until you see the authorization objects for *Spool* (see next page).



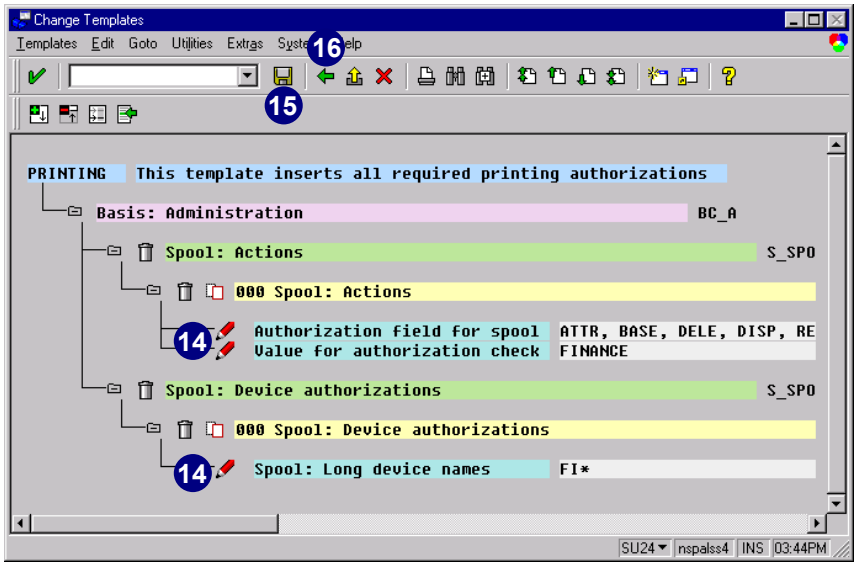
12. Click the circled red minuses (-) both for *Spool: Actions* and *Spool: Device authorizations* to select them. The circled green pluses (+) indicate that the objects have been selected.
13. Choose *Insert chosen*.



14. Maintain all possible open authorization fields for the template.

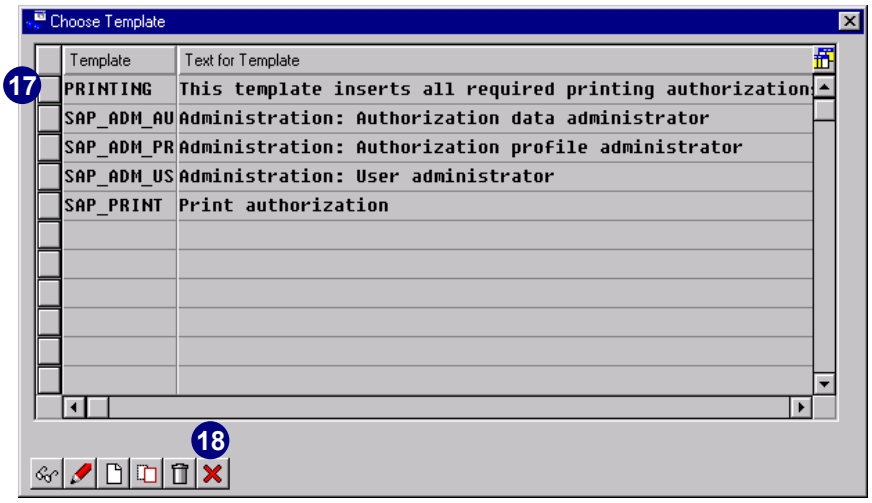
    The two selected authorization objects are transferred back to the first screen.

    In our example, we chose *Change* and maintained the appropriate value for this authorization field.
15. Choose *Save*.
16. Choose *Back*.



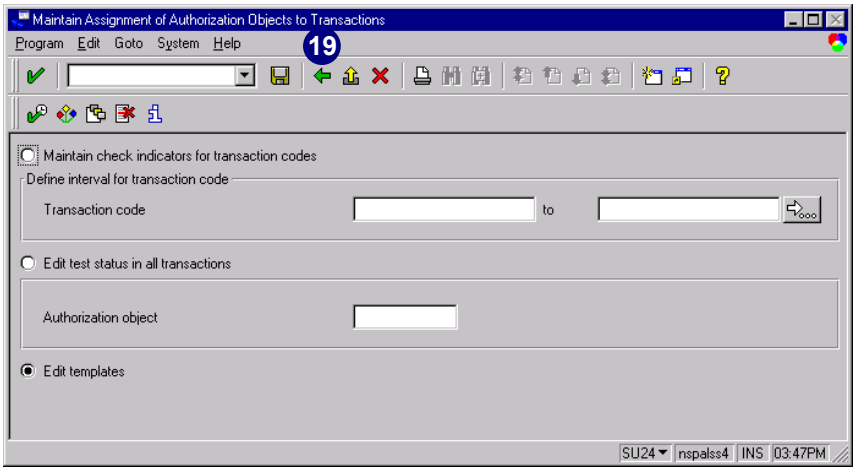
17. Your template now appears in the template list.
18. Choose *Cancel*.

    The new template is now created and can now be included in AGs.

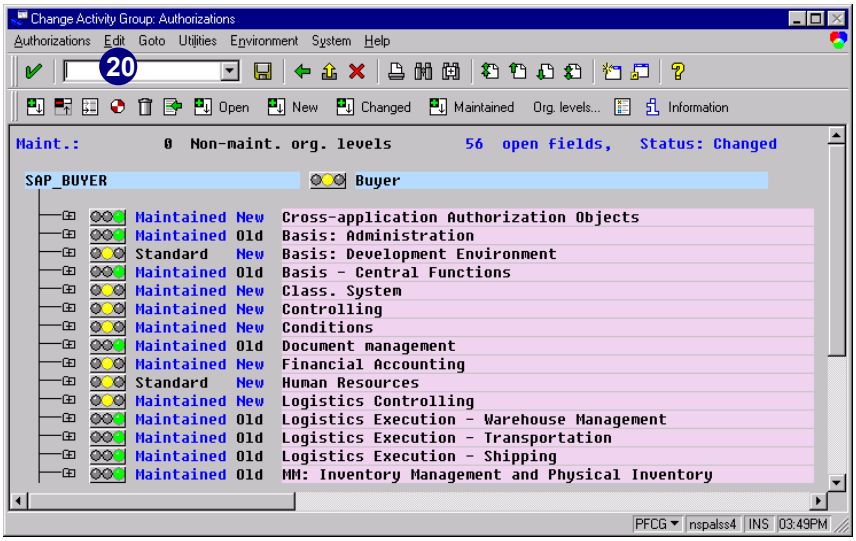


19. Choose *Back* to exit transaction *SU24*.

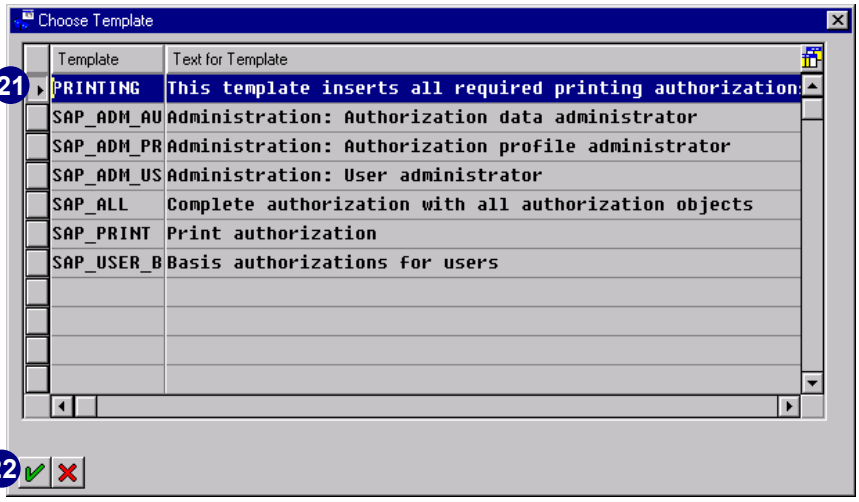
    We will now insert the newly created template into an existing activity group.



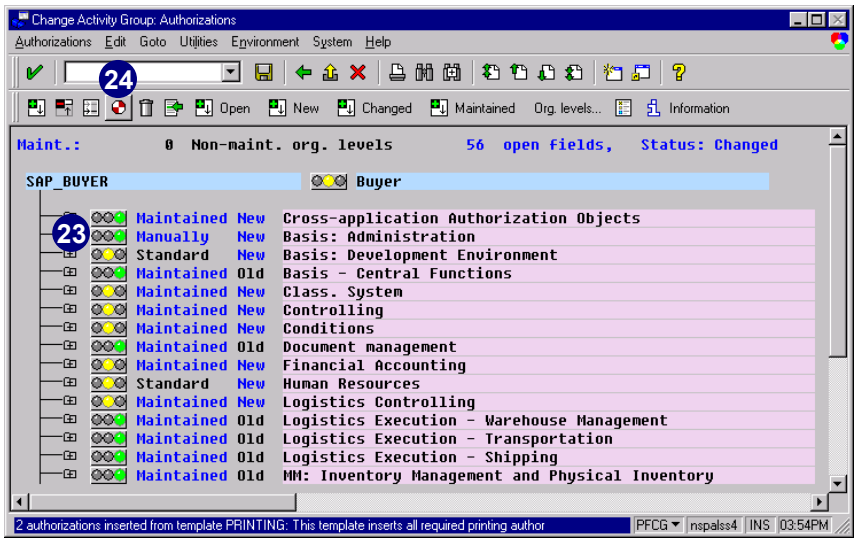
20. From the *Change Activity Group: Authorizations* screen (in transaction *PFCG*), choose *Edit* → *Insert auth* → *From template*.



21. On the popup window, select the template you want to insert. Multiple templates can be selected at the same time.
22. Choose *Continue*.



23. The template was inserted and marked with status *Manually*. The green light indicates that the authorization fields are maintained.
24. Choose *Generate* to regenerate the authorization profile.



If you inserted a template with nonmaintained authorization fields, the lights appear yellow or red for the appropriate authorizations, and you have to first postmaintain all open fields before proceeding.

Inserting Authorizations from a Profile

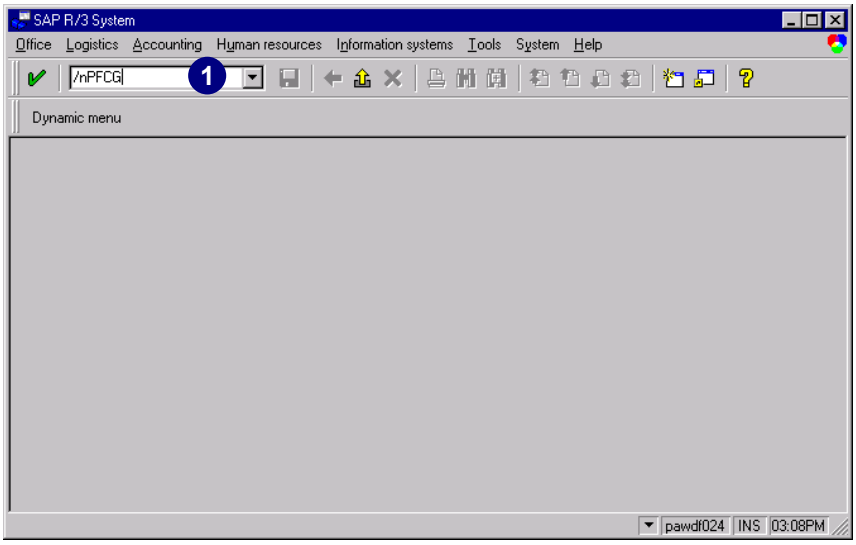
If you already created authorization profiles using transactions *SU02* and *SU03*, you can insert the authorizations in these profiles into the list of the authorizations of the activity group.

Migrating Profiles Created with Transactions *SU02* and *SU03*

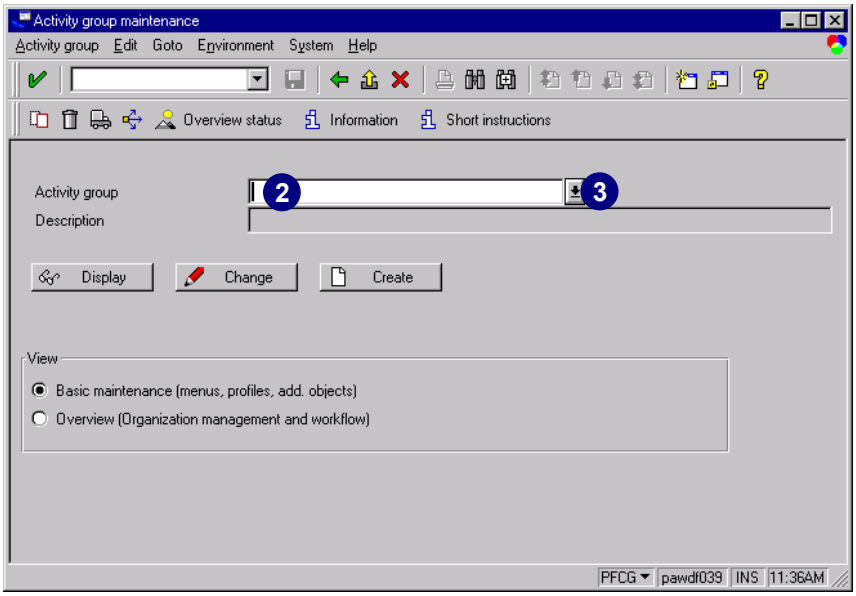
Please note that **no** activity group information (transaction codes accessible automatically maintained for object *S_TCODE* menu paths) can be regenerated for inserted profiles. The technique below **only** allows profiles, created with transactions *SU02* and *SU03*, to migrate to such profiles and later be maintained with the PG. There is no way to recreate the appropriate activity group information.

In certain circumstances, you may first create a template from your profile and then insert the template. Templates are reusable and easy to insert.

1. In the *Command* field, enter transaction **PFCG** and choose *Enter* (or choose *Tools* → *Administration* → *User maintenance* → *Activity groups*).

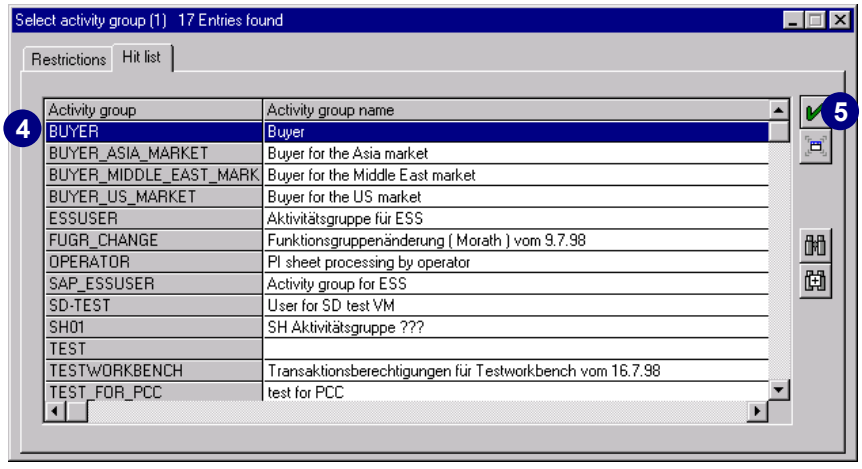


2. Place the cursor in the *Activity group* field.
3. Choose *possible entries*.

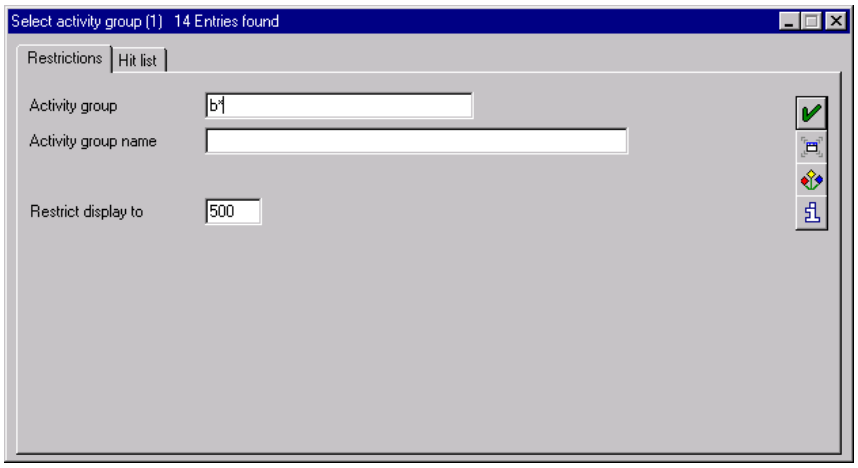


A *Hit list* appears.

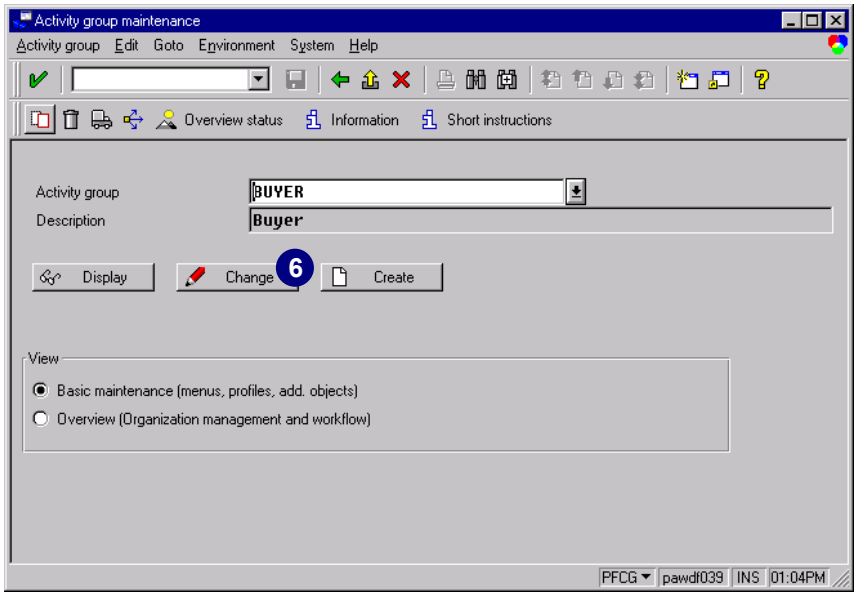
4. Select the activity group you wish to edit.
5. Choose *Copy*.



If the *Hit list* is too long, choose the *Restrictions* tab to narrow your search. Enter the first letters of the activity group you are looking for and choose *Start search*.

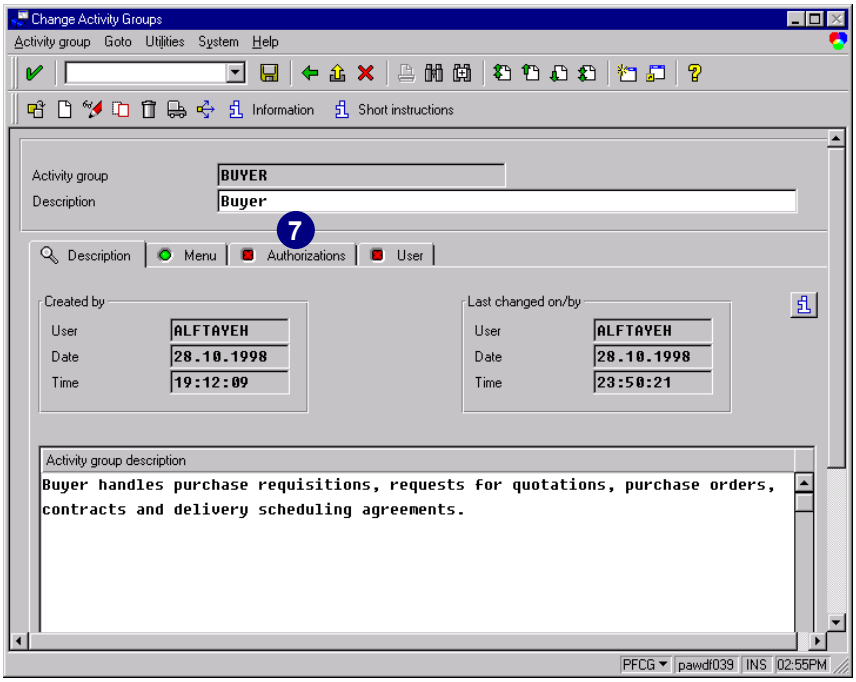


6. Choose *Change* to edit your activity group data.

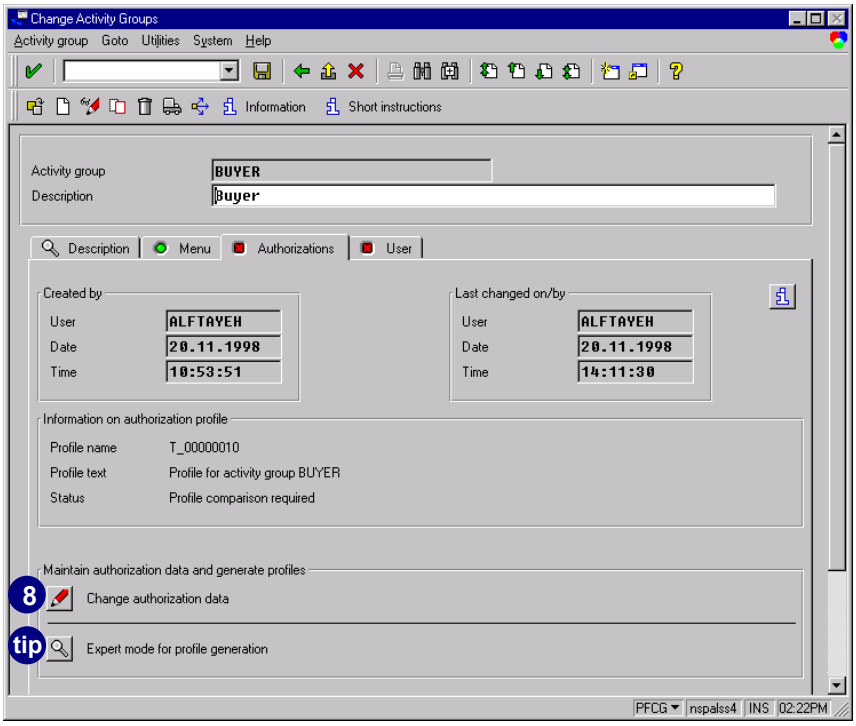


The *Change Activity Groups* screen appears.

7. Choose the *Authorizations* tab.

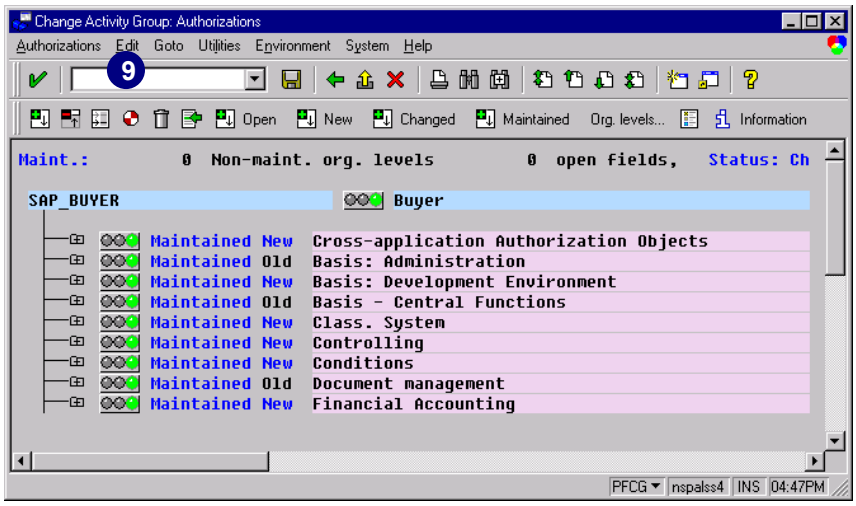


8. Choose *Change authorization data* to change and maintain the authorization data.



In *Expert mode for profile generation* you can select explicitly the option with which you want to maintain the authorization values. This option is automatically set correctly in normal mode.

9. From the *Change Activity Group: Authorizations* window, choose *Edit* → *Insert auth* → *From profile*.



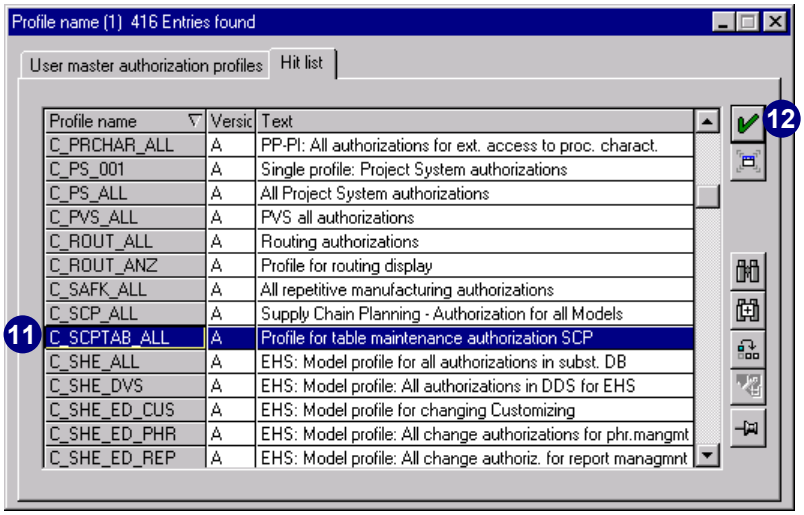
A popup window appears from which you can state which profile you wish to include.

10. Choose *possible entries* for *Profile* if you do not know the name of the profile you wish to include.

If you include a profile that includes the object *S_TCODE* in it, this does **not** add the transaction code to the menu portion of the AG definition.

11. Select the appropriate profile from the list of profiles.

You can only insert authorizations from single profiles. To insert a composite profile, look up the single profiles using transaction **SU02** and select the single profiles from this list.



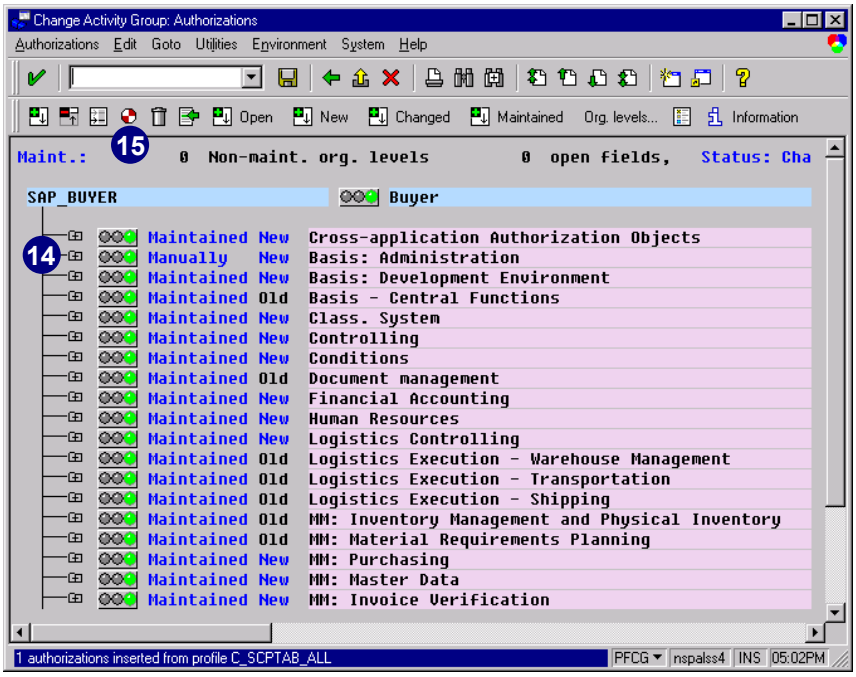
12. Choose *Copy*.

13. Choose *Enter*.

14. All authorizations in the selected profile were transferred and marked with a *Manually* status.

If you insert authorizations from a profile with nonmaintained authorization fields, the yellow or red lights appear for the appropriate authorizations and you have to first postmaintain all open fields before proceeding.

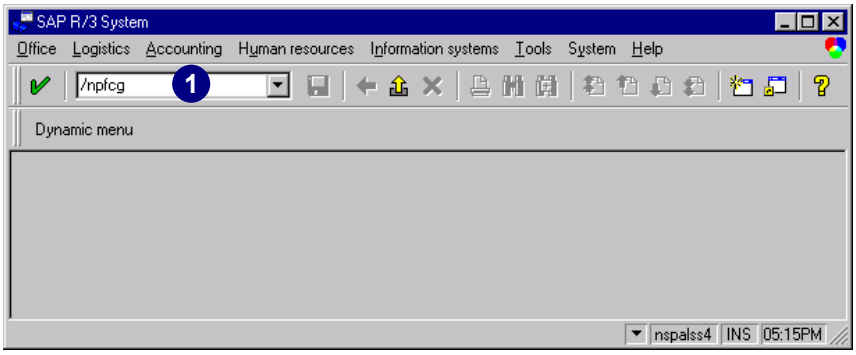
15. Choose *Generate* to regenerate the authorization profile.



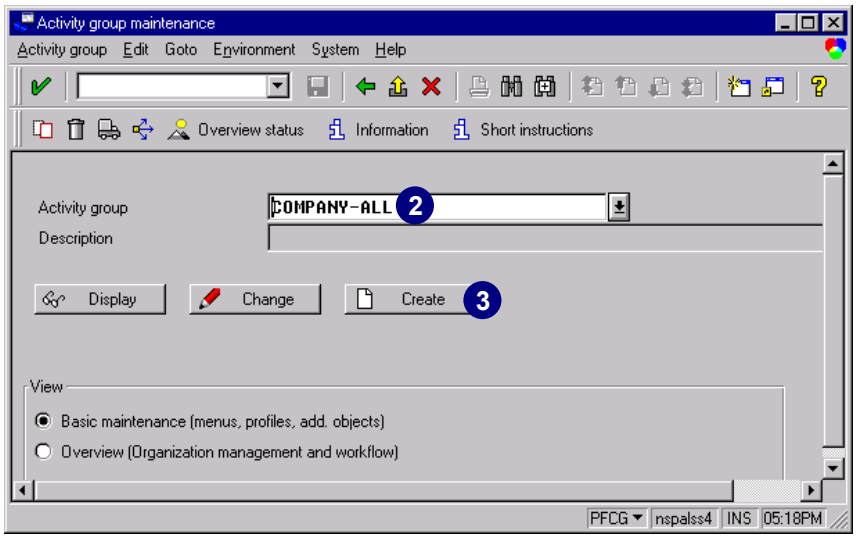
Inserting Full Authorizations: Profile "<YourCompany>-ALL

First, create a new profile *(<YourCompany>-ALL),* modeled after *SAP_ALL,* with the superuser authorizations removed.

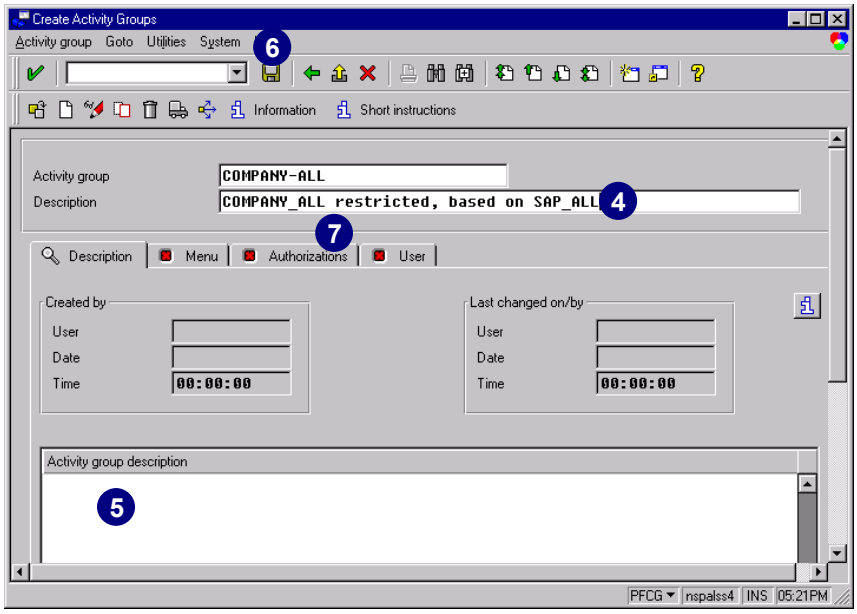
1. In the *Command* field, enter transaction **PFCG** and choose *Enter* (or choose *Tools* → *Administration* → *User maintenance* → *Activity groups*).



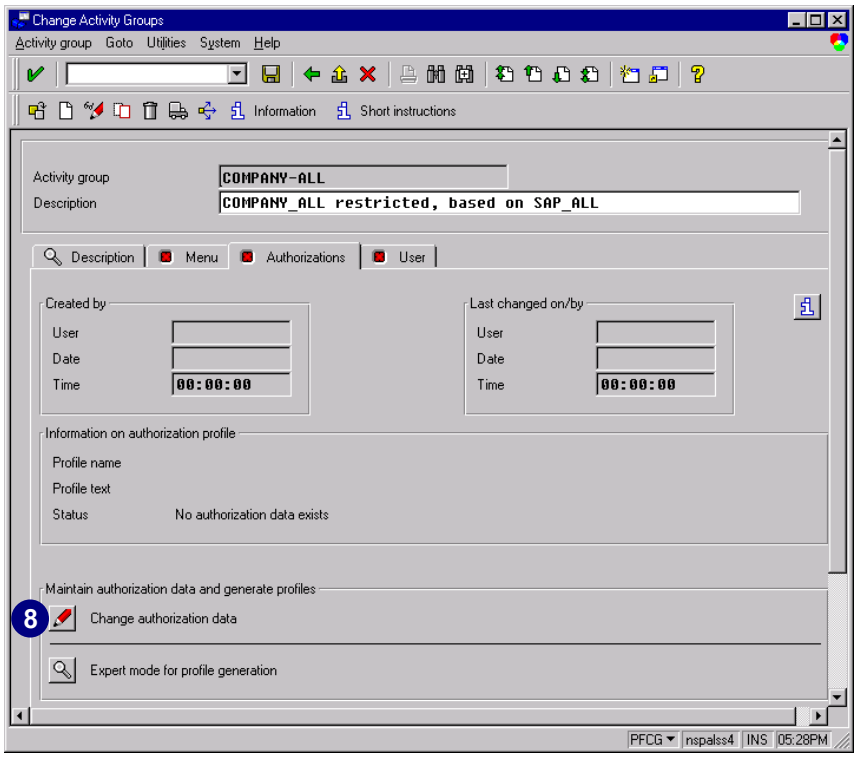
2. Enter a short name in *Activity group*. Exchange *COMPANY_ALL* with your company's name.
3. Choose *Create*.

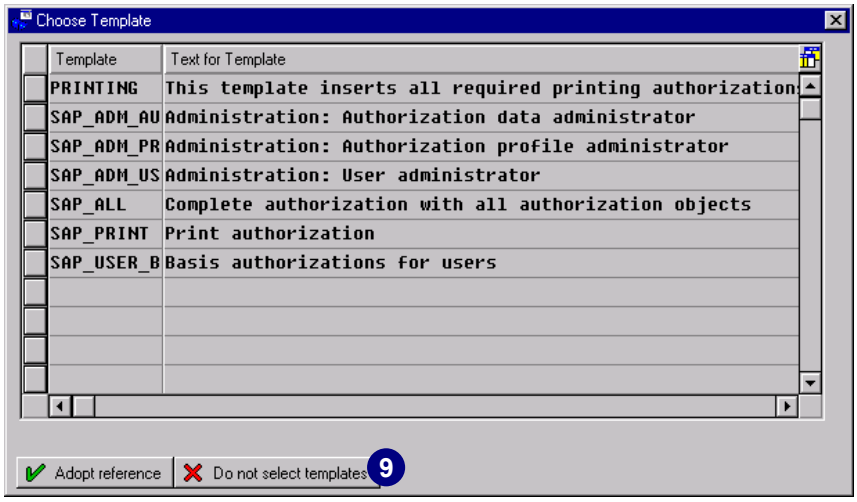


4. Enter a long descriptive name in the *Description* field.
5. Enter descriptive text under *Activity group description*.
6. Choose *Save*.
7. Choose the *Authorizations* tab.



8. Choose *Change authorization data* .

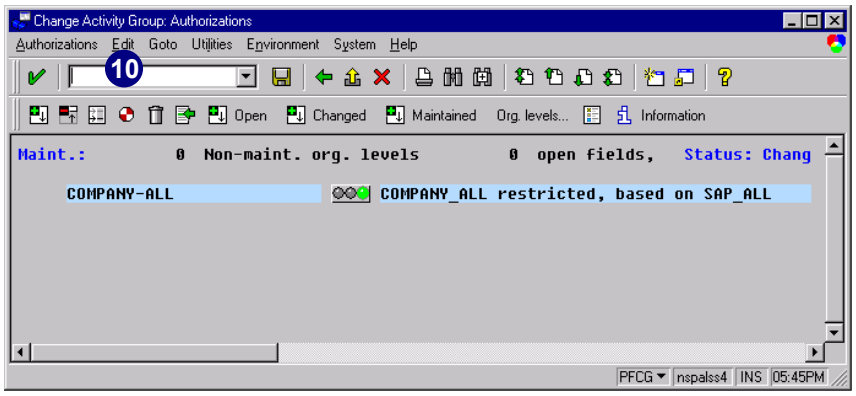




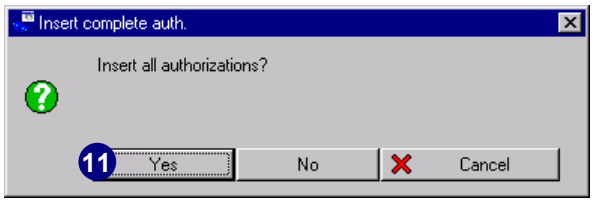
The system displays the *Choose Template* dialog box because no transaction was selected from the company menu tree; you only clicked on the *Authorizations* tab.

9. Choose *Cancel* to not select any templates.

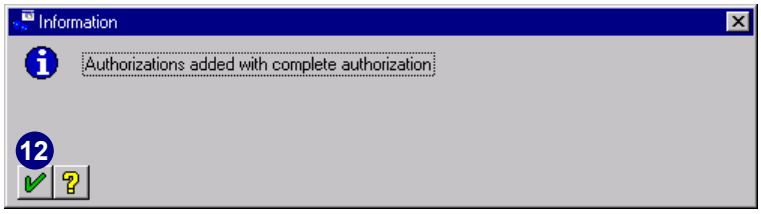
10. On the *Change Activity Group: Authorizations* screen, choose *Edit* → *Insert auth.* → *Full authorization.*



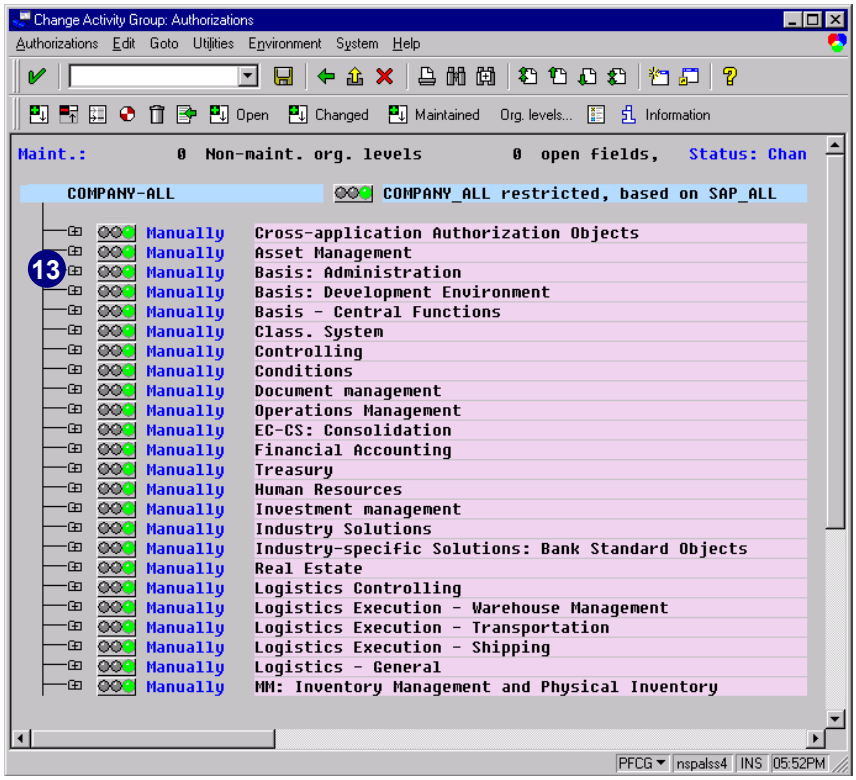
11. Choose *Yes*.



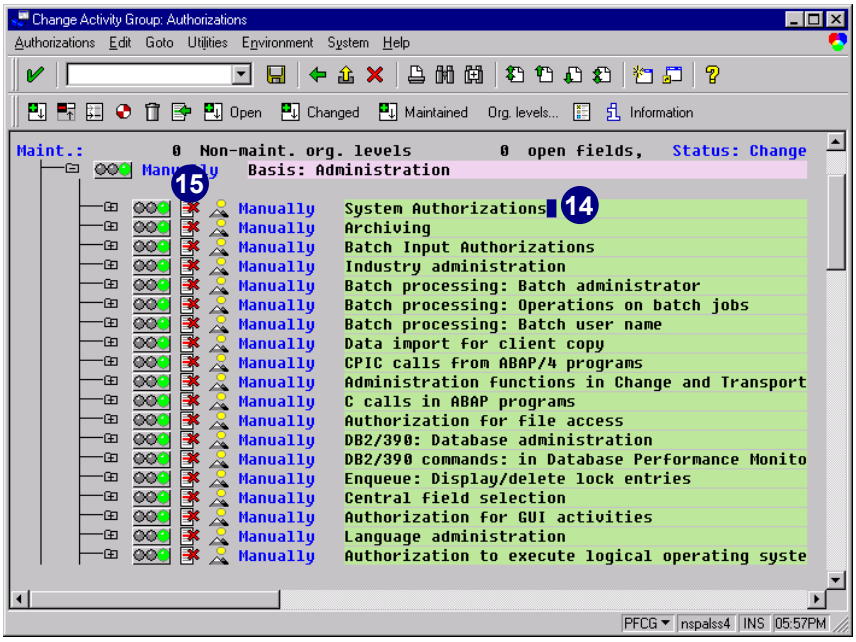
12. Choose *Continue*.



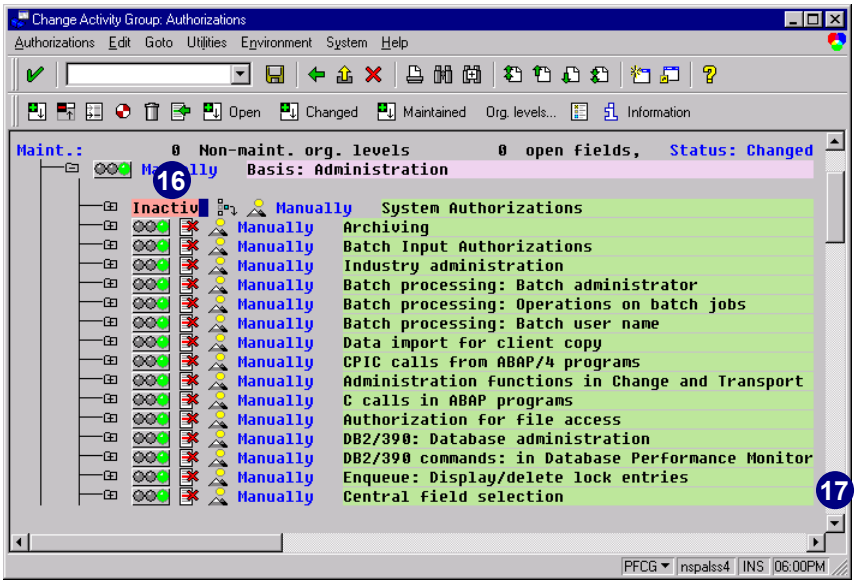
13. Click the node for the object class *Basis: Administration*.



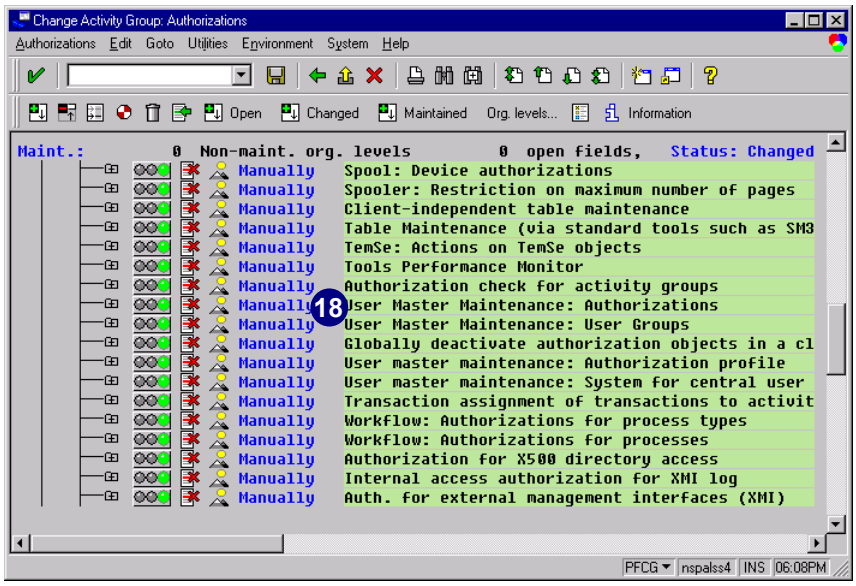
14. Select the *System Authorizations* line.
15. Choose *Inactivate*.



16. The authorization object *System Authorizations (S_ADMI_FCD)* is now inactive and will not be generated into the authorization profiles for *COMPANY_ALL*.
17. Scroll down until you see the authorization objects that begin with *User Master Maintenance*.

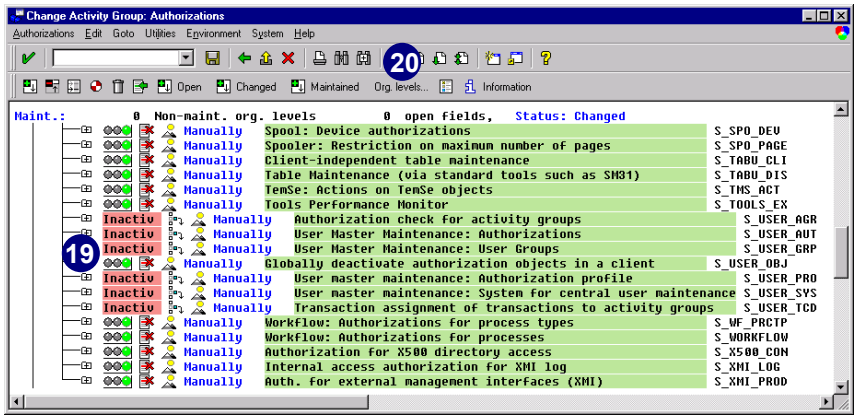


18. Choose *Inactivate* to deactivate the following authorization objects:
    - *Authorization check for activity groups (S_USER_AGR)*
    - *User Master Maintenance: Authorization (S_USER_AUTH)*
    - *User Master Maintenance: User Groups (S_USER_GRP)*
    - *User Master Maintenance: Authorization Profile (S_USER_PRO)*
    - *User Master Maintenance: System for central user (S_USER_SYS)*
    - *Transaction assignment of transactions to activity groups (S_USER_TCD)*

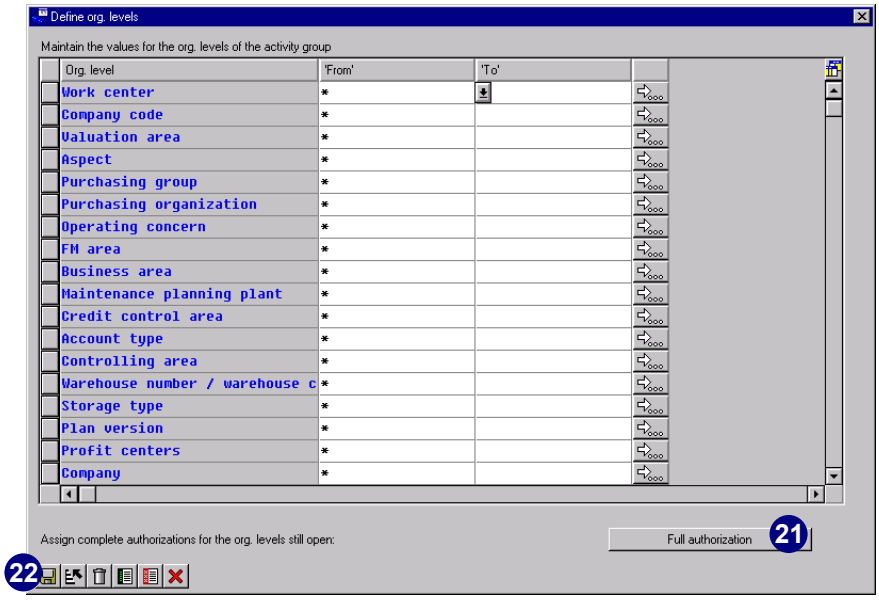


19. Once you have deactivated these critical authorization objects for your authorization profile, select other critical authorization objects and deactivate them, if desired.

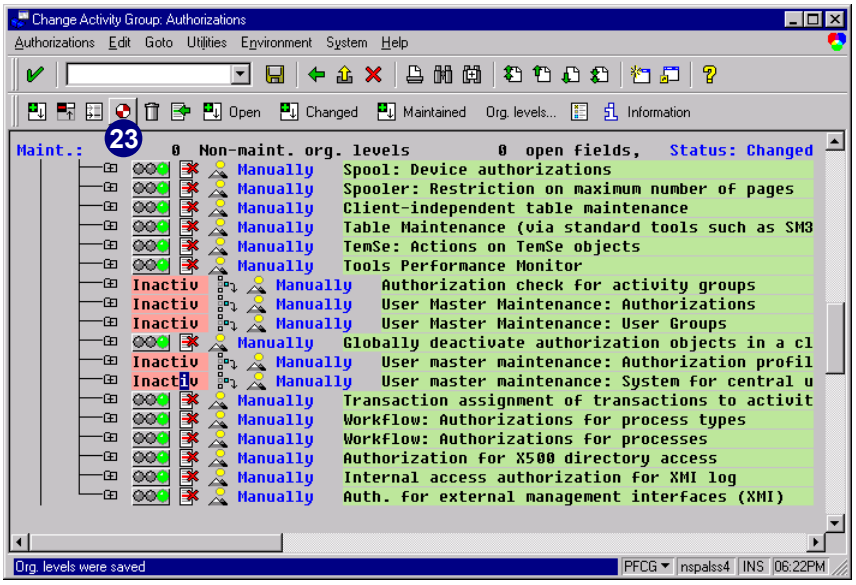
20. Choose *Org. levels*.



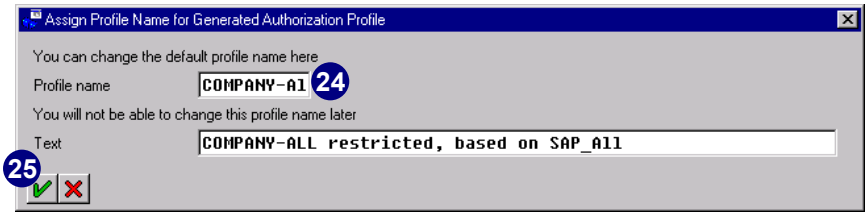
21. Choose *Full authorization*.
22. Choose *Transfer*.



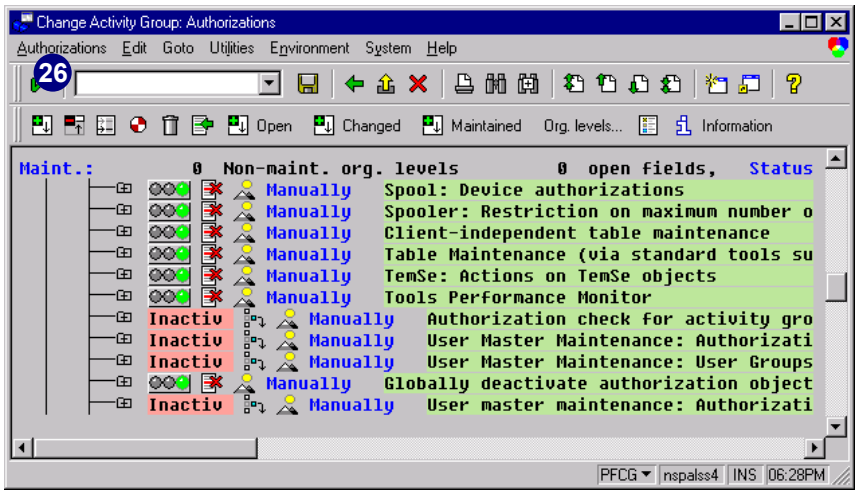
23. Choose *Generate*.



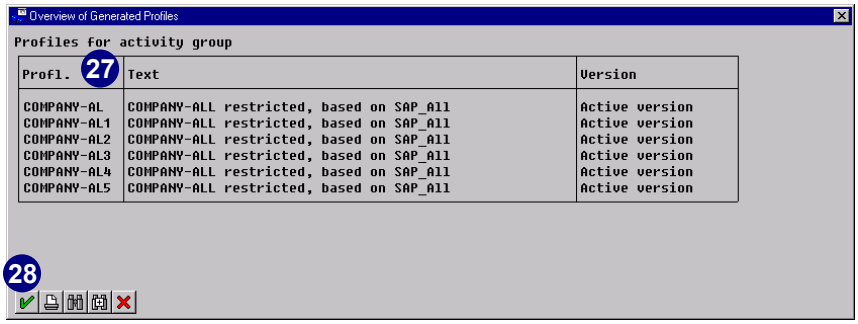
24. You can give the new profile the same name and short text as the activity group (for example, in *Profile name* **COMPANY-AL**).
25. Choose *Execute* and the authorization profile(s) are created.



26. Choose *Authorizations* → *Profile overview.*



27. The names of all of the created authorization profiles appear.
28. Choose *Continue.*



The next steps:

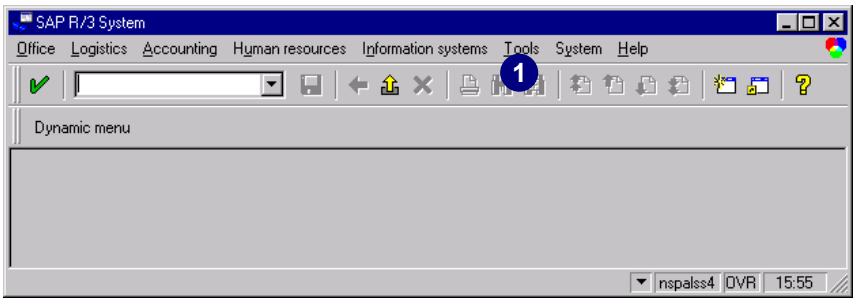
- Create users (please see chapter 3 for more information).
- Assign activity groups to users or PD objects and update user master records (please see chapter 8 for more information).
- Log on as a new user to R/3.

Assigning Transaction Codes to Reports

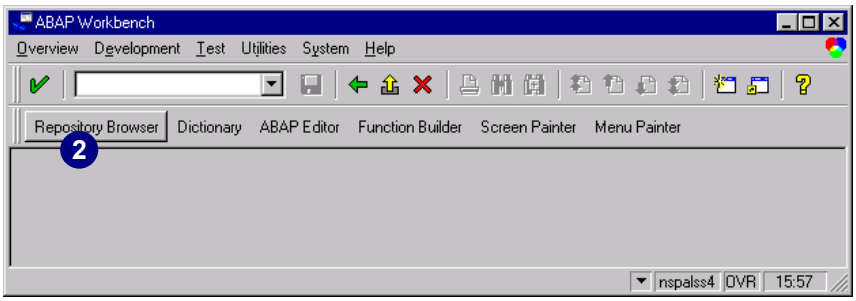
The procedures shown in this section should only be performed in cooperation with a developer or ABAP Workbench expert, because these tasks normally fall within a developer's scope of work.

You can assign transaction codes to stand-alone programs so that you can handle these programs as if they were transactions.

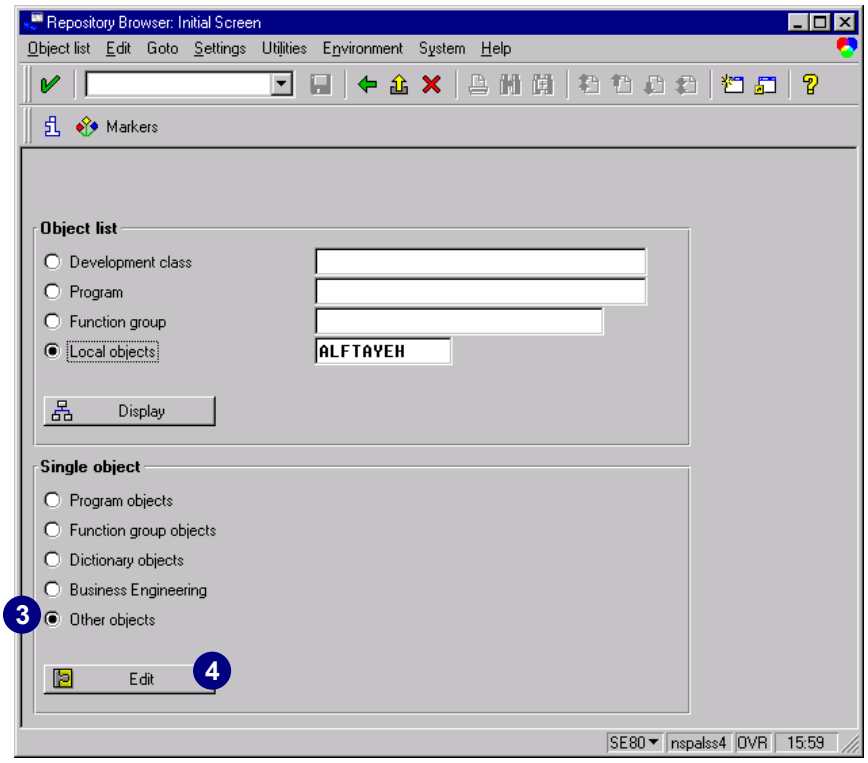
1. Choose *Tools* → *ABAP Workbench*.



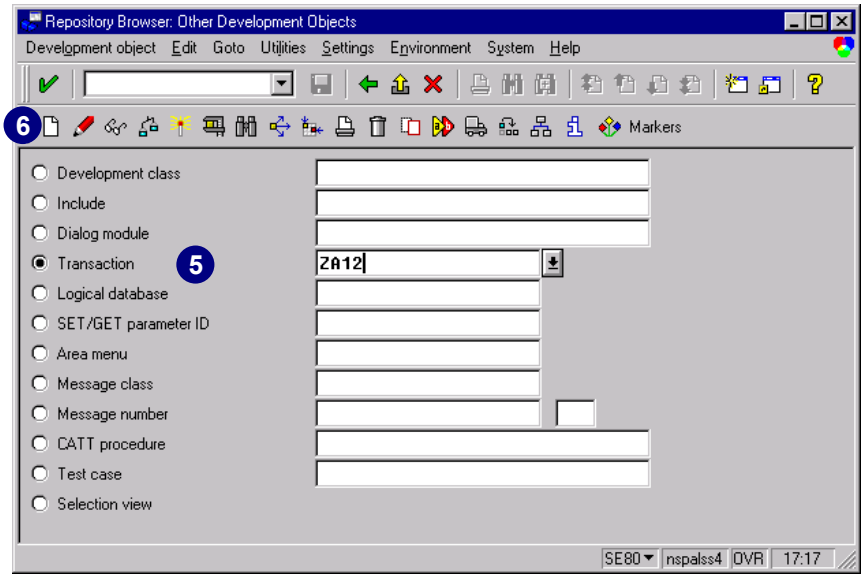
2. Choose *Repository Browser*.



3. Select *Other objects*.
4. Choose *Edit*.



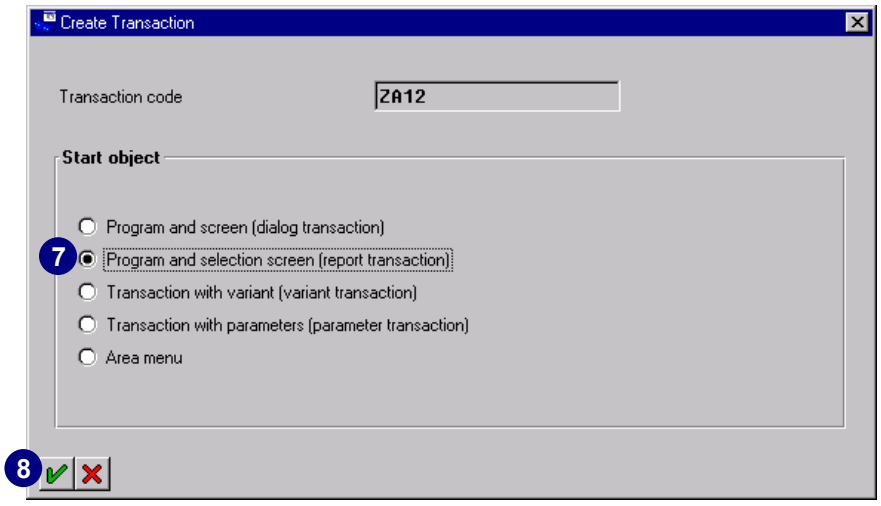
5. Enter the name of the transaction you are creating in the field *Transaction* (for example, **`ZA12`**).
6. Choose *Create*.



7. Select the *Start object* you wish to assign (for example, we assigned a customer-developed report to a transaction code). To do this, we selected *Program and selection screen (report transaction)*.

   If you would like to assign an area menu, select *Area menu*.

8. Choose *Continue*.



9. Enter the *Transaction text*.

10. In *Program*, enter the name of your developed report or the name of the module pool (if a dialog transaction).

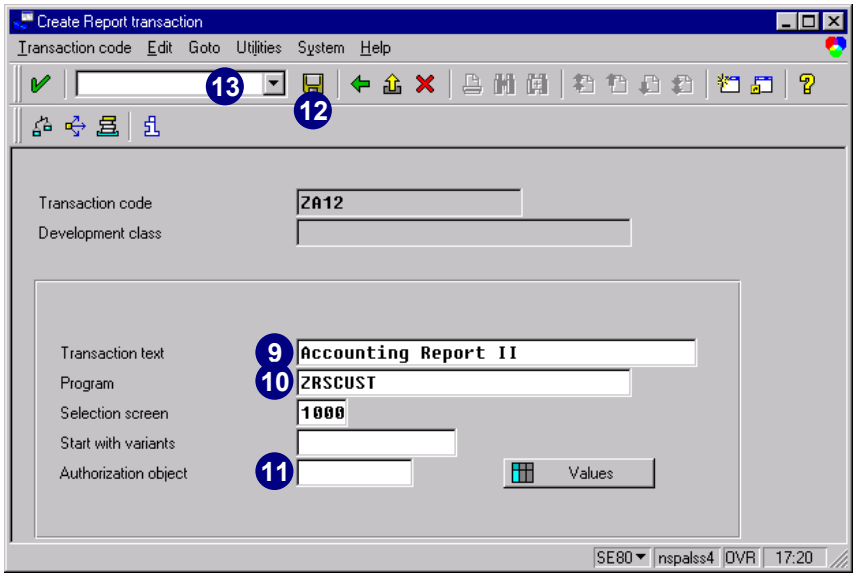
    In our example, we already created and saved a report called *ZRSCUST*.

11. Enter the name of the *Authorization object*. This authorization object will be checked against the authorizations of the user who calls the transaction. If the user does not have the necessary authorizations, the transaction will be canceled.

    If you leave this field blank, no authorization check is performed when the transaction is called except for the S_TCODE value of ZA12 and whatever authorization checks are embedded in the program ZRSCUST.

12. Choose *Save* to save the transaction code.

13. You can now enter transaction **`ZA12`** in the *Command* field to execute your new transaction.



Authorization Checks

Authorizations are checked against objects in the system. The authorization objects enable complex checks (that is, checks linked to several conditions) of an authorization. For a successful authorization check, the user must be verified for each object field.

This check takes place only if you begin a transaction from a menu or if you enter **/n<Transaction code>** in the *Command* field. It is not always performed for called transactions or parameter transactions. The developer is responsible for performing the necessary authorization checks during the program or at the start of the transaction.

Additional Maintenance Requirements

Although you can now see that the new transaction code exists (and you can even put it on a menu path), it does not mean that the profile generator will recognize this transaction code. As such, when new transaction codes are added to the menu structure, the following must be done.

1. Run transaction **SSM1** (**SSM1** = Generate Company Menu).
2. Choose *Generation* → *Reset*.
3. Perform steps 1–2c described in chapter 2, the section *Generating the SAP Standard Menu and Company Menu*.
4. If there are any authorization checks in the transaction, run transaction **SU24** and maintain the check indicators for your transaction. Please see chapter 2, the section *Reducing the Scope of Authority Checks in R/3* to learn how to work with transaction **SU24**.

   These steps need to be performed before the PG generates the appropriate authorization for your developed transaction.

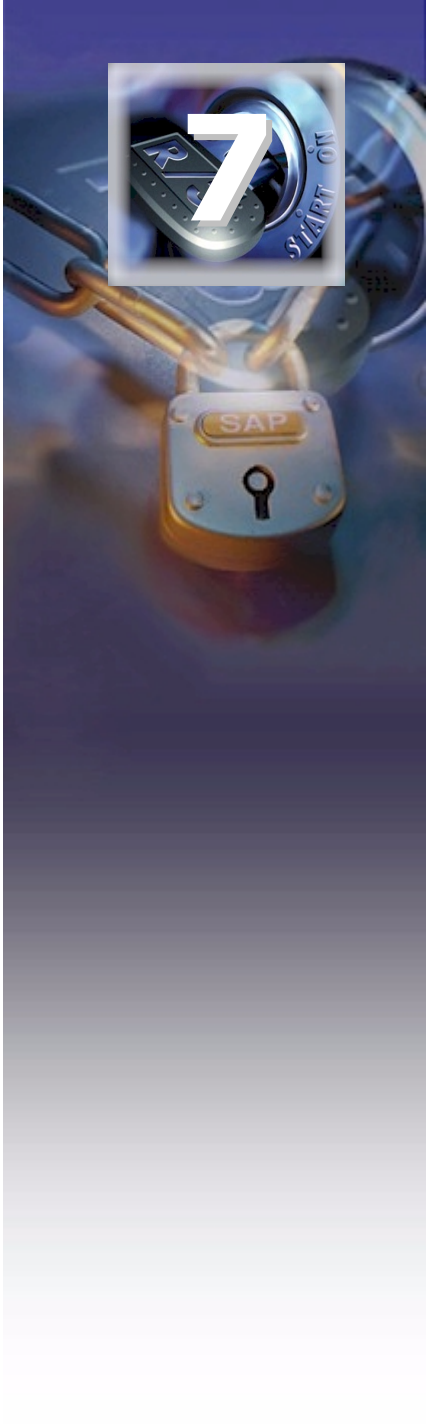
Adding Any Missing Transactions to the Company Menu Tree

A much faster and easier way exists to add a missing transaction code to the company menu. This missing code can be a customer-developed or an SAP-standard transaction that cannot be selected from the menu tree in the standard R/3 System.

What Is Important?

Using the technique described below allows the missing transactions to be selected from within the PG. The added transactions will all appear under *Other transactions* in the company menu tree. Also, when you log on to R/3 with the Session Manager (transaction **SESS**), the added transactions are visible in the company menu tree. However, if you log on to R/3 with the regular SAPgui, the added transactions will not be visible in the menu tree, since you are looking at the standard R/3 menu, not the company menu.

See chapter 2 for a detailed procedure describing how to add missing transactions to the company menu tree.



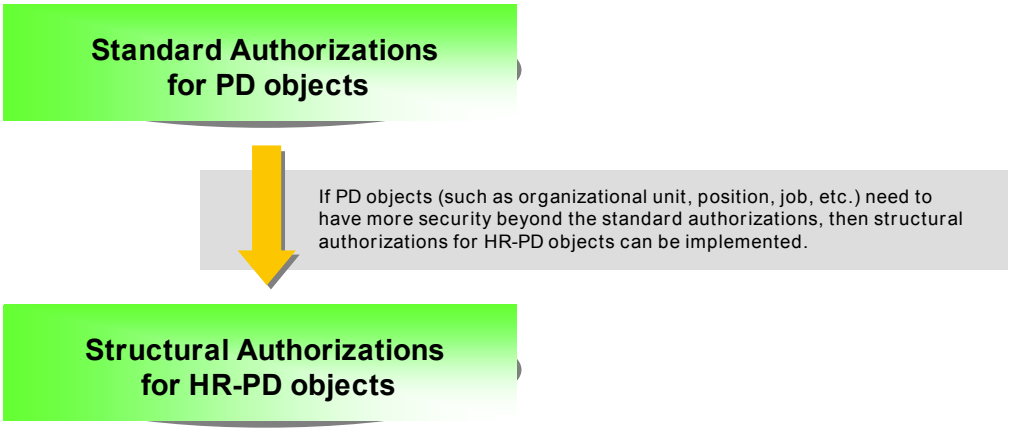
Chapter 7: Structural Authorizations

Contents

Working with Structural Authorizations in Personnel Development

Overview

The following diagram gives a brief overview about the relationship between **standard authorizations** and **structural authorizations** in R/3. We will proceed with a more detailed explanation during the chapter.



If the standard authorizations of Personnel Development (PD) objects (ability to access or not access an object type) in HR are not sufficient (the authorization object that might not be sufficient is PLOG), you might consider using structural authorizations.

Structural authorizations provide more detailed security. However, this security comes at a cost. If you become too zealous and use too many or too complicated structural authorizations, the system response time (performance) can be dramatically affected. The exact impact cannot be noted here as it is dependent on a combination of factors at each R/3 site based on configuration, volume of data records, complexity of structural authorization profiles, and quantity of structural authorization profiles involved. For example, it is possible that only a percentage of users would recognize the effect, while the rest of the users see absolutely no difference in response time.
Structural authorizations require additional maintenance. They are not consistent with the standard authorization concept and therefore require a higher skill set.

Warning: Structural authorizations are **not** an alternative to what has been discussed thus far—they are "in addition to." Structural authorizations have absolutely nothing to do with the Profile Generator (PG).

It is not necessarily required that you use structural authorizations if you implement HR or HR-PD.

Creating a Sample Organizational Plan
To work with structural authorizations in Personnel Development (PD), it is essential that you have an organizational plan in your system. If you have not created an organizational plan for your company, but want to test this functionality, please see chapter 8, the section *Creating a Sample Organizational Plan.*

How you set up an organizational plan depends on three assumptions:

- *You will never implement HR or workflow*

  It is okay that the authorizations administrator uses only this guidebook.
- *You will implement HR or workflow in the future*

  You need to get someone involved in the HR implementation to evaluate your ideas, so you do not cripple yourself in the future by needing a mini-implementation to undo an improperly implemented organizational plan.
- *You are currently implementing or already using HR*

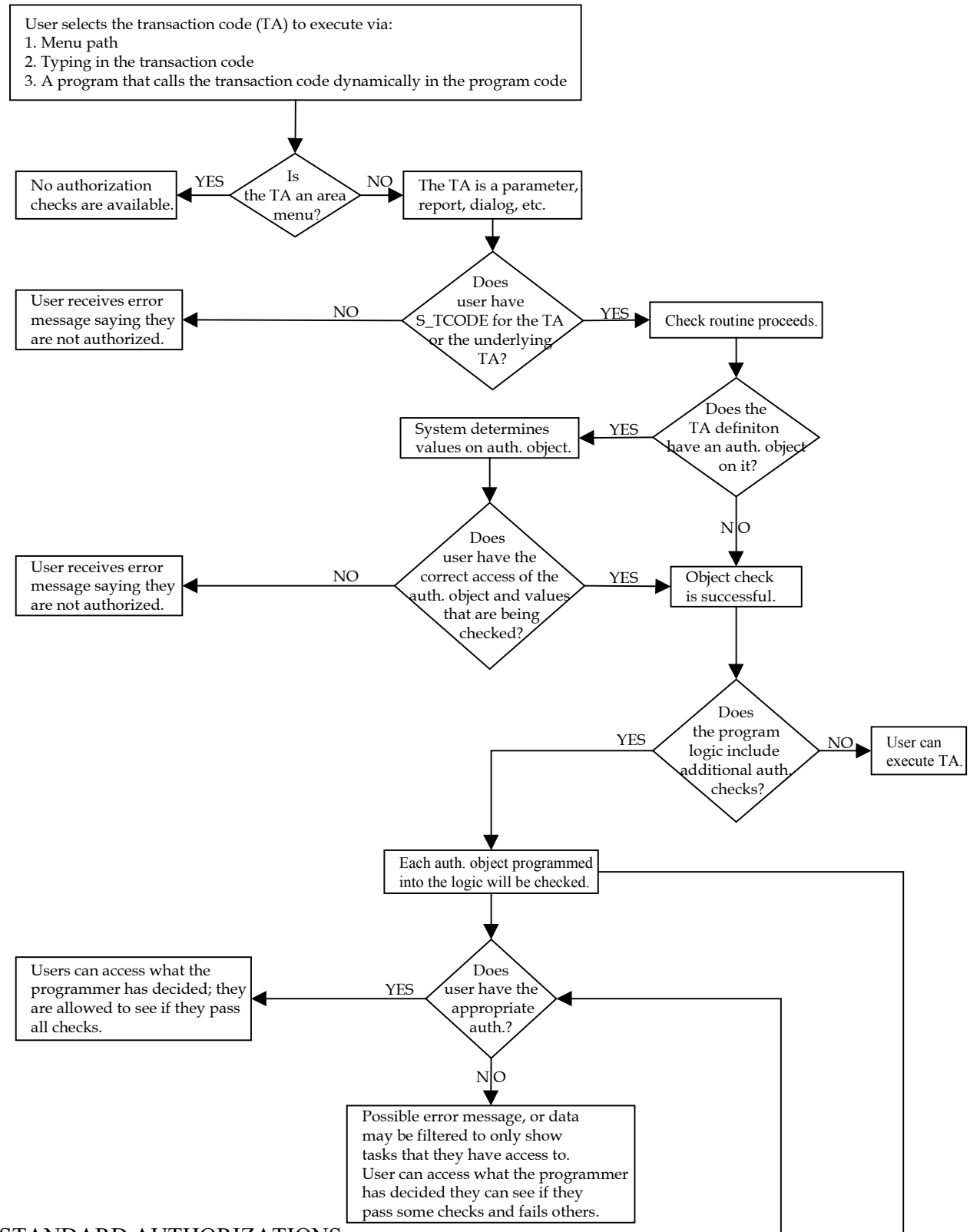
  The authorization administrator cannot create the organizational plan alone. It has to been done with the HR team.

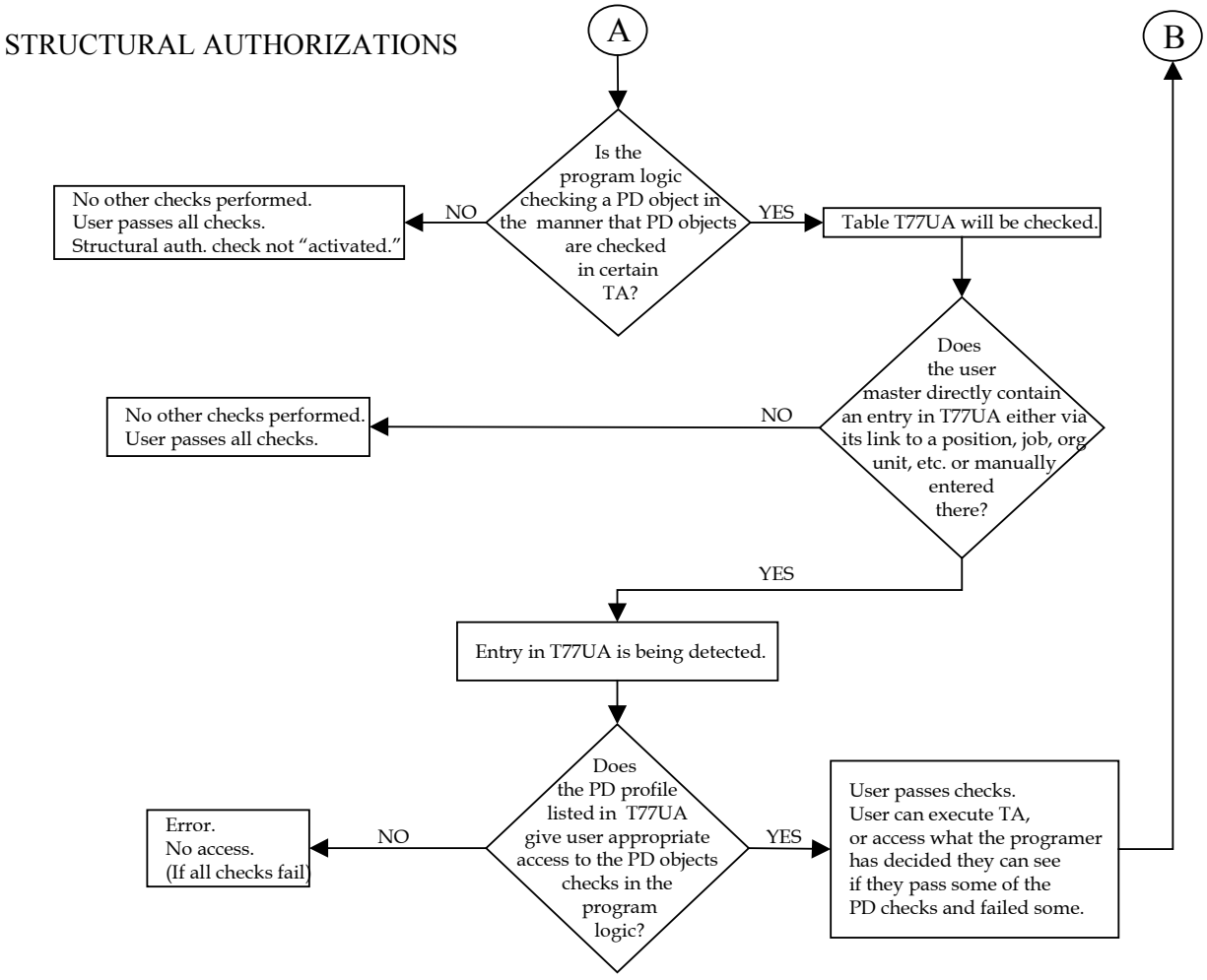
HR-PD background information

In order to work in PD, you must understand two core concepts:

- *Object types* – positions, jobs, organizational levels, etc.
- *Object* – particular positions, particular jobs, particular organizational levels, etc.

The diagram on the next page attempts to demonstrate the relationship between standard authorizations and structural authorizations. Specifically, it shows where the one ends and the other begins.


User selects the transaction code (TA) to execute via:
1. Menu path
2. Typing in the transaction code
3. A program that calls the transaction code dynamically in the program code
Is the TA an area menu?
YES
No authorization checks are available.
NO
The TA is a parameter, report, dialog, etc.
Does user have S_TCODE for the TA or the underlying TA?
NO
User receives error message saying they are not authorized.
YES
Check routine proceeds.
Does the TA definiton have an auth. object on it?
YES
System determines values on auth. object.
NO
Does user have the correct access of the auth. object and values that are being checked?
NO
User receives error message saying they are not authorized.
YES
Object check is successful.
Does the program logic include additional auth. checks?
YES
NO
User can execute TA.
Each auth. object programmed into the logic will be checked.
Does user have the appropriate auth.?
YES
Users can access what the programmer has decided; they are allowed to see if they pass all checks.
NO
Possible error message, or data may be filtered to only show tasks that they have access to.
User can access what the programmer has decided they can see if they pass some checks and fails others.
STANDARD AUTHORIZATIONS
STRUCTURAL AUTHORIZATIONS
B
A



This section describes the special authorizations you can define in Personnel Development (PD), in addition to the basic access authorizations discussed in other chapters of this guidebook. When we previously mentioned basic access authorizations, we were referring to the functionality provided by activity groups and their appropriate generated profiles. The authorization profiles control the types of R/3 activities that users can perform.

A profile usually contains a list of authorizations that, for example:

- Controls access to accounting or personnel records
- Dictates which infotypes users can work within R/3
- Is valid across the complete R/3 System

Activity groups and their authorization profiles can be assigned to users, organizational units, jobs, or positions. The relationship between the organizational objects of positions and activity groups can be seen in the relationships infotype (*1001*) with the relationship type of *B007*.

We will not elaborate further on infotype *1016* (standard profiles), because *1016* was originally designed to allow you to link manually created profiles to a position, organizational unit, or job. With the PG, the activity group (after having authorizations assigned to it) is generated. When it is generated, it creates profiles. Now these profiles it creates are **not** the same as manually created profiles even though you can still see them in *SU03* (profile maintenance). But they cannot be maintained anywhere else except in the particular activity group. As such, infotype *1016* does not serve its original purpose and is not treated the same way.

It is not a prerequisite that you use infotype *1016* in order to use infotype *1017* (PD profiles).

Infotype *1017* allows you to create and maintain structural authorization profiles. The purpose of structural authorization profiles is to restrict access to particular objects in PD. These structural authorizations are more restrictive than what standard authorizations offer as they only restrict based on object type.

Structural authorization profiles control both the objects PD users see and the activities PD users undertake when working with organization plans. A structural authorization profile contains a list of authorizations, plus anything else listed in the profile. You may include an unlimited number of authorizations in one profile and append structural profiles to organizational units, positions, jobs, or tasks (or standard tasks, if your company uses Workflow).

The following example explains how structural authorizations can be used.

Example I

Company A hires people throughout the world. Each office manages its own operations. Each office decides whether new positions are created, changed, or discontinued. As such, each office must have the ability to create and change positions (for example, increase the pay of a position) in the R/3 System. However, an office is not to have access to create or change positions for another office.

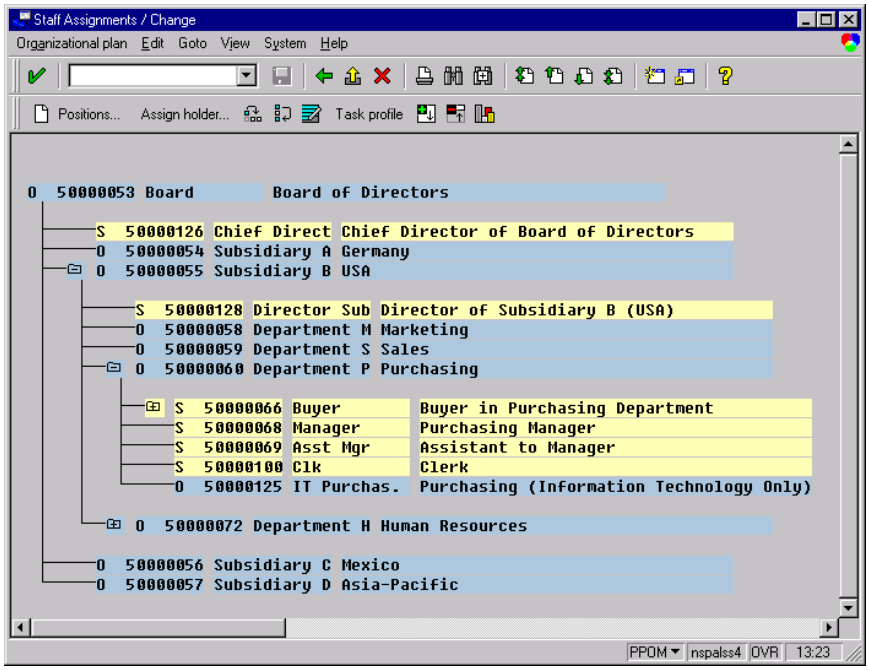
In this case, it is possible (based on company A's configuration) that the standard authorization object PLOG may not be sufficient to provide the restrictions that company A now desires. Structural authorizations can be used to address this type of restrictiveness. (If not, HR may need to be configured enough to allow such authorizations to work without having to use structural authorizations.)

Standard authorizations can distinguish which users have access to positions, but not which "particular" positions. Structural authorizations are implemented in addition to the standard authorizations to determine which particular positions are accessible.

Another way structural authorizations can be used is as follows.

Example II

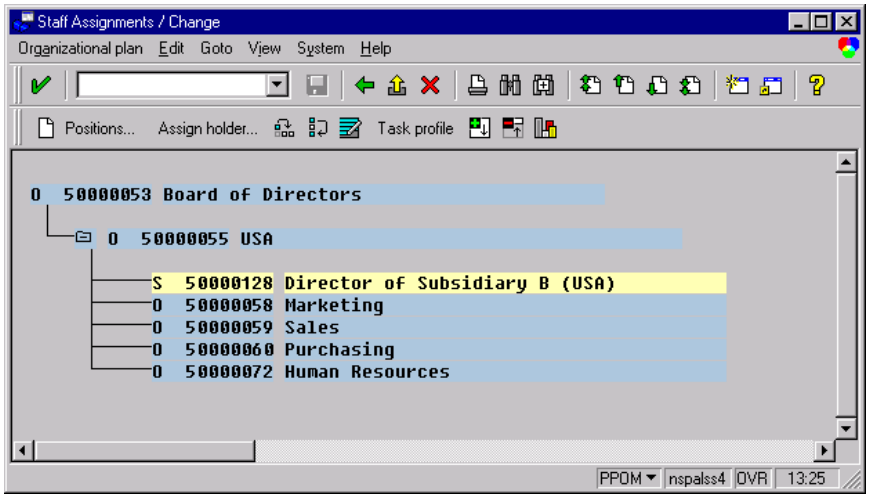
Imagine the following organizational structure as show to the right.



Note that:

- *O* represents an organizational unit
- *S* represents a position

Now imagine we want to give access such that a user can only see a portion of the organizational structure and maintain only the portion he can see. As in this screenshot, such a user would only be able to see the *USA* organizational unit and organizational units that **directly** report to the *USA* organizational unit. Furthermore, they should only be able to see positions that report directly to the *USA* organization.



Such filtering of what can be seen and maintained is what structural authorizations provide. As we will see, although users can view these organizational units, they can only maintain some.

In the example below, we want the user to be able to maintain the organizational unit *USA* and those that report directly to it, but not the organizational unit *Board of Directors*.

To use structural authorizations you need to:

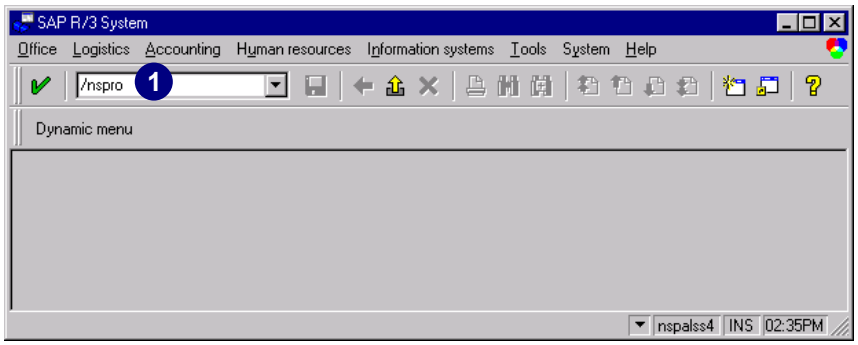
1. Maintain structural authorization profiles in the IMG (can be accessed via table *T77PR*).
2. Link the structural authorization profiles to an organizational object (a position for example via infotype *1017*).
3. Run the program ***RHPROFL0*** (that determines which user master records will be effected).

In the following steps, we show which structural authorizations are delivered with the R/3 System, as well as how to create new ones.

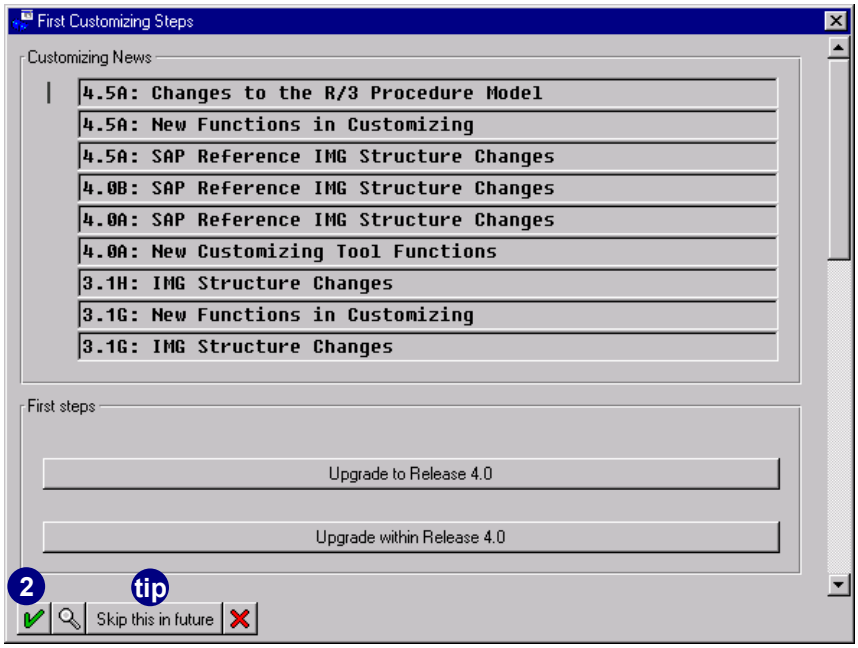
Maintain Structural Authorization Profiles

You can define the structural profiles and set these profiles up in *Customizing* with the Enterprise IMG.

1. In the *Command* field, enter transaction **SPRO** and choose *Enter* (or choose *Tools* → *Business Engineer* → *Customizing*).



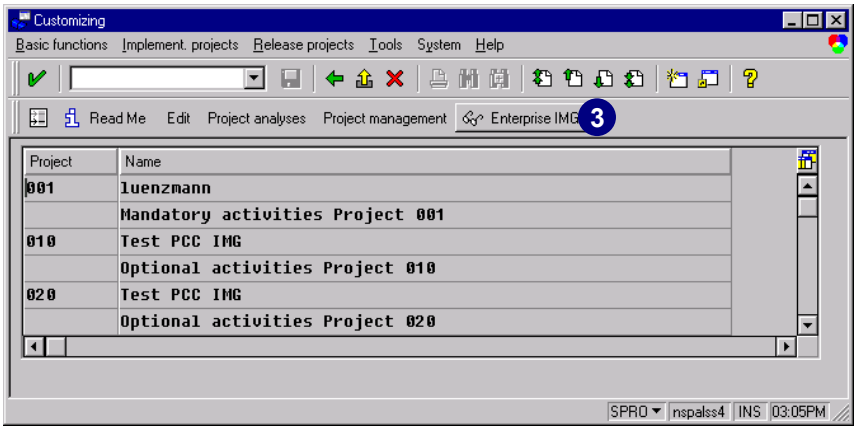
2. Choose *Continue*.



If you have already read the *Customizing News* or do not want to see this screen each time you enter the IMG, you can choose *Skip this in future*. The news can be read later on.

If you have not generated the Enterprise IMG, you must do so before proceeding.

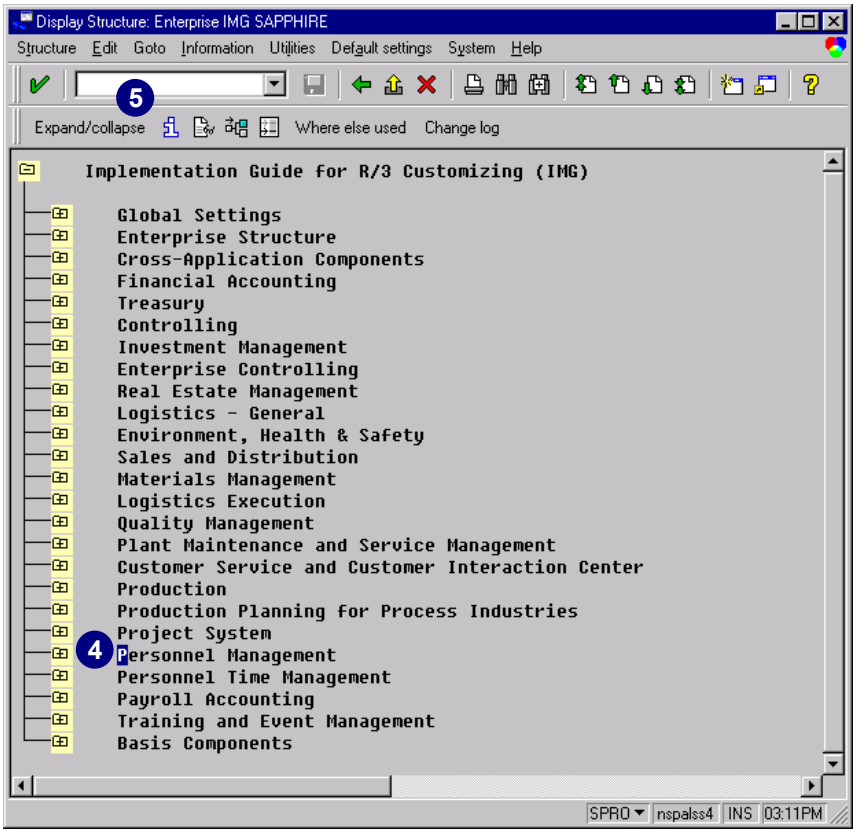
3. Choose *Display Enterprise IMG*.



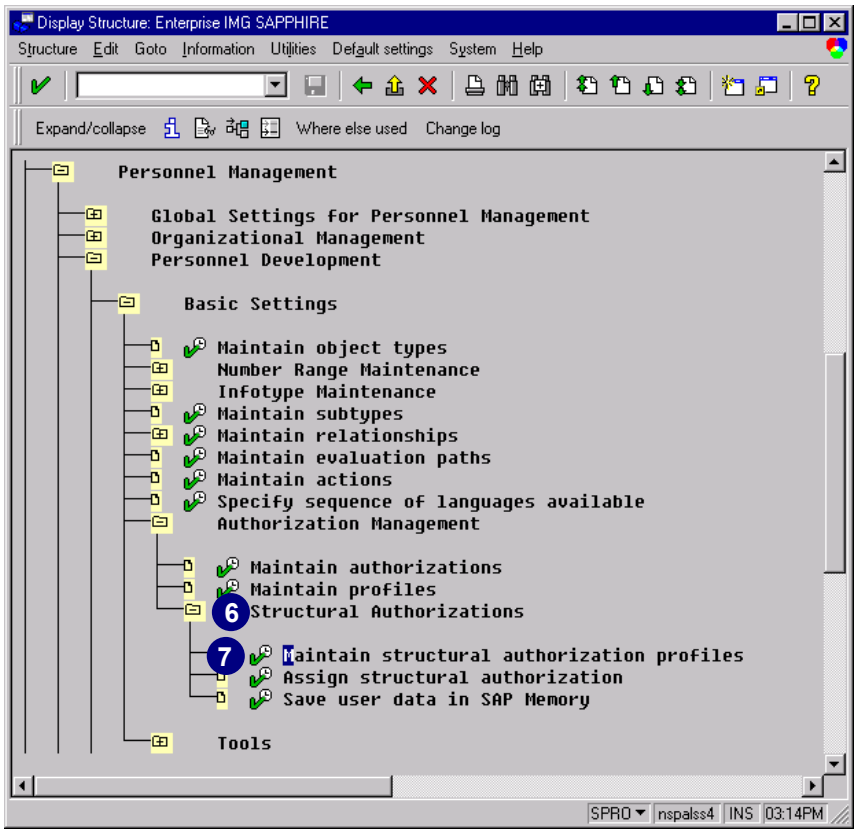
This sample Enterprise IMG may differ from your Enterprise IMG.

4. Select the *Personnel Management* line.

5. Choose *Expand/collapse* or click the node in front of the desire category to expand the hierarchy.

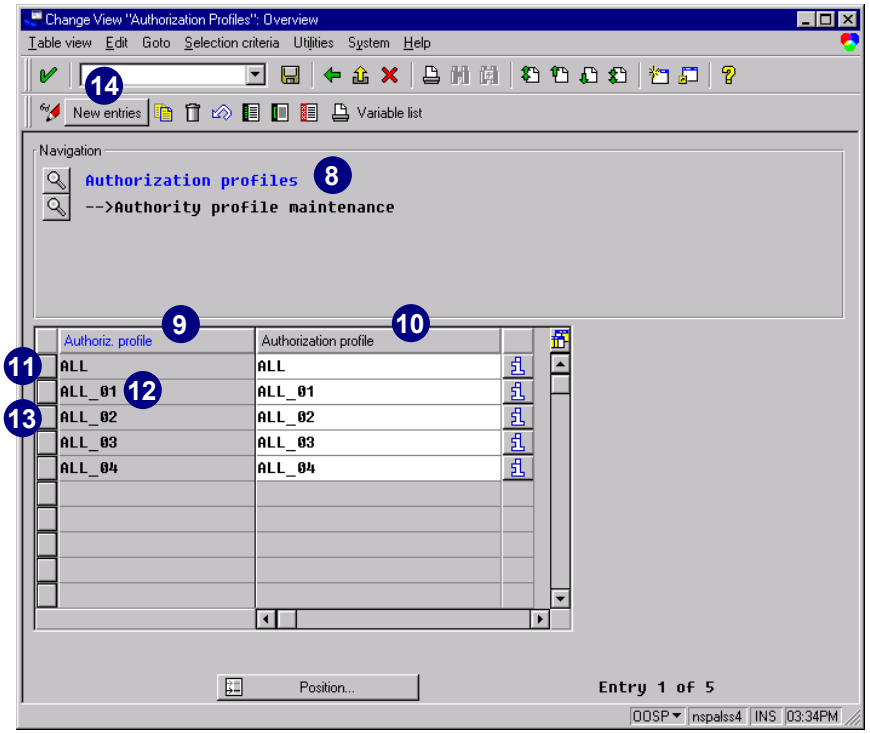


6. Expand the hierarchy down to *Structural Authorization*. Use the path *Personnel Development* → *Basic Settings* → *Authorization Management* → *Structural Authorizations*.
7. Choose *Execute* next to *Maintain structural authorization profiles*, or enter transaction **OOSP** and choose *Enter* .



You are now in *Change Mode* for maintenance view of structural authorization profiles.

8. The *Authorization profiles* button under *Navigation* shows the list of existing structural profiles in your system. SAP delivers, as a default, five structural profiles (those that begin with *ALL*).
9. The *Authoriz. Profile* column shows the technical name of the structural profile.
10. The *Authorization profile* column shows the long text of the structural profile.
11. *ALL* allows users to view all objects in all plan versions that may exist in the system, and gives them ability to perform all the activities for PD objects in these plans.



12. *ALL_01* allows users to view the objects in plan version *01* and perform all the activities with PD objects in this plan.
13. *ALL_02* allows users to view the objects in plan version *02* and perform all the activities with PD objects in this plan.
14. To create a new structural profile, choose *New entries*.

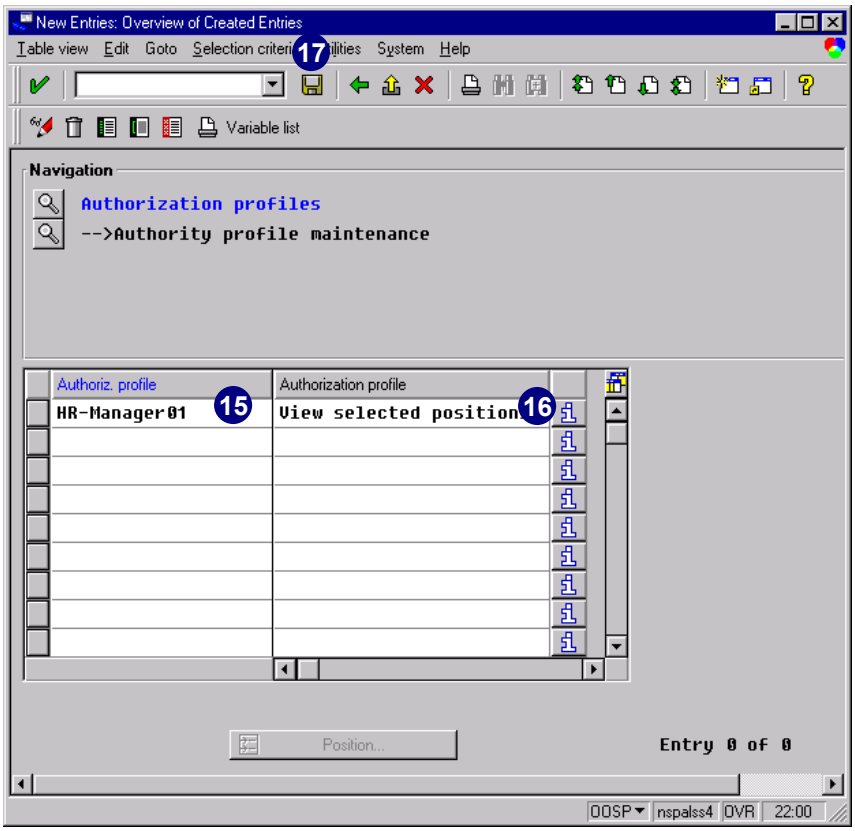
Do not get confused by the use of the word "authorization profile." It has **absolutely nothing** to do with the word "authorization profile" as used in the rest of the system.

First give your structural authorization profile a name:

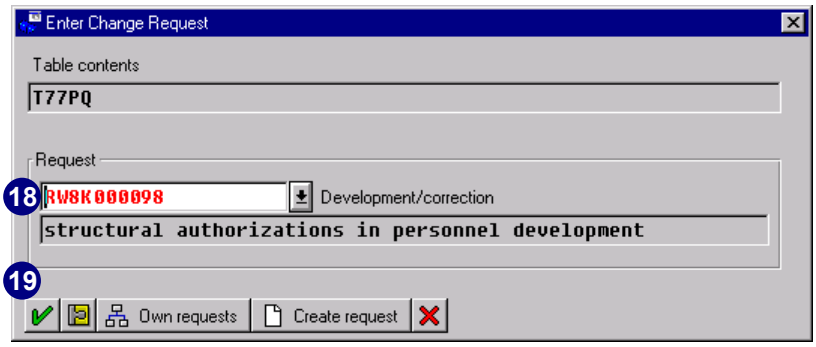
15. Enter the technical name for the structural profile in *Authoriz. Profile*.

There are no restrictions on the *Authoriz. Profile* technical name, but you would be wise to create a good naming convention for your company.

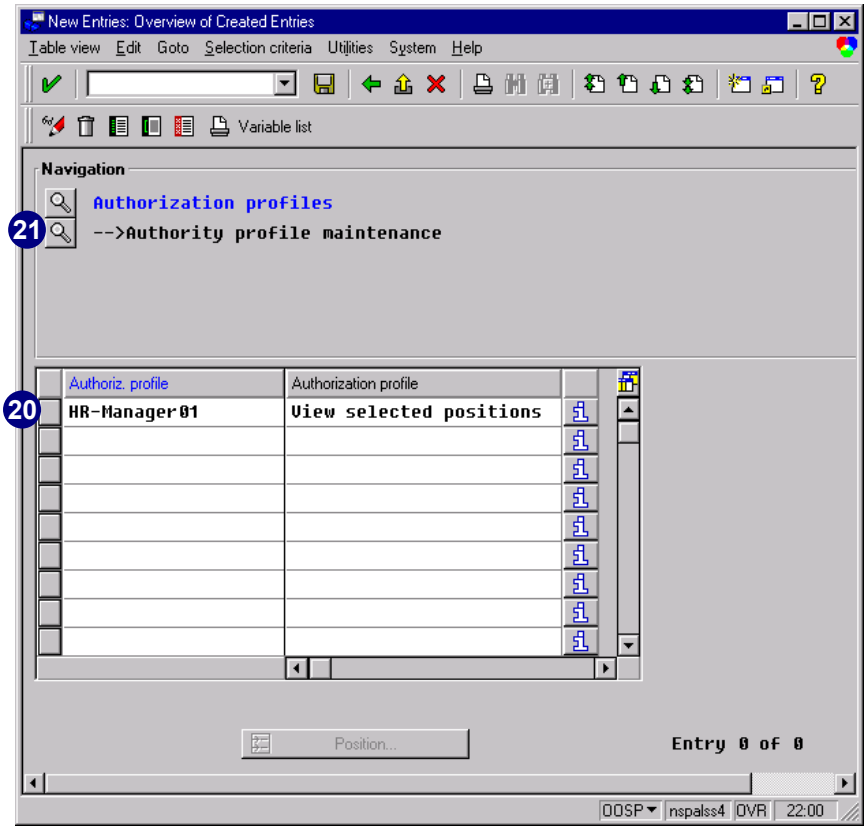
16. Enter a descriptive text for the new structural profile in *Authorization profile*.
17. Choose *Save*.



18. Enter your change request name in *Request*.
19. Choose *Continue*.

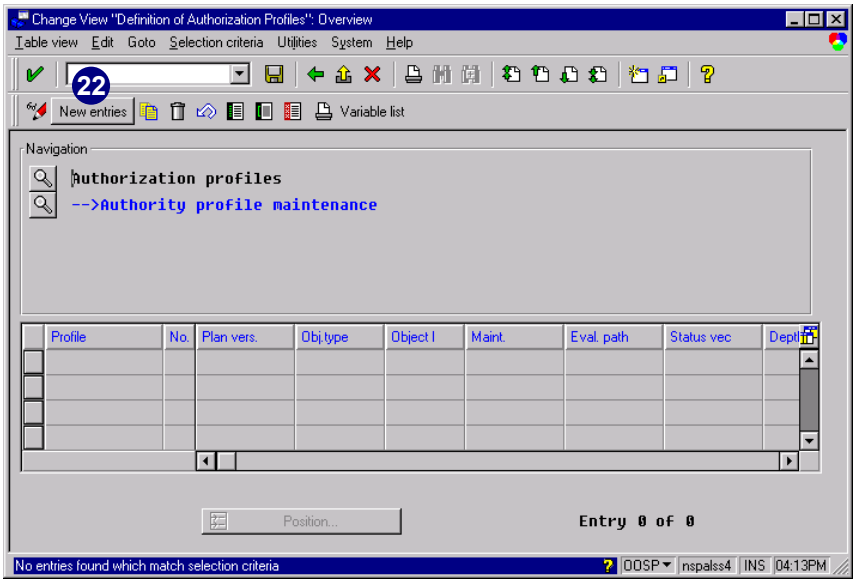


20. Select the new profile.
21. Choose *Detail Level* next to *-->Authority profile maintenance*.



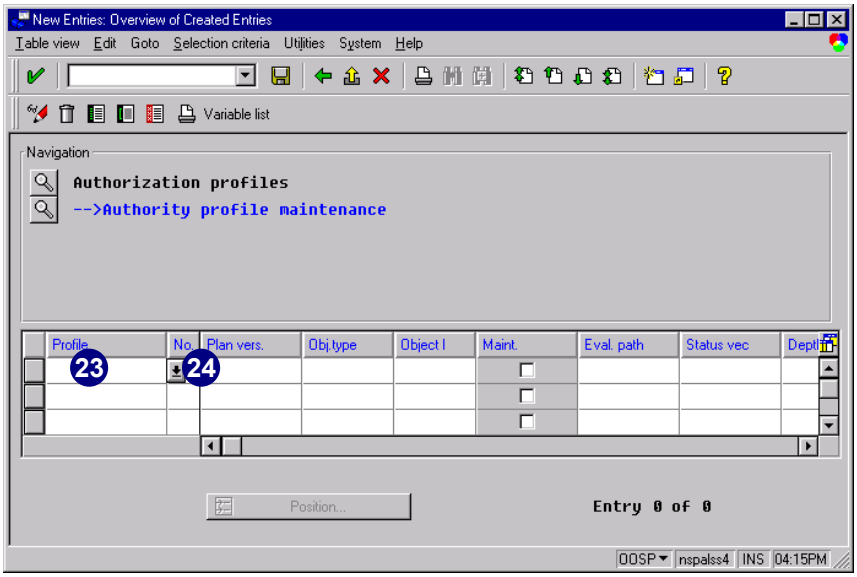
22. Choose *New entries*.

    On this screen, we define for what particular object this structural authorization profile gives access.

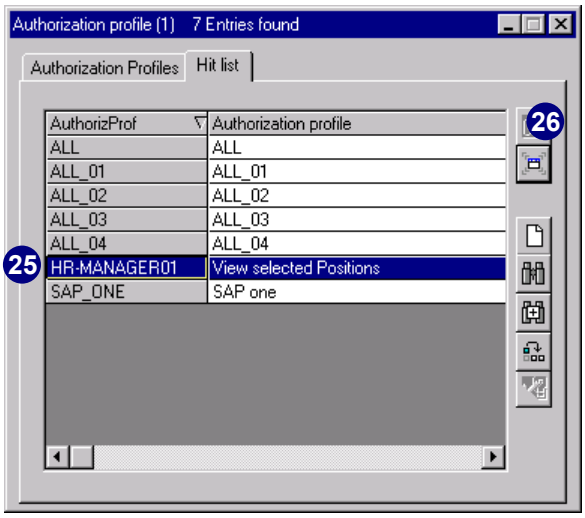


23. Place the cursor in the *Profile* field.
24. Choose *possible entries*.

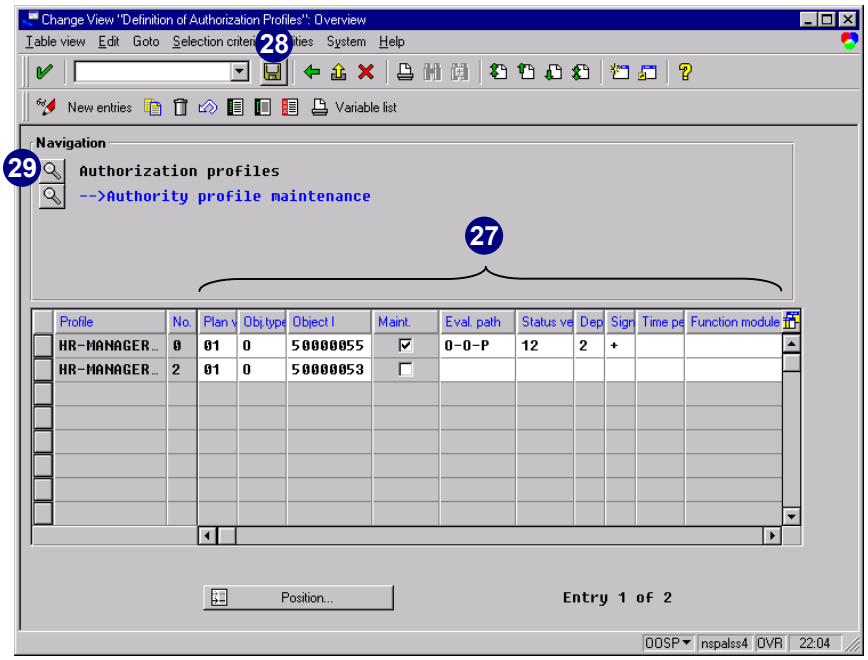
    Make certain you choose the same name as in the step before.



25. Select the new structural profile from the list.
26. Choose *Copy*.



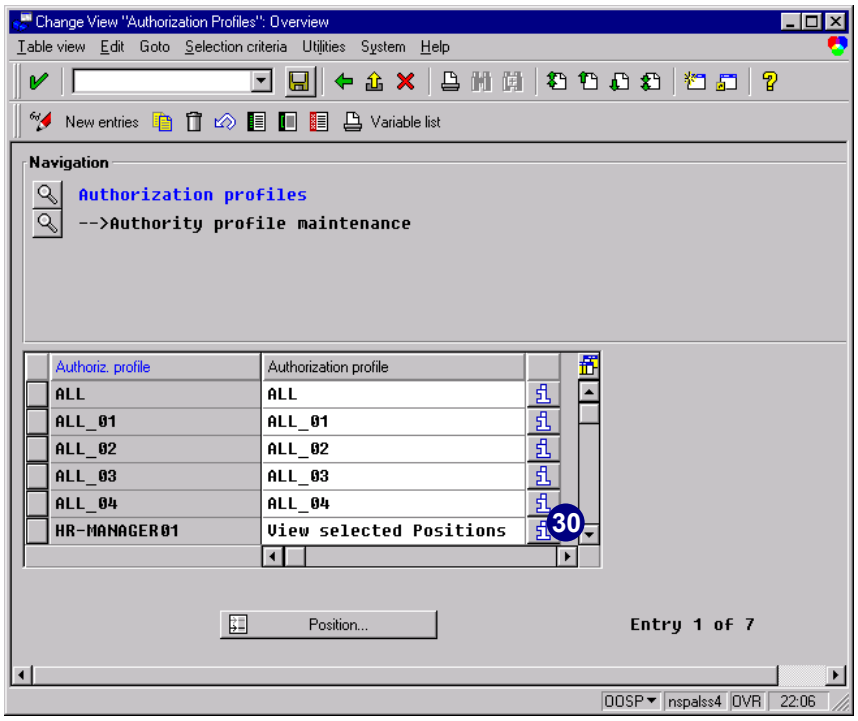
27. You can now define the structural authorization for the following areas:
    - *Plan version*
    - *Object type*
    - *Object ID*
    - *Maint.*
    - *Evaluation path*
    - *Status vector*
    - *Depth*
    - *Sign*
    - *Time period*
    - *Function module*
28. Choose *Save* to process the *Change Request Query* window.
29. Choose *Authorization profiles*.



Area	Explanation
Evaluation paths	You can specify an evaluation path to determine that users are only authorized to access objects along a certain menu path. When you use an evaluation path, you must complete the object ID field.
Status vector	You can specify a status vector to determine that a user only has access to objects whose relationship infotype records have a particular status, for example, planned or active status. (*12* means, in this case, one and two and not twelve.)
Display depth	You can specify a display depth to determine what level in a hierarchical structure a user may access.
Sign	The plus and minus signs determine if you go up or down in the structure from a particular point (+/- is equivalent to up/down.)
Time period	The time period determines that a profile is dependent on the validity period of a structure.
Function module	You can specify a function module that dynamically determines a root object at runtime. You also have to specify a plan version and an object type. The advantage of using function modules is that when a root object is dynamically determined at runtime, a user-specific profile is created. While SAP provides only two modules with detail programming, you can create your own. The SAP-standard provided modules are: ▸ RH_GET_MANAGER_ASSIGNMENT (determines as the root object the organizational unit to which the user is assigned as manager via relationship A012). ▸ RH_GET_ORG_ASSIGNMENT (determines as the root object the organizational unit to which the user is assigned organizationally.)

The evaluation paths are maintained in PD configuration and must be understood by your PD person before using structural authorizations (see table *V_T778A*). It is expected that any person that claims to be proficient in HR-PD thoroughly understands the concept of evaluation paths. If not, seriously reconsider the idea of implementing structural authorizations.

30. Choose *Information* to display an overview of the profile's settings.

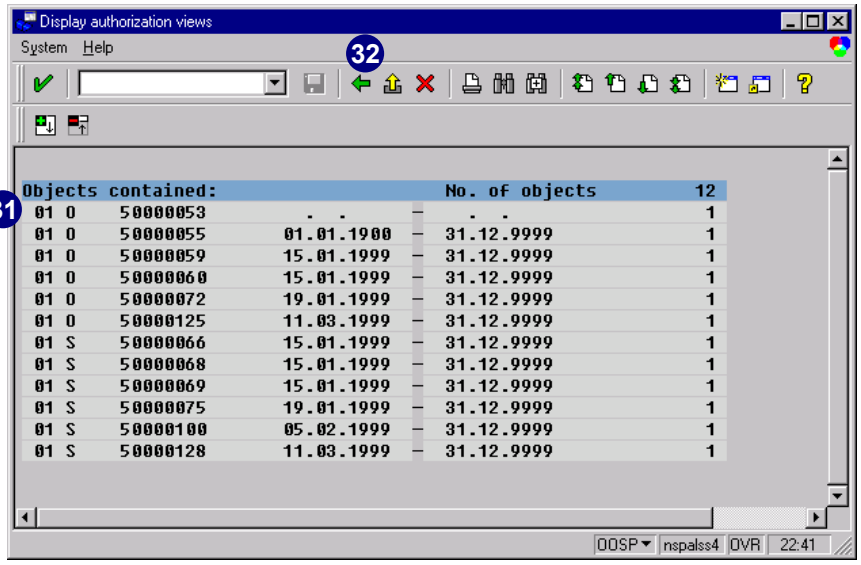


31. The structural profile appears.

    Note that the information displayed is determined dynamically based on the information in the system. For example, if organizational unit *50000058* is deleted now and you choose the *Information* button again, it does not show up on screen.)

32. Choose *Back* to exit the transaction.

    Assigning a structural profile to a position authorizes the position holder to view positions only in that specific plan version.



Assigning Structural Authorization Profiles

You may assign the structural profile(s) to users in one of two ways and place time constraints on such assignments.

These two ways are:

- Method I: Manually (maintaining as table entries in customizing)
- Method II: Report execution which maintains the customizing table for you (customizing production system).

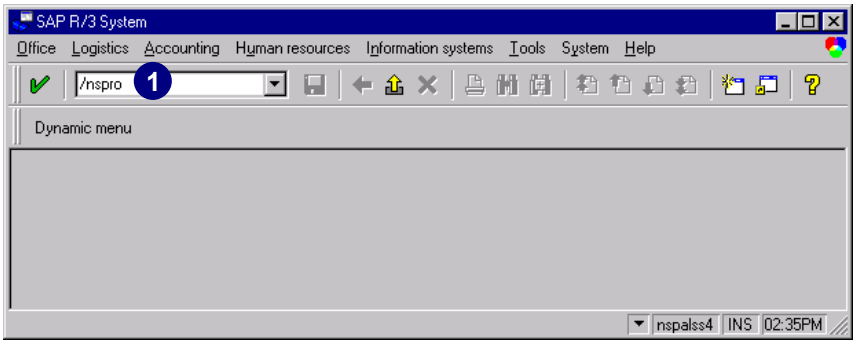
We do not recommend assigning structural profiles the manual way. Manual maintenance affects customizing tables and these tables cannot be changed in a production client. However, if the program *RHPROFL0* is used, this program updates the tables for you in any system without the need of a change request.

Rather than manually assigning structural authorization profiles, maintain the infotype *1017* for a specific PD object, for example, a position. If you run report *RHPROFL0* to later update the user master records, this report creates the required entry in table *T77UA* (the structural profile assignment to the actual position holder).

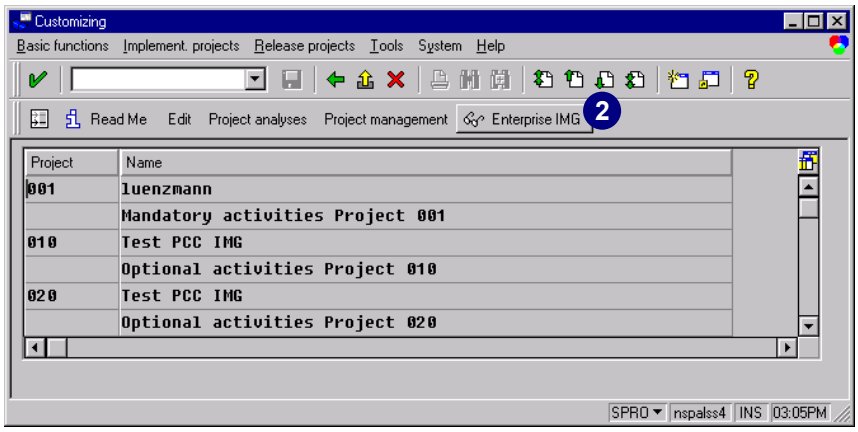
Method I: Assigning Structural Profiles Manually

In the Enterprise IMG , you can manually assign structural profiles in *Customizing*.

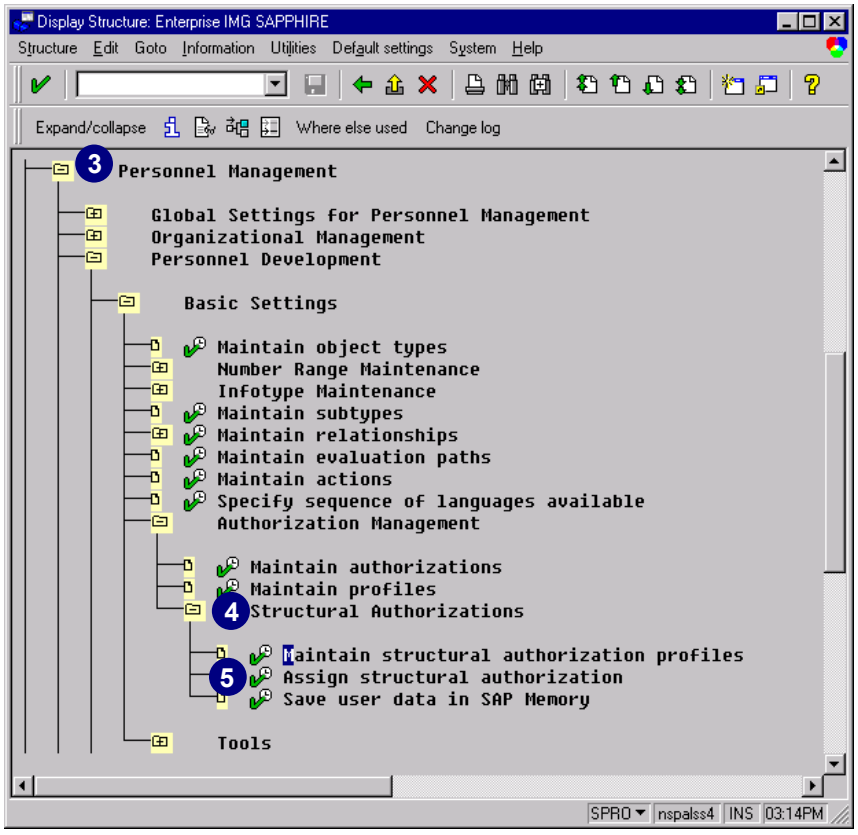
1. In the *Command* field, enter transaction **SPRO** and choose *Enter* (or choose *Tools* → *Business Engineer* → *Customizing*).



2. Choose *Display Enterprise IMG*.

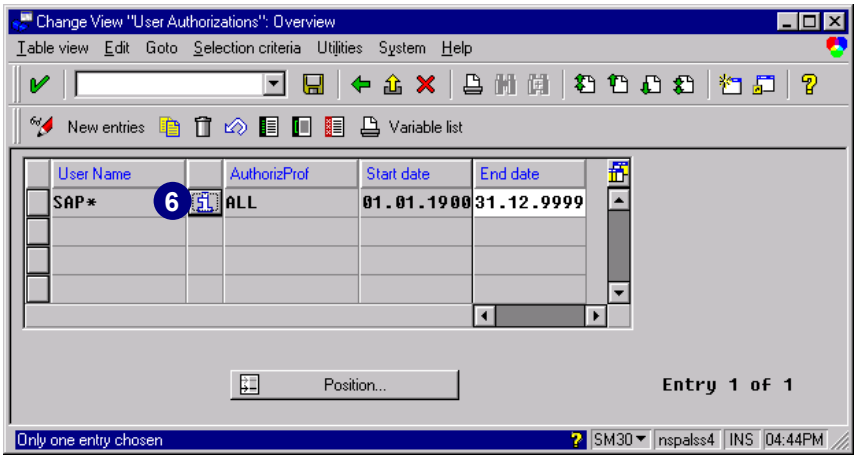


3. Select the *Personnel Management* line and expand it.
4. Expand the hierarchy down to *Structural Authorization*. Choose *Personnel Development* → *Basic Settings* → *Authorization Management* → *Structural Authorizations*.
5. Click *Execute* next to *Assign structural authorization* or enter transaction **OOSB** and choose *Enter* .

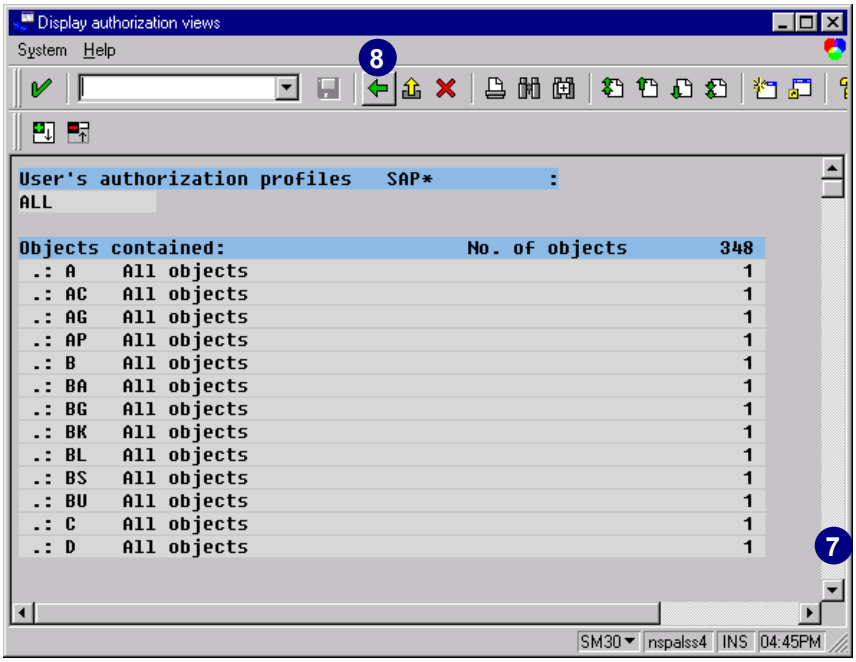


You are now in change mode.

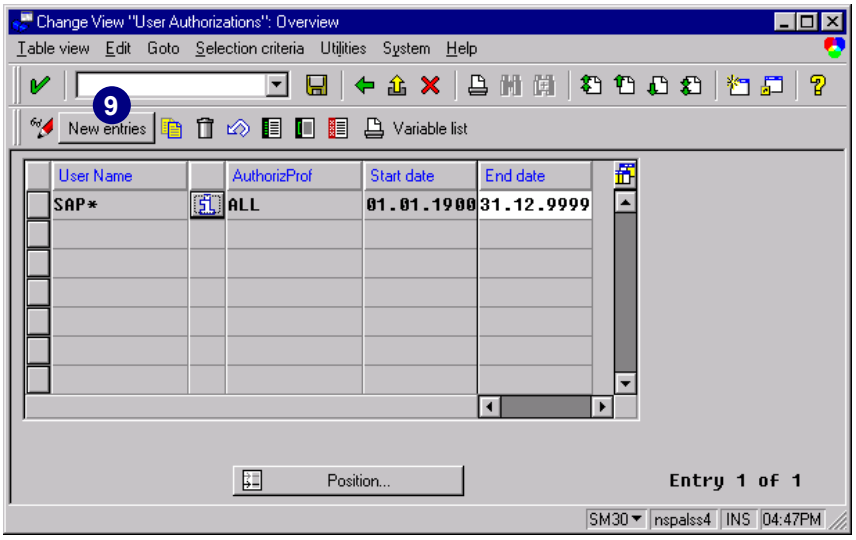
6. Choose *Information* to see what user *SAP** is allowed to view in PD. The system comes standard with *SAP** as the only user listed in this table. Under **no** circumstances should you delete this entry.



7. You can scroll down to see all the values in the list.
8. Choose *Back*.



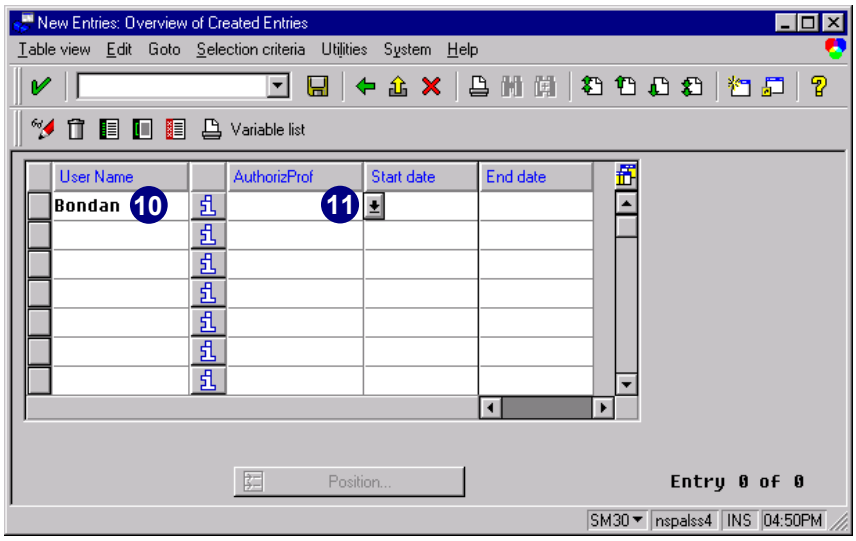
9. Choose *New entries*.



10. Enter a *User Name*.

    As the system does not validate this field on this screen, users not yet created can be assigned here.

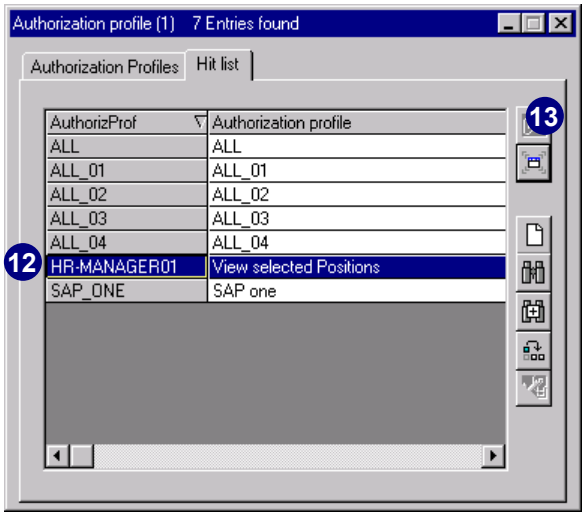
To obtain a list of R/3 users, run transaction **SU01D** in a second session window.



11. Choose *possible entries* in *AuthorizProf*.

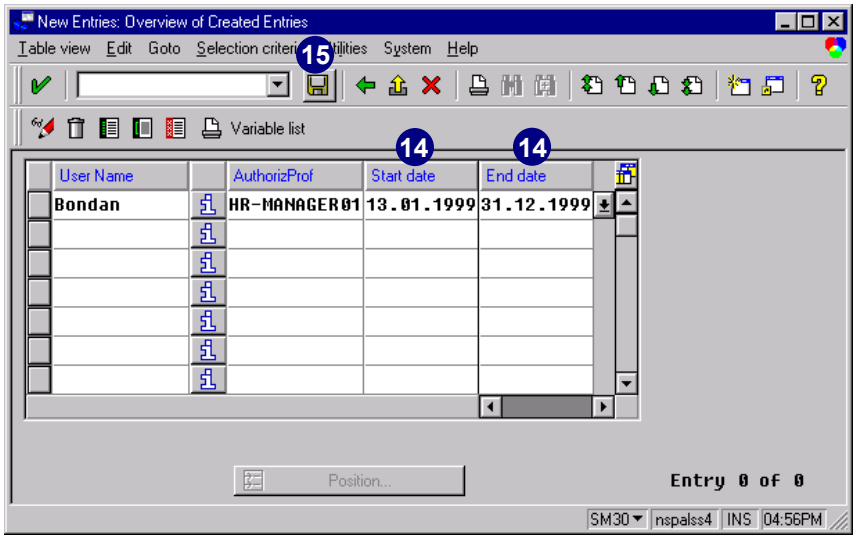
12. Select the appropriate structural authorization profile.

13. Choose *Copy*.

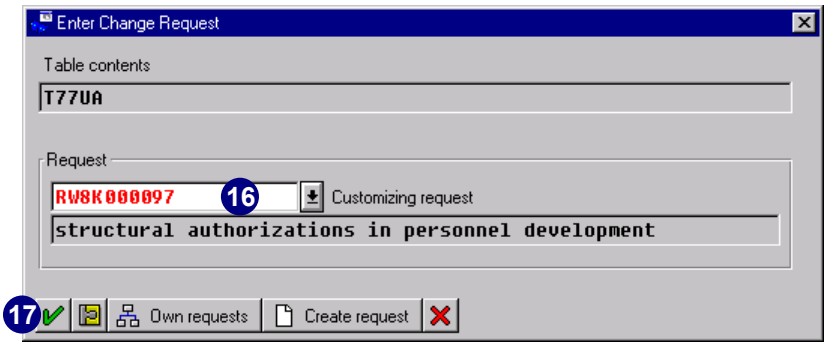


14. To limit the structural profile assignment, enter a start and end date.

15. Choose *Save*.



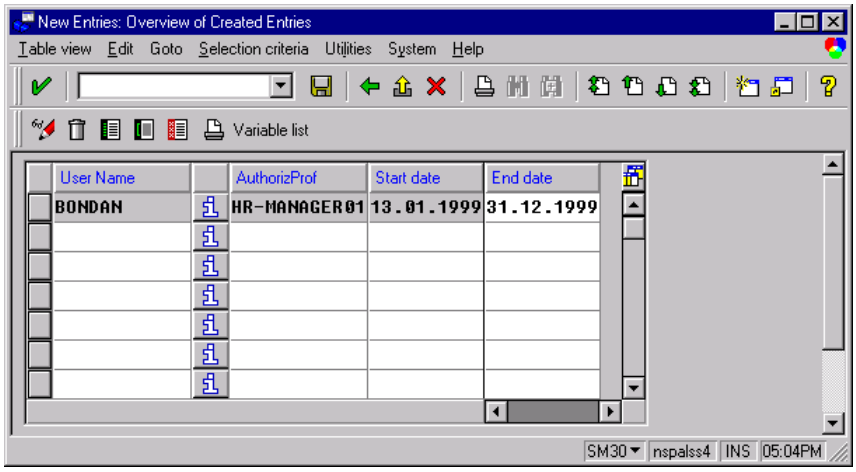
16. Enter a change request name in *Request* or use *possible entries* to select.
17. Choose *Continue*.



Congratulations! You successfully finished this procedure.

Note that a user may exist multiple times in this table during overlapping time periods and different PD structural authorization profiles. In such cases, the user has multiple access for varying periods.

Now, you may either enter names of more users to whom you want to assign structural profiles, or exit this transaction.



Users who are not specified by their user names are treated like user *SAP**. Run transaction **RE_RHAUTH00** to display the authorized objects by user or structural profile.

Method II: Populating Table T77UA Using Program RHPROFL0

In this section, you will learn more about report *RHPROFL0*.

There are two prerequisites before executing this program.

Prerequisites	
Prerequisite 1:	The link between the user login name and the HR-PD object must exist before you get anything meaningful out of this program, for example: a. Position linked to a user b. Position linked to a personnel number c. Other
Prerequisite 2:	The PD object must have infotype *1017* maintained. This maintenance is accomplished via *Human resources* → *Organizational Management* → *Detail maintenance*.

This program creates structural authorization profile assignments for users within an organizational structure. As explained in *Working with Structural Authorizations in PD*, a distinction is drawn between the so-called SAP-standard authorization profiles and structural profiles.

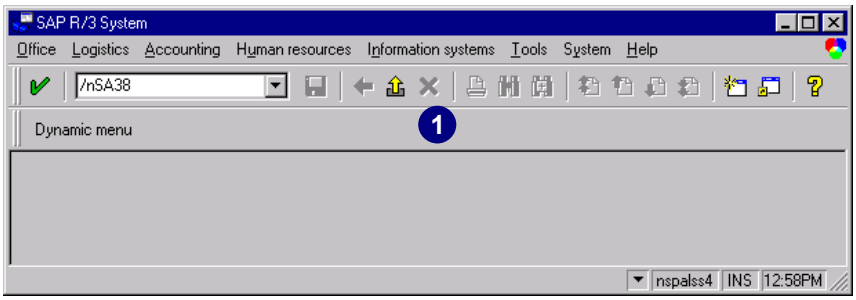
The report evaluates all position holders in the PD organizational structure selected on the selection screen of the *RHPROFL0* report. For each position holder, structural profiles (in infotype *1017*) are read at the respective job, task, or standard task level. The report then generates the corresponding structural profile assignments to the actual position holder (R/3 user).

Integration between Personnel Administration (PA) and PD must be active.

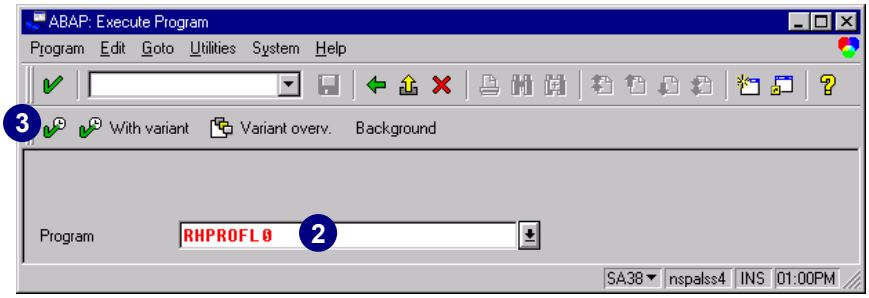
Please remember that the position holder assignment to the system user (R/3 user) must be made in PA. To do this, maintain infotype *0105* (communication) for each position holder in personnel master data. The PA-PD integration switch must be turned on.

To ensure that only valid authorization profiles are in the user master record each day, conduct a daily profile comparison. For the changes in the user master record to be effective, the comparison must be conducted before the user logs on.

1. In the *Command* field, enter transaction **SA38** and choose *Enter* (or choose *System* → *Services* → *Reporting*).



2. Enter **RHPROFL0** in the field *Program*.
3. Choose *Execute*.



Report *RHPROFL0* offers the following options:

- *Dialog Mode*

  With this option, you can first get a list of the appropriate users and choose the *Generate* button, or you may begin process generation and get the list later.

- *Standard Authorizations* (infotype 1016)

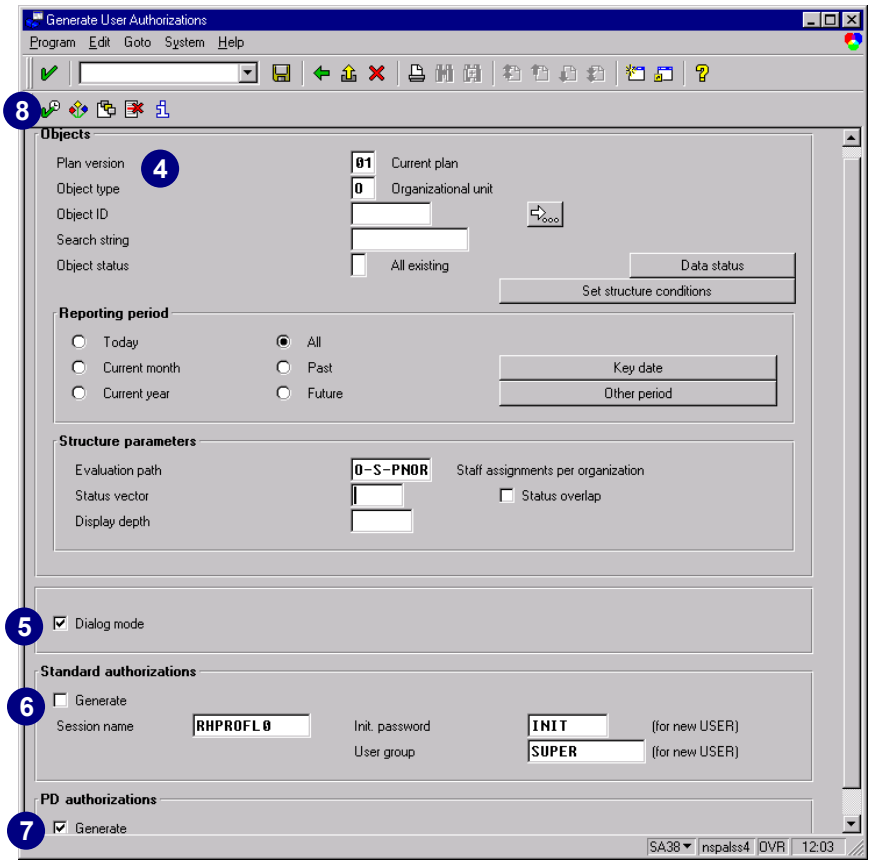
  We do not discuss infotype 1016 in this book.

- *PD Authorizations* (infotype 1017)

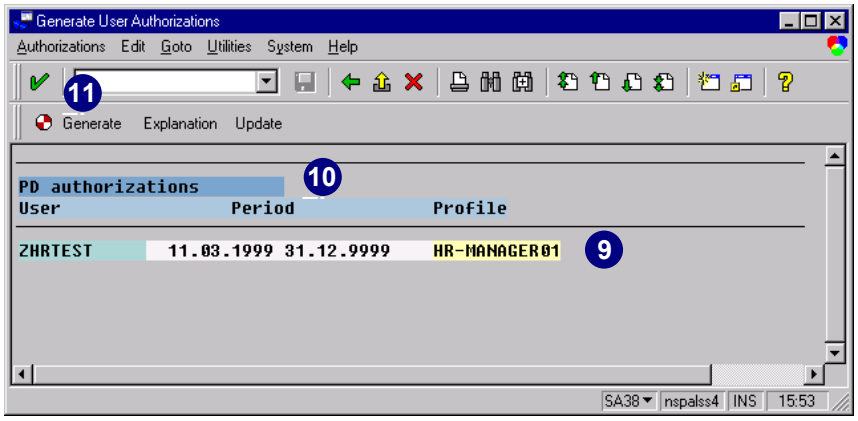
  This option ensures that the report creates all the assignments between the position holders and structural profiles. This process requires that infotype *1017* is maintained for the appropriate position.

4. You may either enter specific evaluation data in the fields within *Objects* or leave the default setting. Press *F1* while the cursor is in a field, to obtain field documentation.
5. Select *Dialog Mode*.
6. Deselect *Generate*.

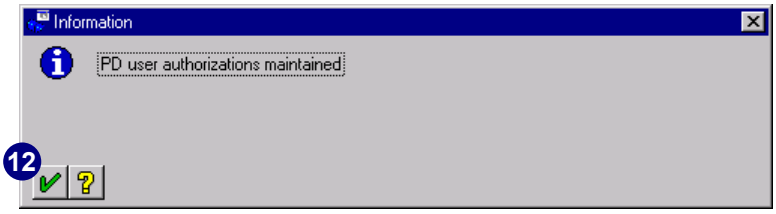
   The field in the *Standard authorizations* box are utilized by infotype *1016*, which is not discussed in this book. In previous releases, infotype *1016* served much of the same purposes as the PG does today. Its usefulness today has been overshadowed by the PG.
7. Select *Generate*.
8. Choose *Execute*.



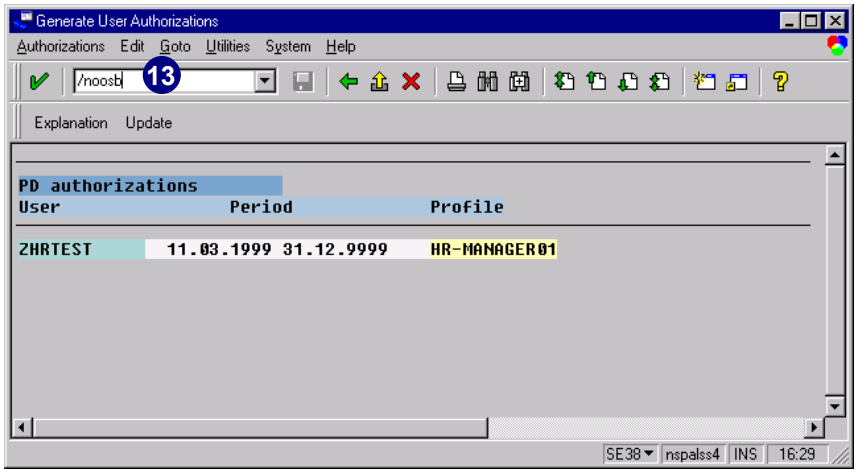
9. As mentioned eariler, certain prerequisites are needed before running this program in order to receive output as that shown here. Specifically, we linked the PD object to a structural authorization profile that, in turn, was somehow directly or indirectly linked to a logon user ID (we linked organizational unit *50000055* to the structural authorization PD profile called *HR-MANAGER* via infotype *1017*). A position in this organizational unit was, in turn, linked to a user called *ZHRTEST*. Therefore, when the report was executed, it identified that the assignment between the structural profile and the actual holder (user id) needed to be created. The actual R/3 user assigned was *ZHRTEST*.



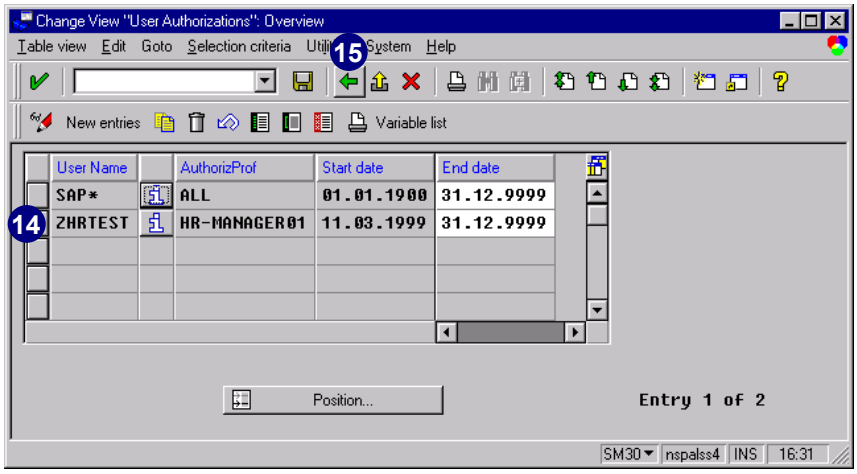
10. The result appears under *PD authorizations* on the screen.
11. If you agree that this user is to receive this structural authorization, then choose the *Generate* button. Choosing *Generate* places this entry in table *T77UA* (the table discussed in the previous section with transaction *OOSB*).
12. A popup window appears informing you that the system has updated the information in table *T77UA*. Choose *Continue*.



13. To see for yourself that the program worked successfully, enter transaction **/nOOSB** in the *Command* field.



14. You now see the entry created for user *ZHRTEST* with the structural authorization profile *HR-MANAGER01*.
15. Choose *Back* to exit.



Integration: Linking Logon Names to Personnel Numbers and Positions

Access security setup extends from the hiring process until the new person associated with the personnel number logs on to R/3. This section assumes that you work with the Profile Generator (PG), HR-Organizational Management, and HR-Personnel Administration.

At this point, we assume that the following tasks have already been completed:

An organizational plan for your company has been maintained

Jobs, positions, org units, etc., have been created

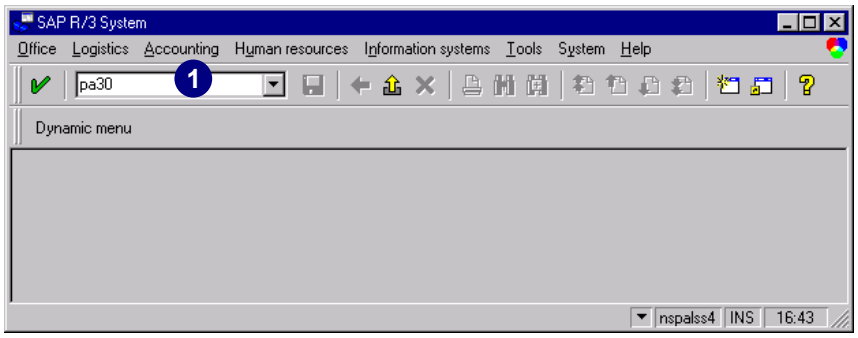
Activity groups have been created and the appropriate authorization profiles generated

Activity groups have been assigned to organizational units, jobs, or positions

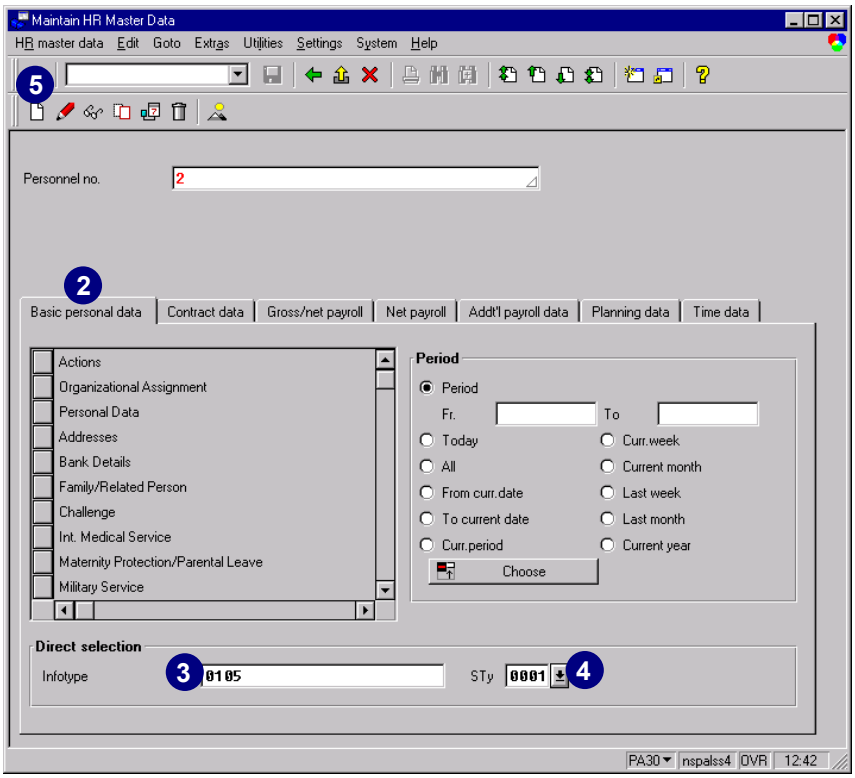
A personnel number exists (this is accomplished through HR functionality such as the hiring event and it is not discussed in the *Authorizations Made Easy* guidebook).

The next step is to:

1. In the *Command* field, enter transaction **PA30** and choose *Enter* (or choose *Human Resources* → *Personnel Management* → *Administration,* then *Maintain Master Data*).



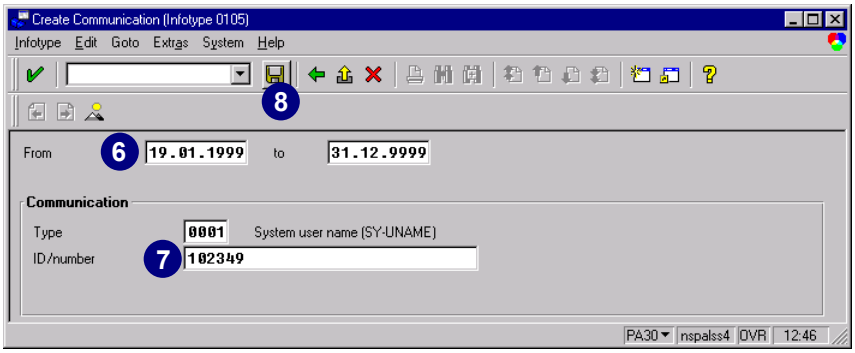
2. Choose the *Basic personal data* tab.



If you are implementing HR, please speak with the appropriate members of your HR team before changing any data with this transaction. This transaction is very powerful and the *Period* section on this screen needs to be considered before changing/creating the information as shown below.

3. Enter **0105** in the *Infotype* field. This infotype is known as the "communication infotype." What it does is link (or set up the communication between) the HR personnel number to the R/3 logon ID user.
4. Enter **0001** in the *Sty* field (which stands for subtype). The subtype designates that the communication being set up is the one for the logon user ID connection.
5. Choose *Create*.

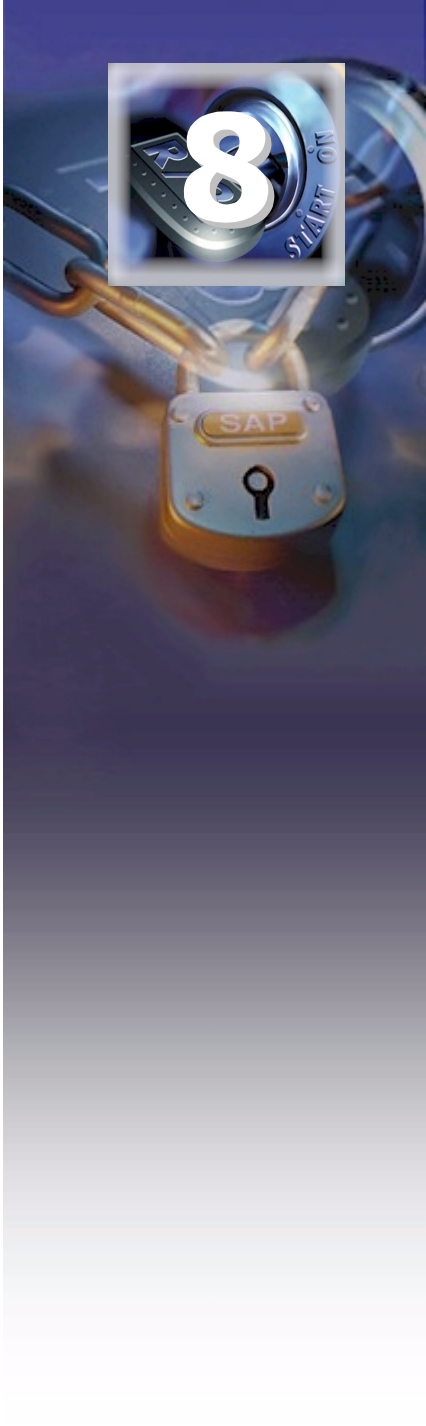
Determine the R/3 user name:



6. Enter the start date for the first R/3 System logon for this user (this is not validated).
7. Enter the user *ID/number* to be created (this number is not validated, as such; you can set up these linkages before actually creating the logon user IDs.)
8. Choose *Save*.

It is a good idea to make your logon IDs identical to your personnel numbers. For example, if a personnel number is *102349*, then the logon ID would also be *102349*. Following this convention will make implementing, monitoring, analyses, and long-term maintenance of the authorization system much easier. Experiences have proven this.

While it is possible to link positions directly to users, it is more realistic that positions get linked to personnel numbers. By performing the steps above, the personnel number is now, in turn, linked to the logon user ID. When the *RHPROFL0* program is run, it picks up the fact that a position contains a personnel number linked to a logon user ID and can now determine to which user ID to give which structural authorization profile. This integration leverages and demonstrates the power of the SAP R/3 System.



Chapter 8: Assigning Activity Groups and Users

Contents

Overview

Depending on the area of the system where you work, assigning activity groups to R/3 objects (such as users, positions, jobs, or organizational units) affects the following areas:

- In Session Manager, these assignments determine the user menu users see when they log on.
- In Business Workflow, these assignments determine the system tasks that a user can perform (for workflow users, it is mandatory to only include tasks in activity groups).
- In Human Resources, these assignments serve as highly detailed object descriptions (for job, position, descriptions, etc.).

The same activity group can be assigned to several different objects. A single object may also be related to several different activity groups. The different activity groups assigned to an object are together referred to as the object's activity profile. The various R/3 objects are:

- **R/3 users –** Object type *US*

  An R/3 user is an individual who is:
  - Recognized by R/3
  - Allowed to log on
  - Allowed to perform specified system activities

  For the system to recognize users, their names must be entered in the Basis component of the user master record.

- **Work center** - Object type *A*

  A work center identifies a location where work is carried out. A location can represent a geographic location, such as the Philadelphia branch office or the Singapore subsidiary, or it can be more precise. For example, it can identify a specific workstation with certain materials and equipment, on a specific floor of a specific building. Work centers can be used with jobs and tasks to create comprehensive job descriptions. The job identifies the job classification, the tasks indicate the types of duties performed, and the work center identifies where the tasks are carried out.

- **Job** - Object type *C*

  A job is a general classification of work duties, such as secretary, computer programmer, instructor, and many employees may hold the same job. (For example, there might be 20 employees known as secretary.) Jobs are normally used to create positions. Anyone who holds a job automatically inherits the infotype settings, attributes, and properties of the job. Unless these groups grant general access rights, such as those required to work with SAPoffice, be careful when assigning activity groups to jobs.

- **Organizational unit** - Object type *O*

  Organizational units represent organizational entities designated to perform a specified set of functions. For example, organizational units represent subsidiaries, divisions, departments, groups, special project teams, etc. Identify the organizational structure at your firm by creating organizational units and identifying the relationships among the

units. An employee assigned to an organizational unit automatically inherits the infotype settings, attributes, and properties of this unit.

Unless these groups grant general access rights, such as printing, be careful when assigning activity groups to jobs. For example, if authority profiles tend to be fairly standard for all workers in an organizational unit, then it may be most effective to assign activity groups and their profiles to organizational units. If exceptions occur, create additional activity groups. If, however, authorities vary by job or position, it may be best to assign activity groups to the specific jobs or positions.

- **Person** - Object type *P*

  A person.

- **Position** - Object type *S*

  A position represents a unique individual employee assignment within a company (for example, the marketing secretary, sales manager, etc.) Positions should not be confused with jobs and are usually created based on jobs. Anyone who holds a position automatically inherits the infotype settings, attributes, and properties of the position. This process allows you to handle authorization management in almost a completely position-oriented fashion. Since all of the access rights are now linked to the position, it does not matter who fills this position. Once a user changes positions, the authorization profile automatically changes after the user master record is updated.

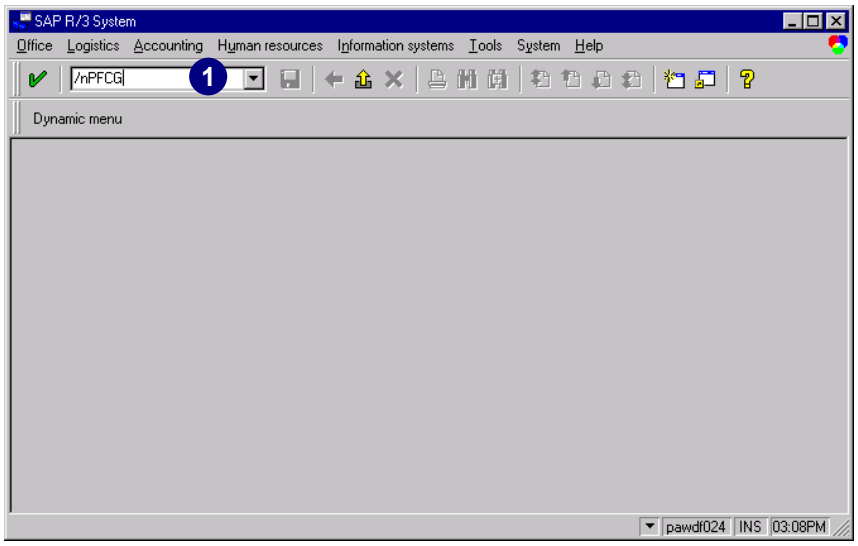
Assigning Activity Groups

Make sure you assign the activity group to the specific position that will receive an authorization profile. If you assign the activity group to a job, all of the positions created from that job will inherit the activity group and its authorization profile(s).

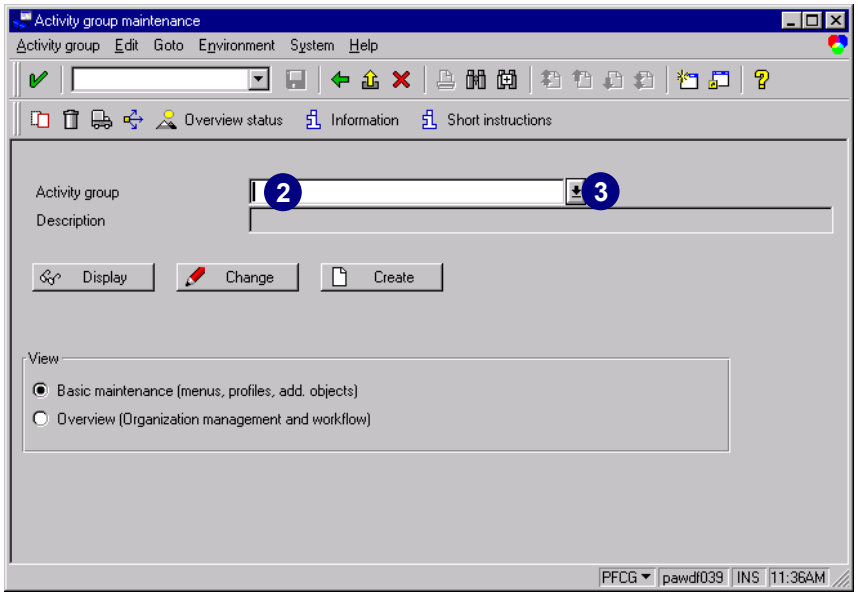
Assigning Users to Activity Groups

Using transaction **PFCG**, verify that the authorization profiles have been generated (the light on the *Authorizations* tab should be green).

1. In the *Command* field, enter transaction **PFCG** and choose *Enter* (or choose *Tools* → *Administration* → *User maintenance* → *Activity groups*).

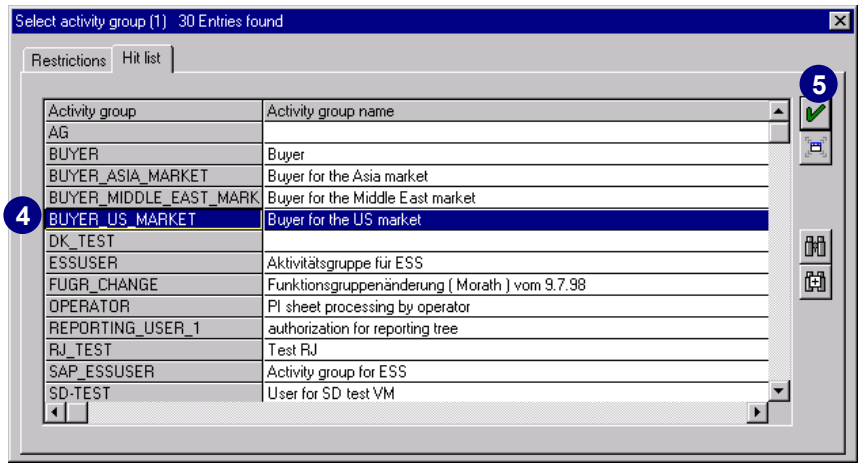


2. Place the cursor in the *Activity group* field.
3. Choose *possible entries*.

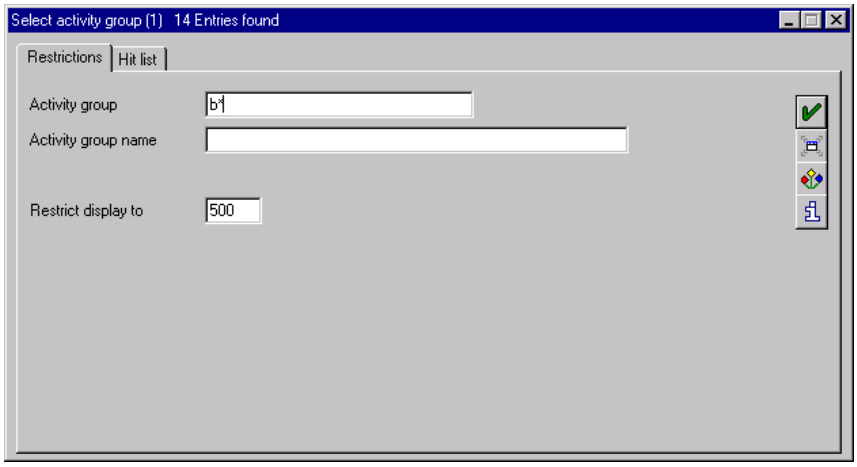


A *Hit list* appears.

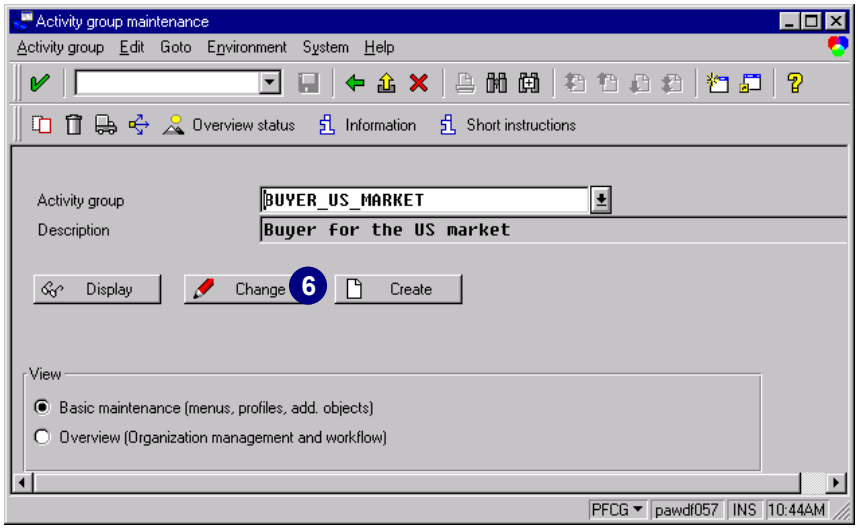
4. Select the activity group you want to edit.
5. Choose *Copy*.



If the *Hit list* is too long, choose the *Restrictions* tab to narrow your search. Enter the first letters of the activity group you are looking for and choose *Start search*.

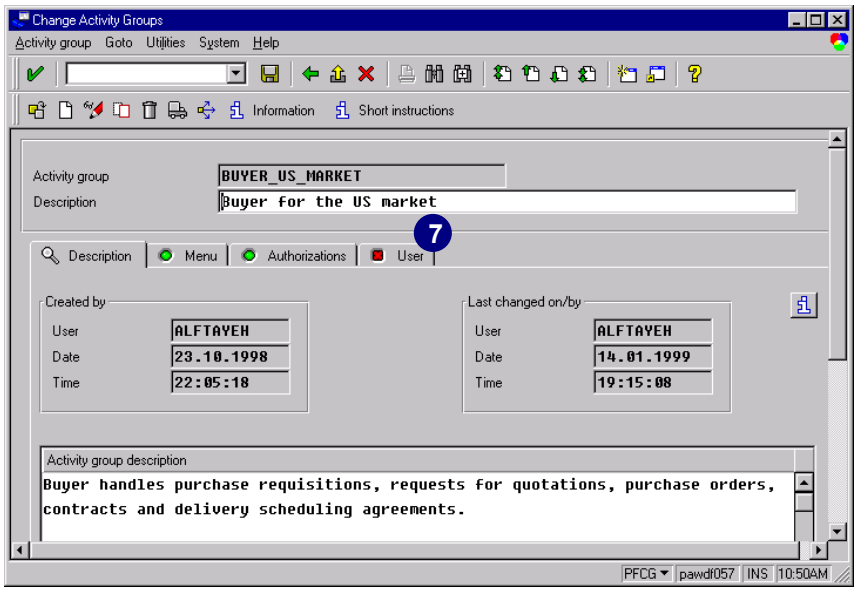


6. Choose *Change* to edit your activity group data.



The *Change Activity Groups* window appears.

7. Choose the *Users* tab to select one or more users to assign to this activity group.

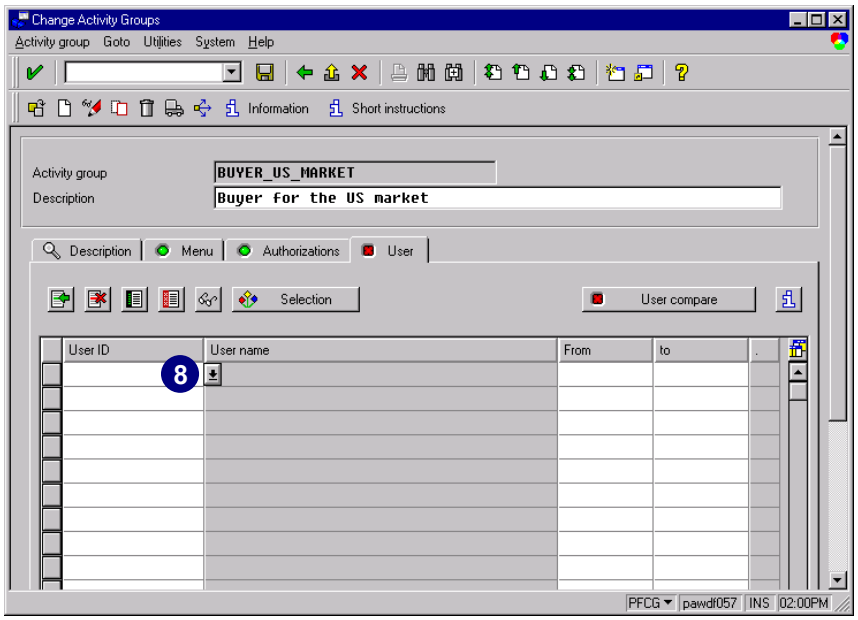


There are different ways to assign the user to the selected activity group:

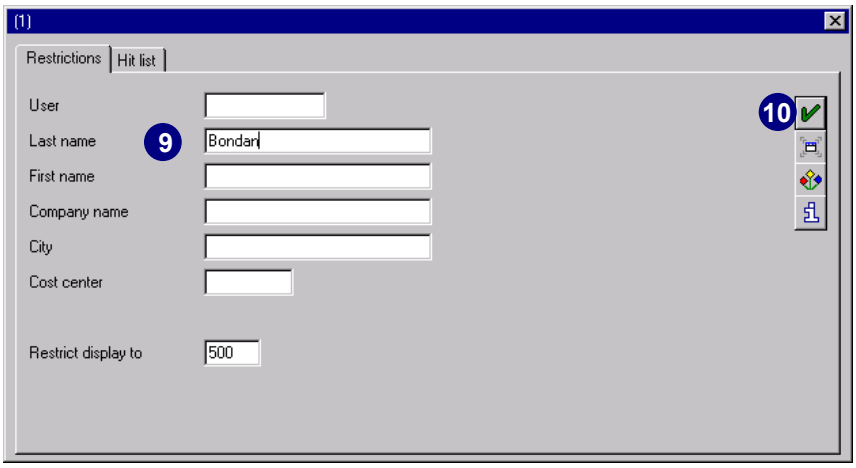
- Typing the user ID directly or making a selection with *possible entries*.
- Selecting from the selection list.
- Using Organization Management.

To enter the user directly, go to step 8; to use the selection list, go to step 13.

8. Choose *possible entries* or enter the user directly.

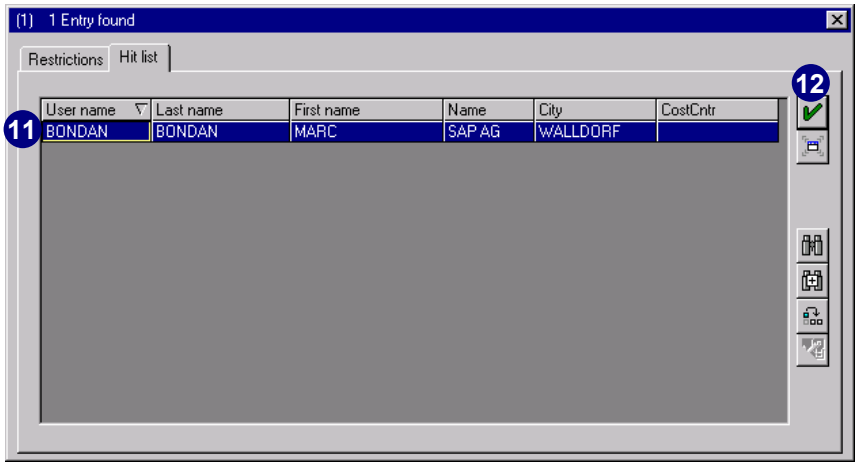


9. Enter an identification for the required user.
10. Choose *Start Search*.

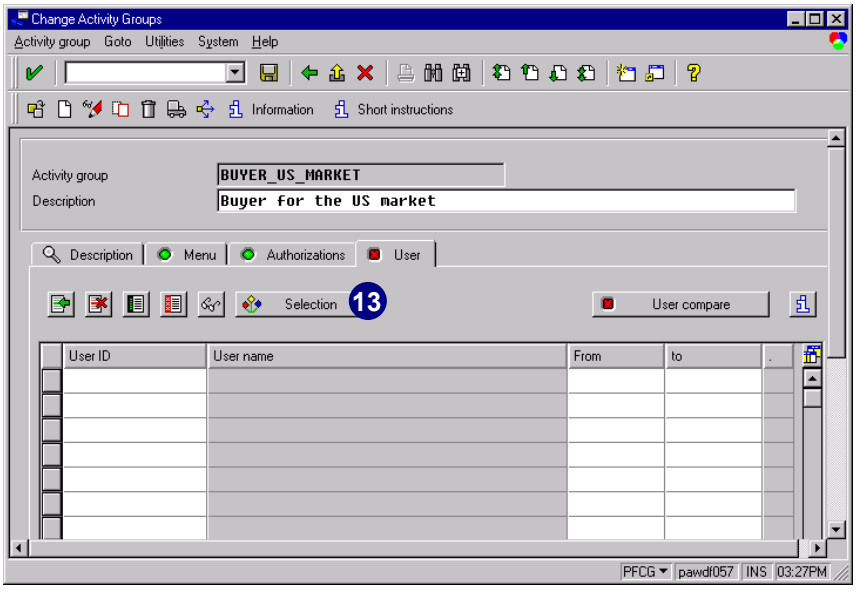


11. Select the user.
12. Choose *Copy*.

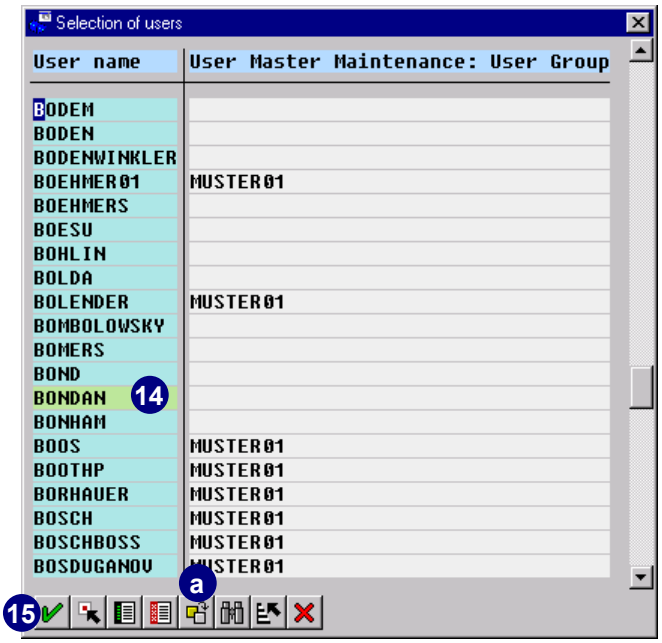
    Continue with step 16.



13. Choose *Selection* to select the user from a selection list.



14. Select the user.
    It is possible to select several users.
15. Choose *Copy*.



If you cannot find the required user or if you want to choose the user through a user group then:

a. Choose *New value selection*.

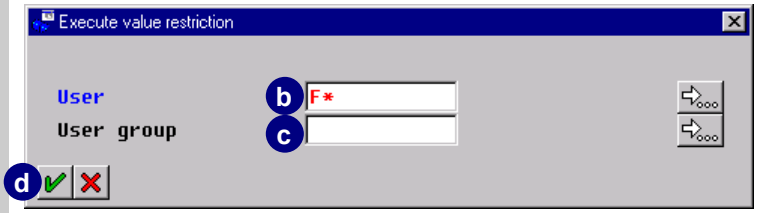
b. Enter the first letter(s) of the user name and an asterisk (*) to expand selection list.

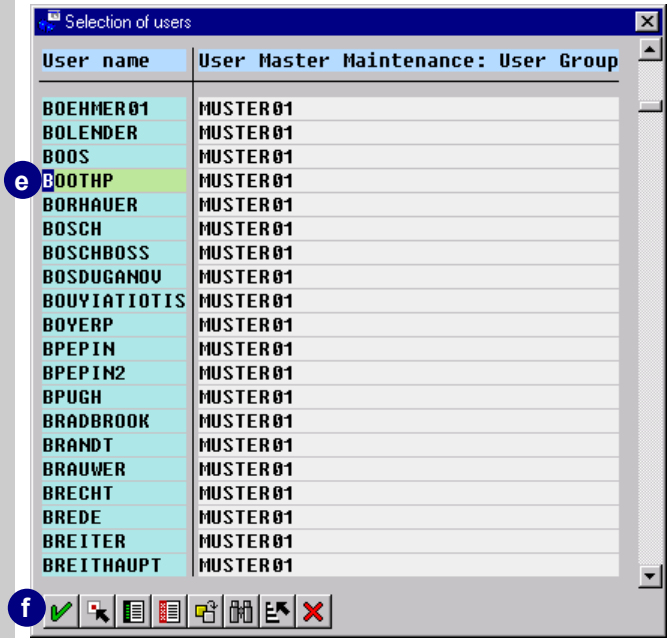
c. To find the user through through their user group, use the *User group* field.

d. After either of the above steps, choose *Continue*.

e. Select the user.
   It is possible to select several users.

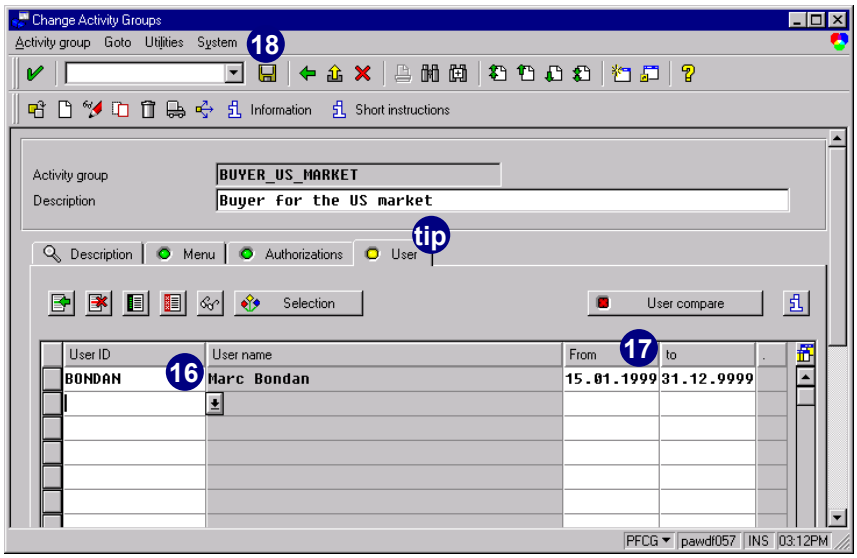
f. Choose *Copy*.





16. The user appears with *UserID* and full name.
17. Restrict the start and end date of the user assignment by entering the required period.

    The system enters by default the currrent date as the start date of the user assignment and *31.12.9999* as the end date.
18. Choose *Save* to secure your selection.



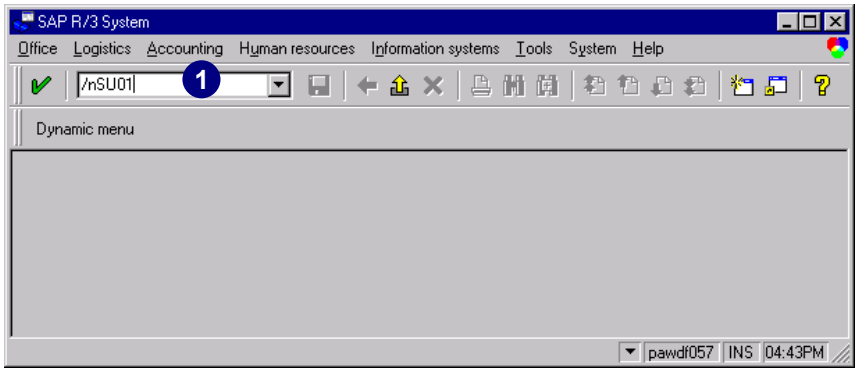
Status Display on the Tab
The status display on the *User* tab displays whether or not users are already assigned to the activity group. If the display appears in red, no users are assigned. If green, at least one user is assigned to the group. If yellow, it means that although users have been assigned to the activity group, the user master record comparison is not current.

Time-Dependency of User Assignment and Authorizations
If you also use the activity group to generate authorization profiles, then you should note that the generated profile is not entered in the user master record until the user master records have been compared. When you specify the users for the activity group, the system defaults to the current date as the start date of the user assignment, and *31.12.9999* as the end date. If you want to restrict the start and end dates of the assignment, for example if you want to define a temporary replacement for a user, the system automatically makes the changes to the user. This automatic adjustment of the user's authorizations is executed by report *PFCG_TIME_DEPENDENCY*. In this case, you should schedule report *PFCG_TIME_DEPENDENCY* daily, for example early in the morning, to run in the background (in transaction **`SA38`**, for example). This report compares the user master records for all activity groups and updates the authorizations for the user master records. The system removes authorization profiles from invalid user assignments and enters authorization profiles from valid assignments.

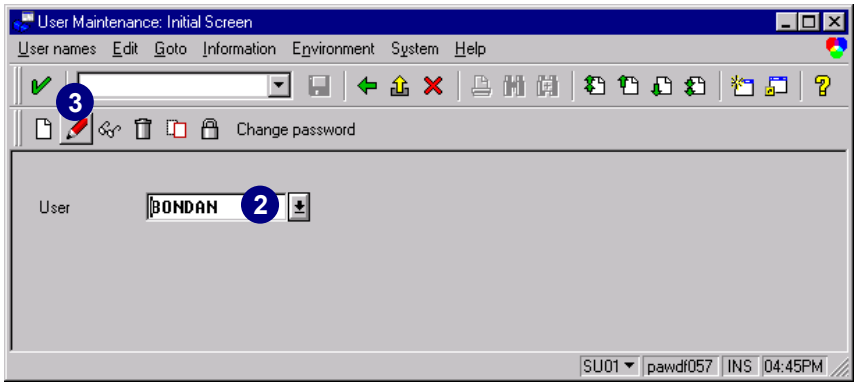
Assigning Activity Groups to Users

You can assign activity groups and their authorization profiles to individual users. Using transaction **PFCG**, verify that authorization profiles have been generated (the light on the *Authorization* button should be green).

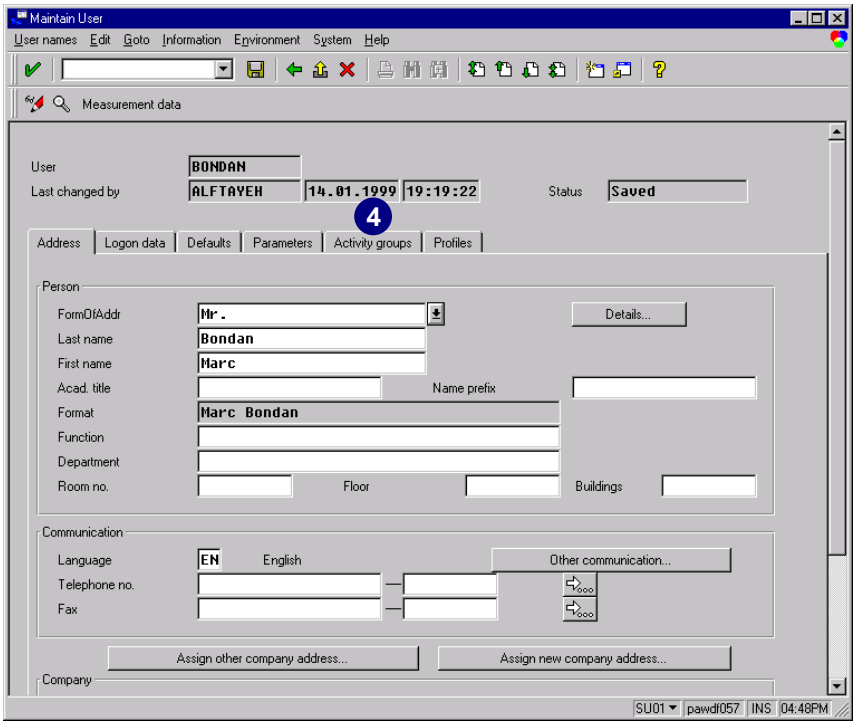
1. In the *Command* field, enter transaction **SU01** and choose *Enter* (or choose *Tools* → *Administration* → *User maintenance* → *Users*).



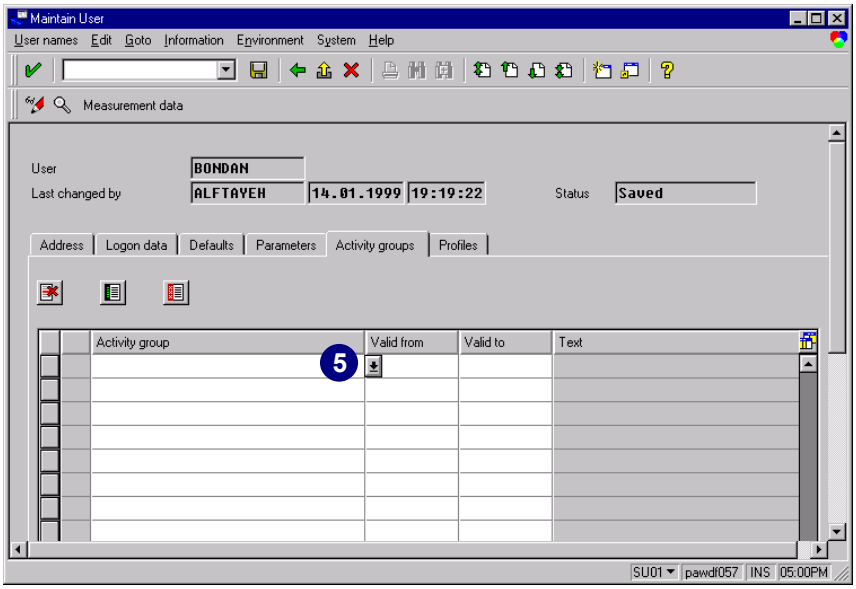
2. Enter the user name for whom you would like to assign an activity group, or use *possible entries*.
3. Choose *Change*.



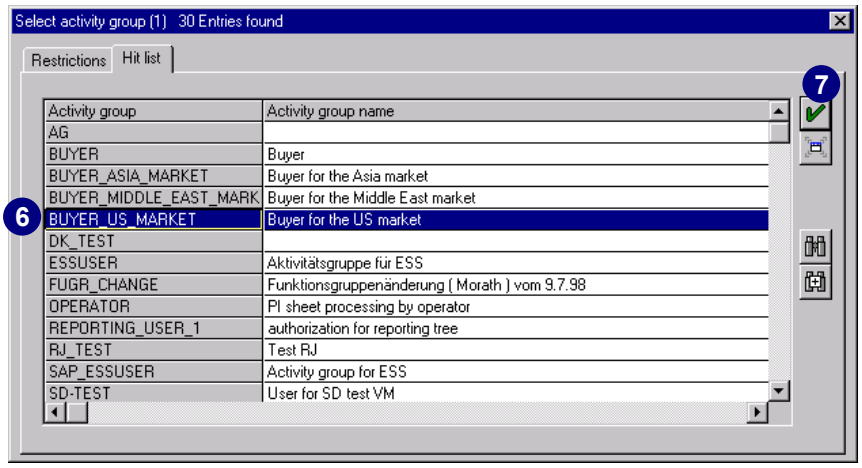
4. Choose the *Activity groups* tab.



5. Choose *possible entries* to select an existing activity group.

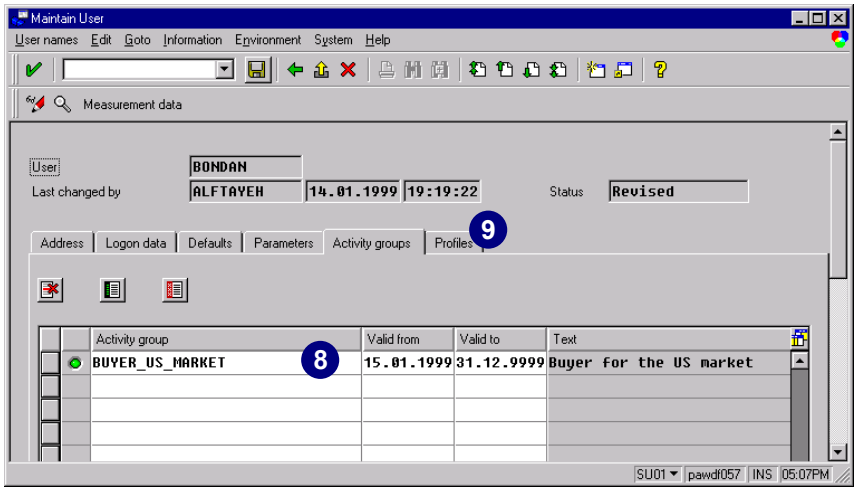


6. Select the activity group(s) you want to assign to the user (more than one selection is possible).
7. Choose *Copy*.

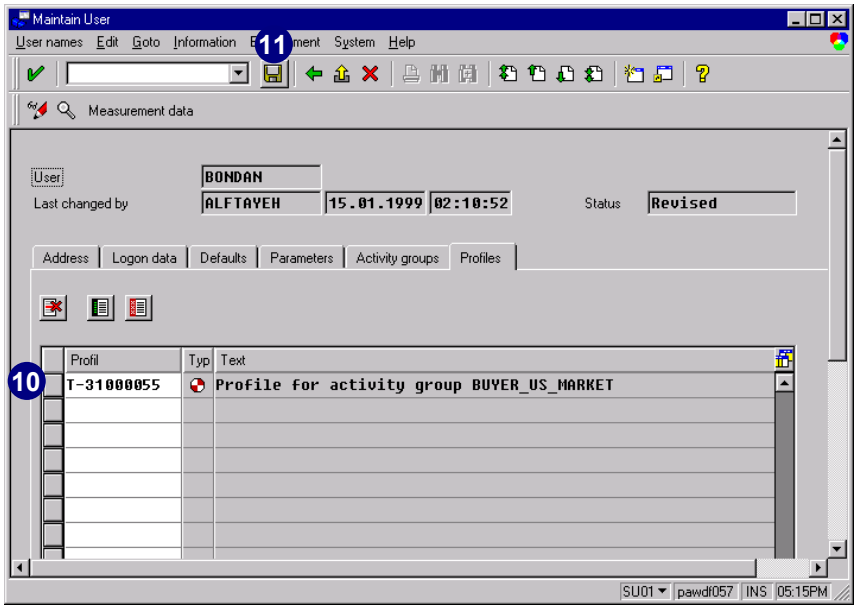


8. The assigned activity group appears with the validity period. Restrict the start and end date of the assignment by entering the required period.

   The system enters by default the current date as the start date and the *31.12.9999* as the end date.
9. Choose the *Profiles* tab.

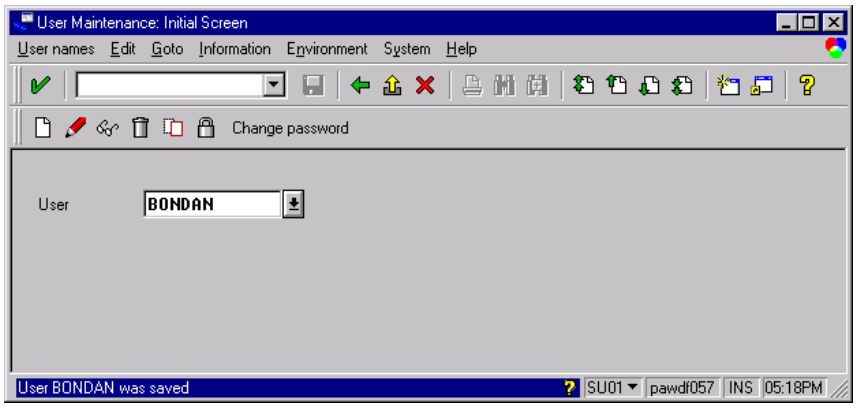


10. All authorization profiles transferred into the user master record appear in the column *Profil*.
11. Choose *Save*.



12. You have saved all changes to the user master record.

    Having finished this task, the user can now log on to R/3.



Remember, as long as an activity group is assigned to an R/3 user, you can change this activity group and the appropriate authorization profiles as often as you want **without** updating the user master record.

If an activity group is changed so that one profile becomes two or more, these profiles are automatically assigned to all the users for whom the old profile belonged. The user master of this user automatically gets updated.

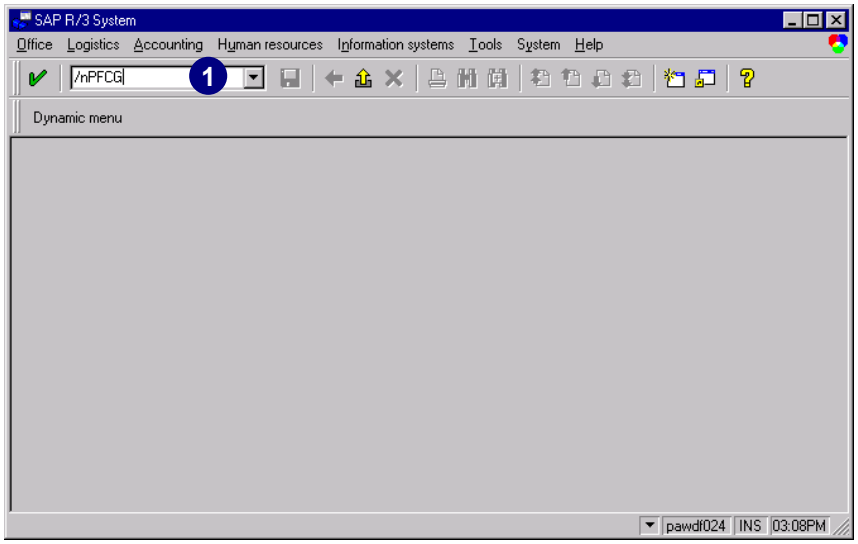
Assigning PD Objects to Activity Groups

You can assign PD objects such as positions, jobs, or organizational units to activity groups. Using transaction **PFCG**, verify that the authorization profiles have been generated (the light on the *Authorizations* tab should be green).

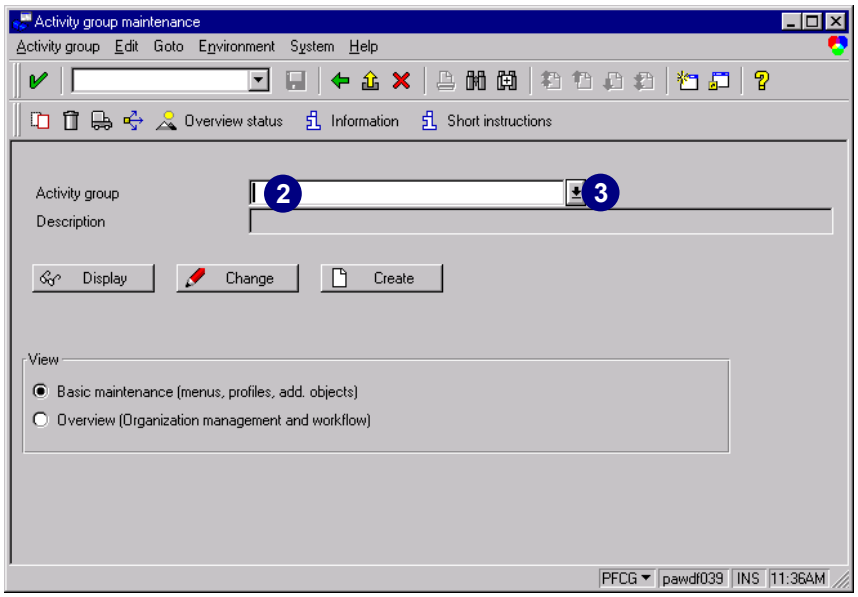
Create a Sample Organizational Plan

To assign PD objects to activity groups, your system must have an organizational plan. If you have not created one for your company but you want to test this functionality, please see *Creating a Sample Organizational Plan* on page 8–35.

1. In the *Command* field, enter transaction **PFCG** and choose *Enter* (or choose *Tools* → *Administration* → *User maintenance* → *Activity groups*).

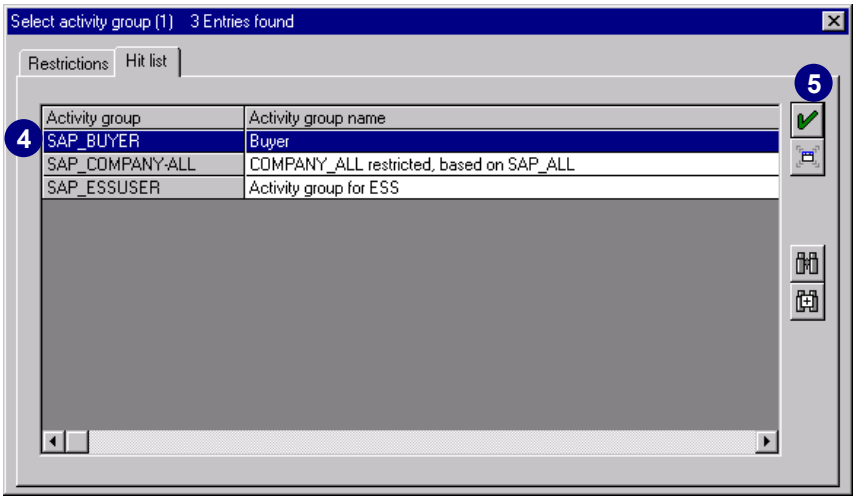


2. Place the cursor in the *Activity group* field.
3. Choose *possible entries*.

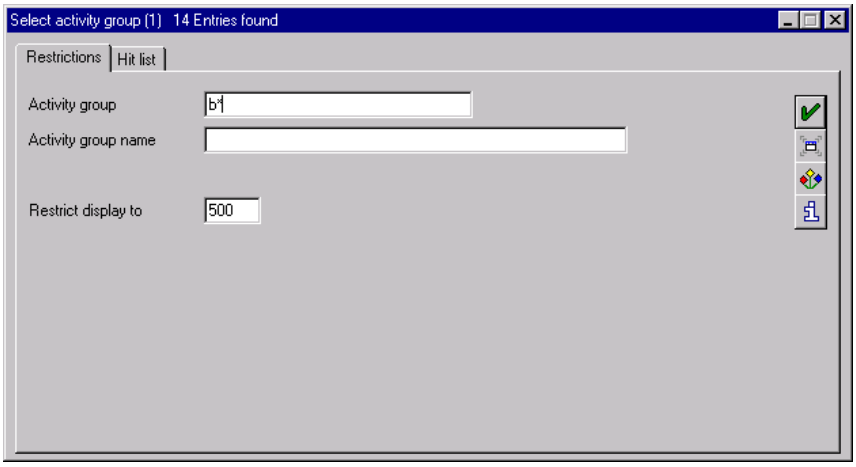


A *Hit list* appears.

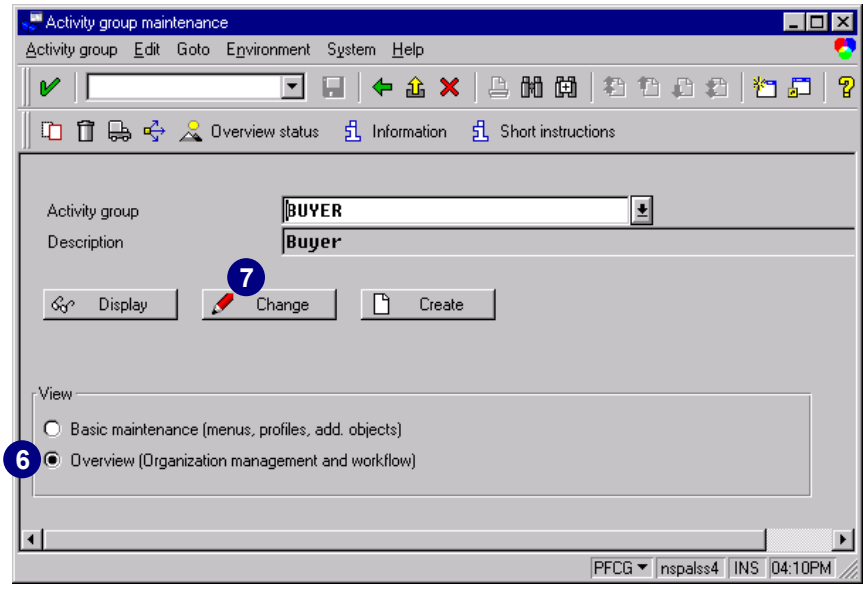
4. Select the activity group you want to edit.
5. Choose *Copy*.



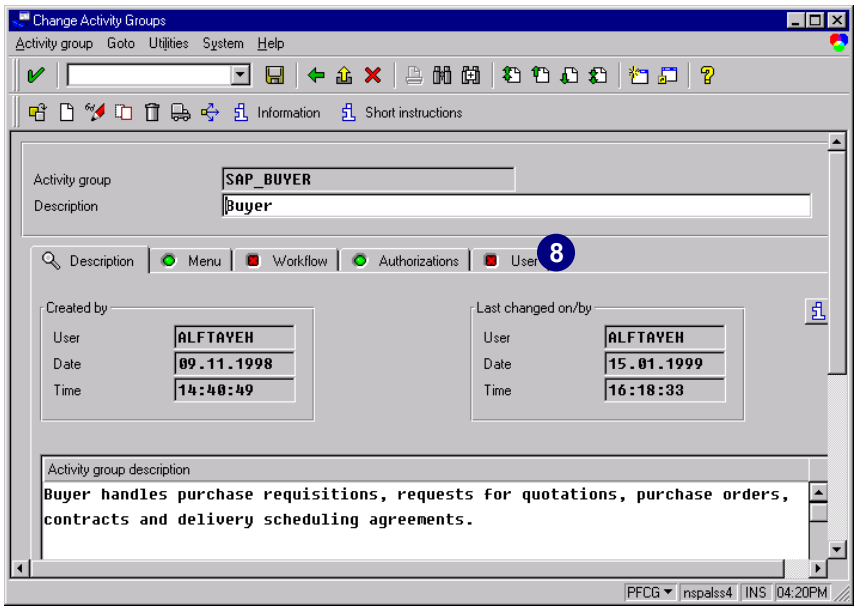
If the *Hit list* is too long, choose the *Restrictions* tab to narrow your search. Enter the first letters of the activity group you are looking for and choose *Start search*.



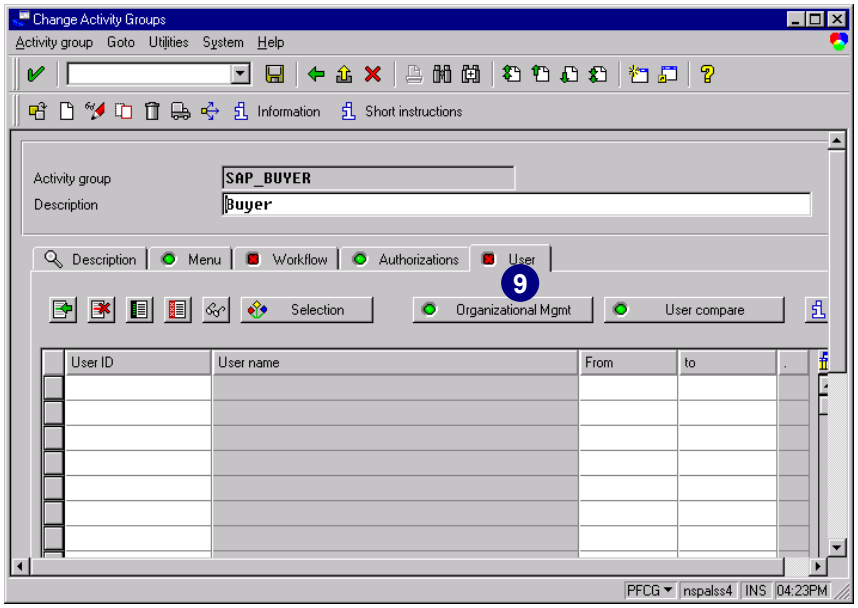
6. Select *Overview (Organization management and workflow)* to assign this activity group to PD objects.
7. Choose *Change* to edit your activity group data.



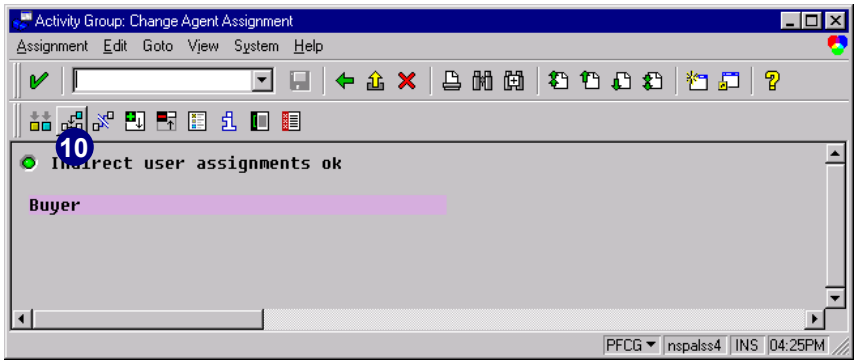
8. Choose the *User* tab to select one or more PD objects to assign to this activity group.



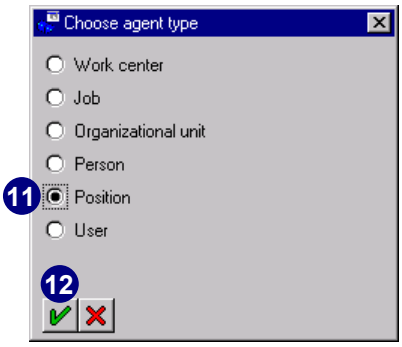
9. Choose *Organizational Mgnt*.



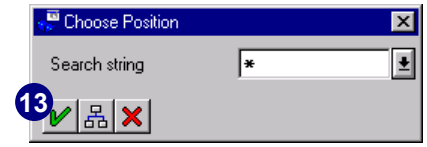
10. Choose *Create* to create the assignment.



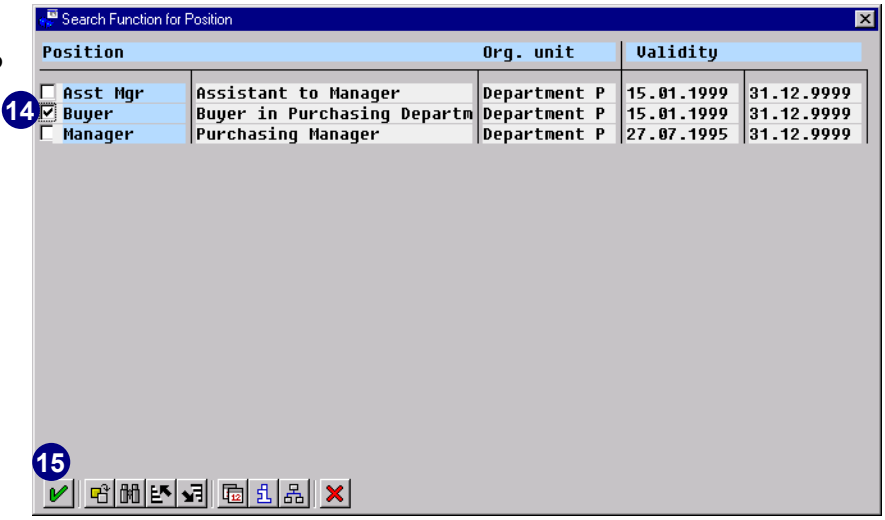
11. Select the object to be assigned.
12. Choose *Continue*.



13. Choose *Continue* to get a list of positions.



14. From the list of positions, select the position you would like to assign to the selected activity group (more than one position may be selected).
15. Choose *Continue.*



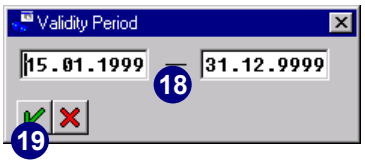
16. A relationship was created between the activity group and the desired position.
17. Choose *Period* to change the default validity period.

The *Validity Period* identifies the lifespan of the relationship between the activity group and the position we just created. This information is essential if you want your user master records automatically updated. Transaction *SUPC* helps you decide whether to include or remove a profile from a user master record. The report *PFCG_TIME_DEPENDENCY* ensures the consistency of the assignment between users and profiles.

You can determine the correct lifespan for the relationship. For example, the authorization profile for the activity group related to the position should be inserted in the assigned user master after today.

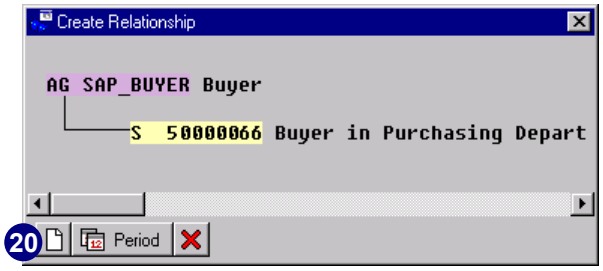
18. Enter the required dates.

    When you create a new relationship, the system automatically proposes today's date as the start date. The system also uses the current object's end date. If there is no specified end date, the system's default end date is usually 12/31/9999.



19. Choose *Continue*.

20. Choose *Create*.

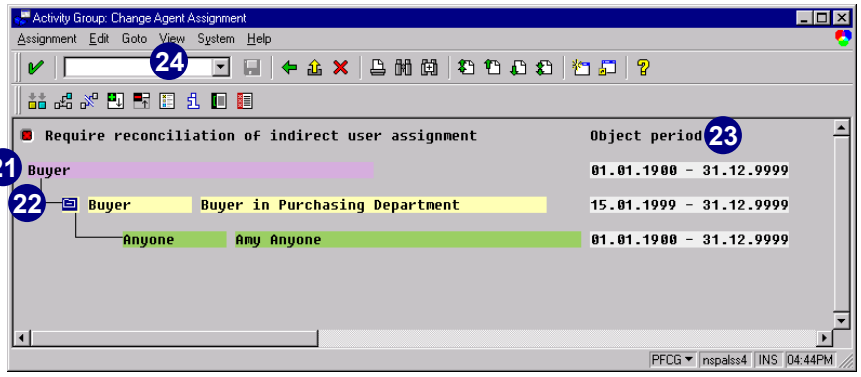


21. Under the activity group, notice the position assigned to this activity group.

22. Under the position, notice the user assigned to this position.

23. To see the lifespan of each of the objects displayed in the list choose *View* → *Object period on*.

24. To see the technical names in the list, choose *View* → *Key on*.



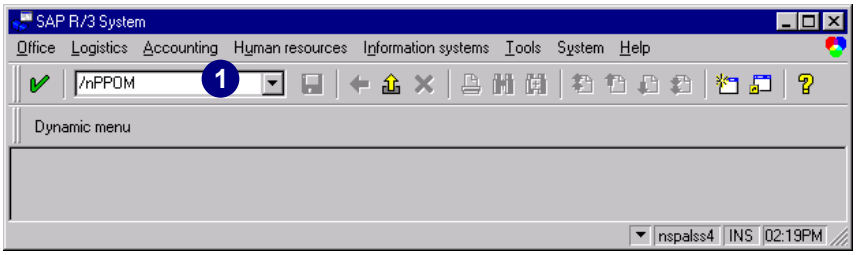
    The next task is to update the user master records so that the appropriate profiles are inserted into this record. The user master either can be updated manually or with a batch report.

    Please see *III. Running Report PFCG_TIME_DEPENDENCY as a Background Job* on page 8–32.

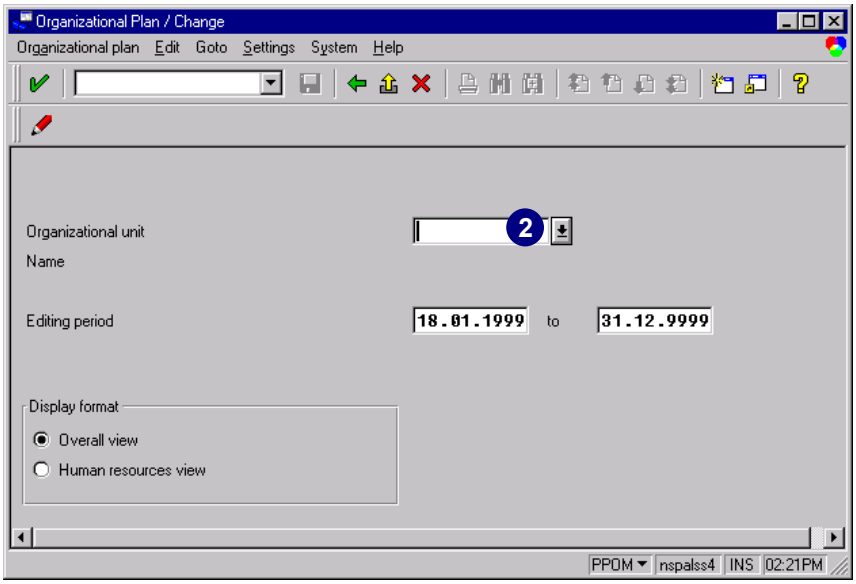
Assigning Activity Groups to PD Objects

You can assign activity groups and their authorization profiles to PD objects. Using transaction **PFCG**, verify that these profiles have been generated (the light on the *Authorizations* tab should be green).

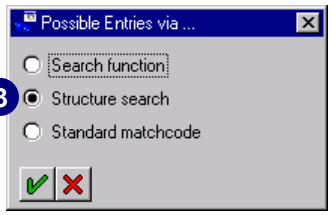
1. In the *Command* field, enter transaction **PPOM** and choose *Enter* (or choose *Human resources* → *Organizational management* → *Simple maintenance* → *Basic org. plan* → *Change*).



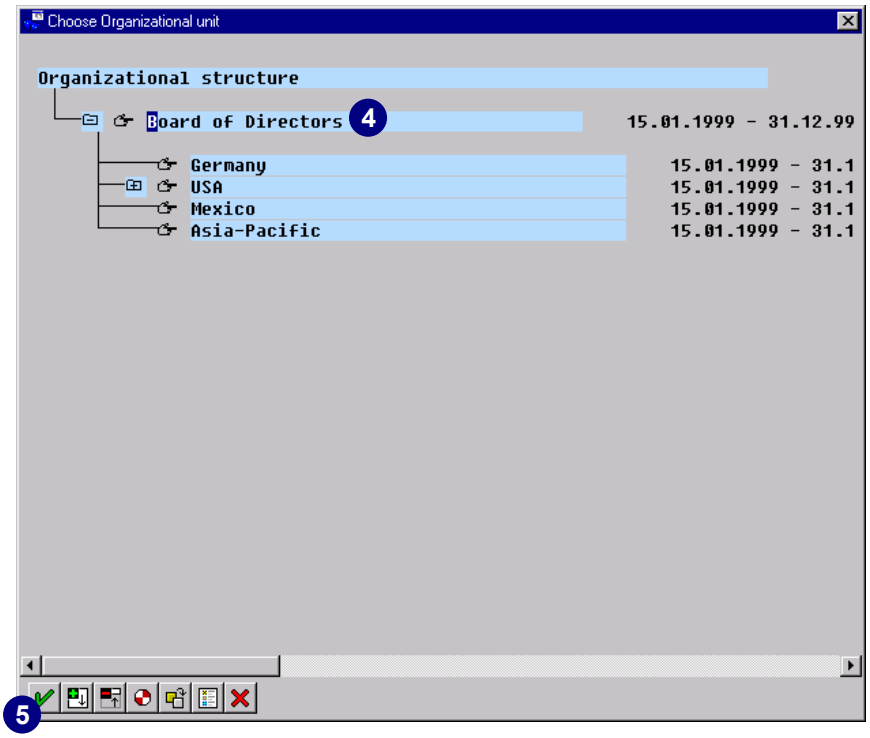
2. Choose *possible entries* for *Organizational unit* to select the appropriate root organizational unit.



3. Select *Structure search*.



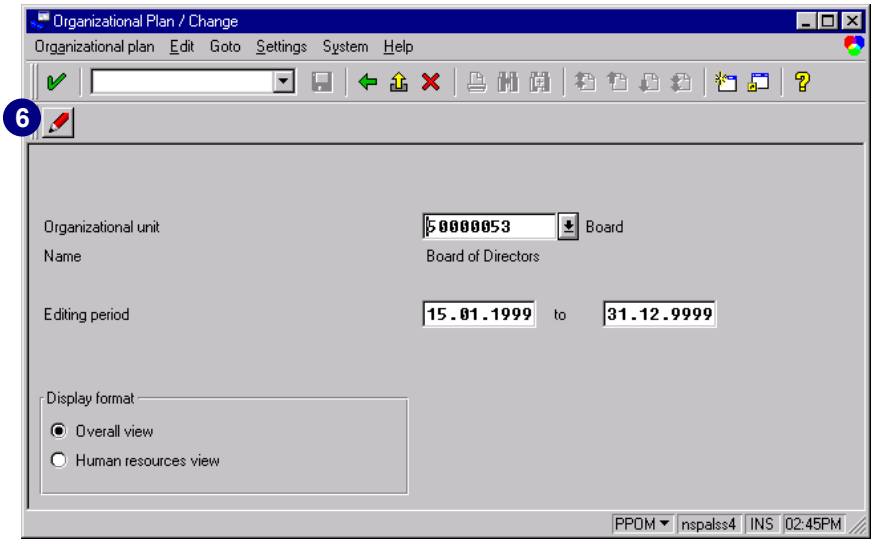
4. Select the appropriate root organizational unit. In this example, we chose the root organizational unit from the sample organizational plan.



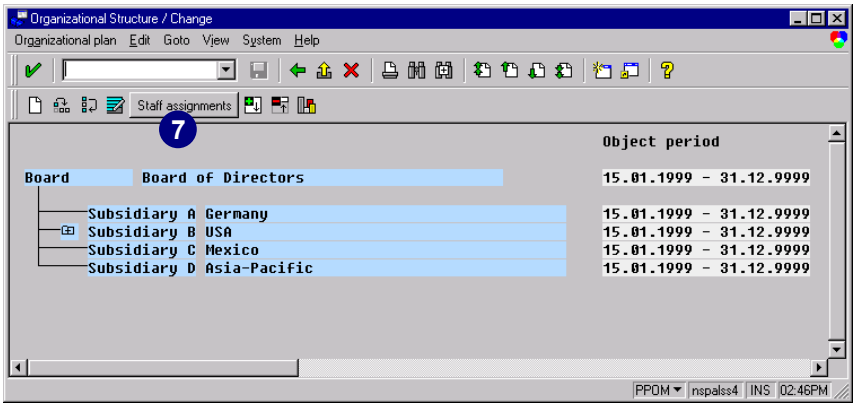
Create a sample organizational plan for testing purposes. For more information, please see the section *Creating a Sample Organizational Plan* on page 8–35.

5. Choose *Choose*.

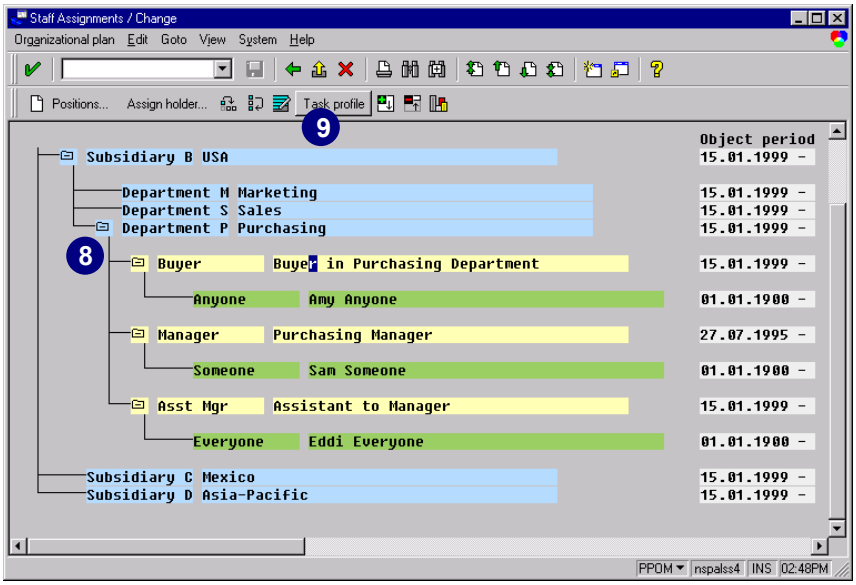
6. Choose *Change*.



7. Choose *Staff assignments*.

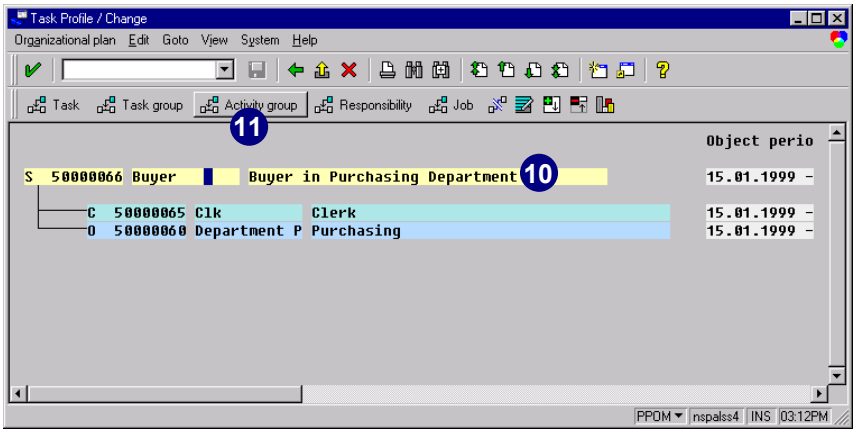


8. Expand the organizational units and select the correct unit to assign to the activity group(s).
9. Choose *Task profile*.

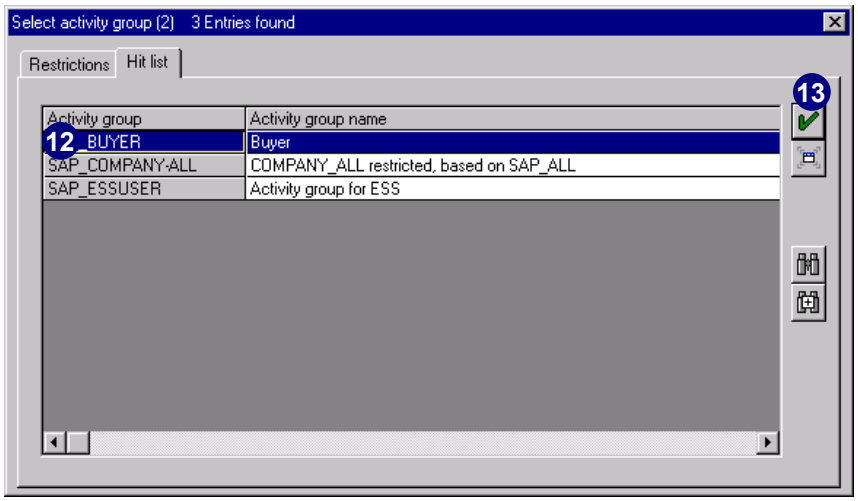


To get an explanation of the colors, choose *View* → *color legend*. To view the technical names, choose *View* → *Key on*.

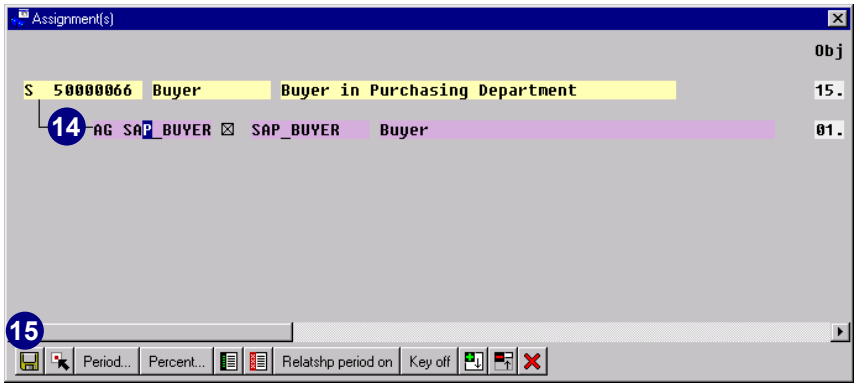
10. Place your cursor on the desired position to assign an activity group.
11. Choose *Assign Activity group*.



12. Choose the appropriate *Activity group.*
13. Choose *Copy*.

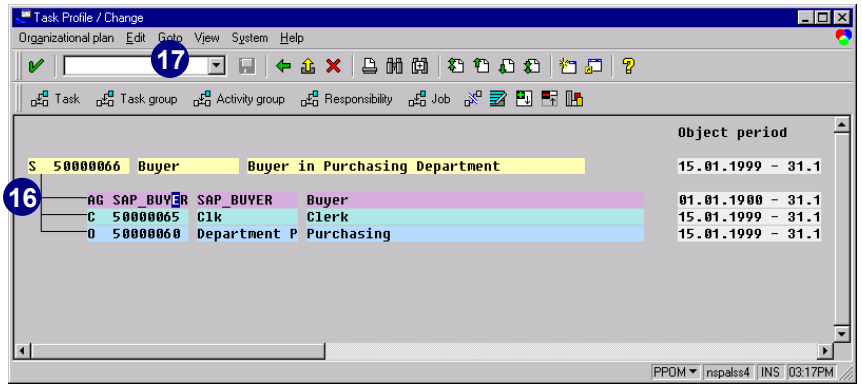


14. A relationship between the position and the activity group was created.
15. Choose *Save*.



16. The relationship between the position and the activity group was saved.
17. If you would like to call transaction *PFCG* (activity group maintenance) at this point, place your cursor on the activity group and choose *Goto* → *Activity group.*

    The next task is to update the user master records so that the appropriate profiles are inserted into the user master record and assigned to the organizational units.



Transferring Users from an IMG Project to an Activity Group

If you have assigned users (resources) to an IMG project in the project management, you can transfer these users to the activity group.

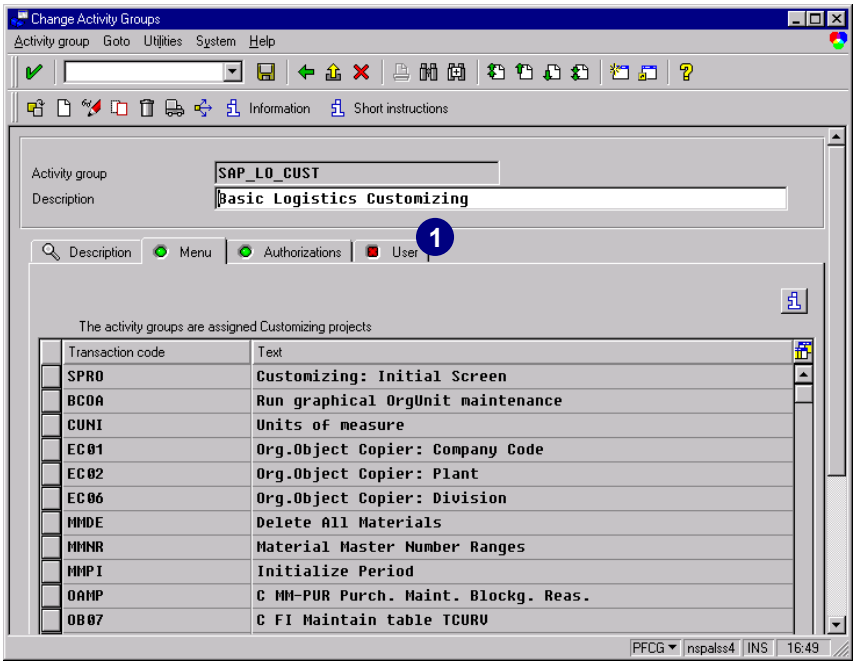
Note that you must call this function again each time you make changes in the IMG project administration.

For the following example we assume that:

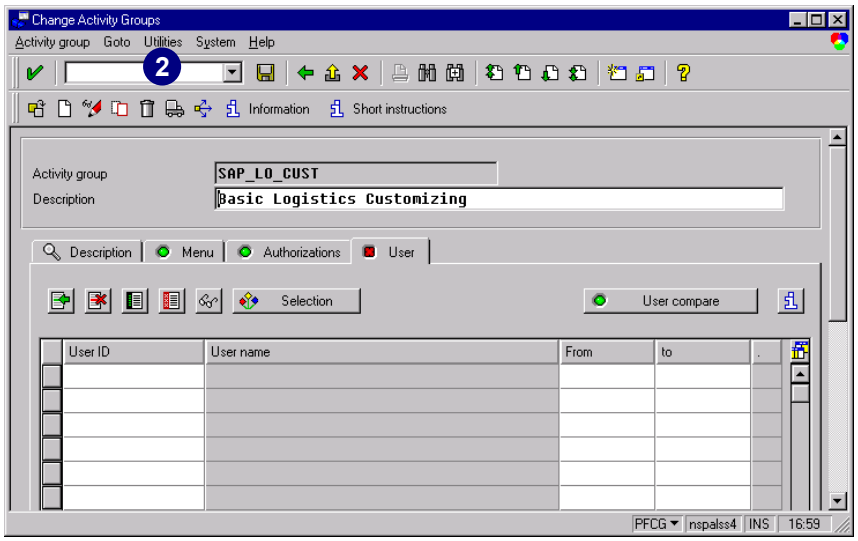
- An IMG project with at least one assigned user exists
- You assigned an IMG project or project view to the activity group (see chapter 5, the section *Assigning IMG Projects or Project Views to Activity Groups*)
- You maintained the authorizations for the customizing activity group (see chapter 5, the section *Maintaining and Updating Customizing Authorizations*)

1. On the *Change Activity Groups* screen for your customizing authorization, choose the *User* tab.

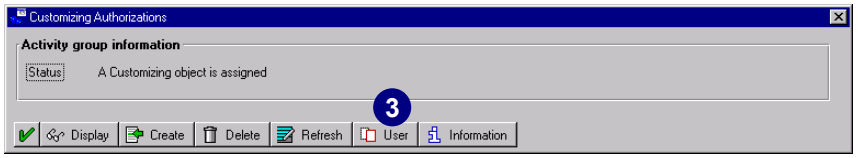
The green light on the *Menu* and *Authorizations* tabs indicates that those data are already maintained, whereas the red light on the *User* tab indicates that no user is assigned yet.



2. Choose *Utilities* → *Customizing auth.*.



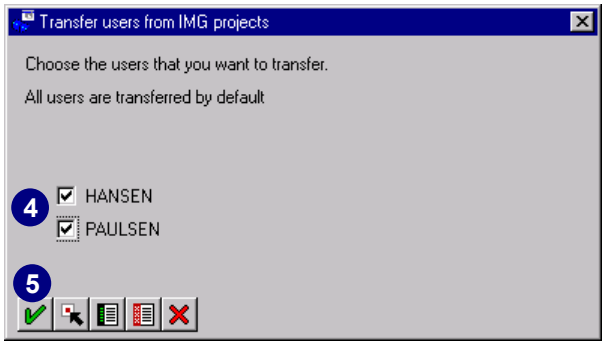
The status indicates that you have already assigned a customizing project.



3. Choose *Transfer user assignment from projects*.

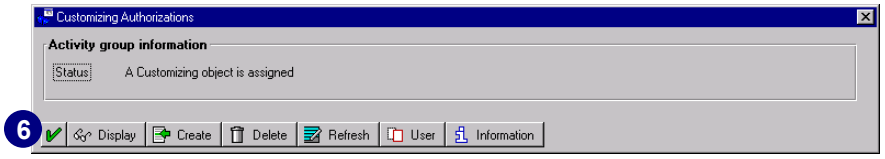
4. Deselect or select the desired users.

All users are selected and will be transferred by default.

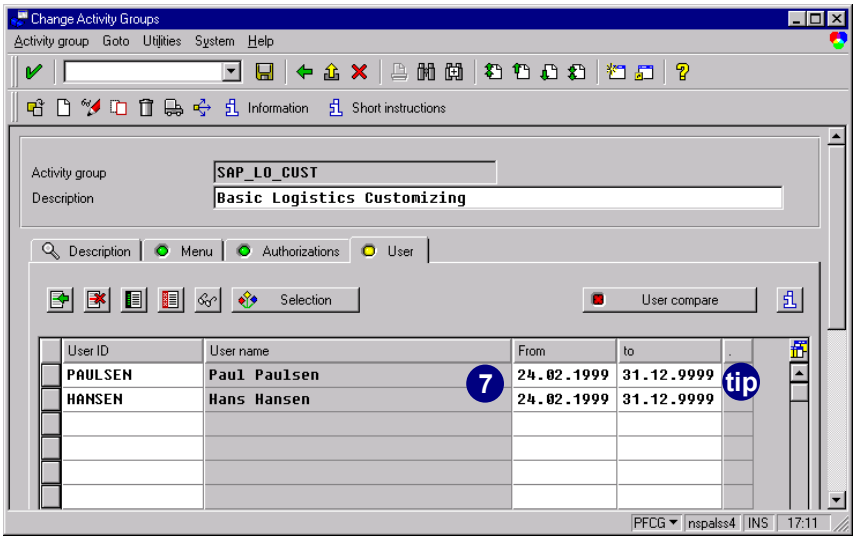


5. Choose *Continue*.

6. Choose *Continue*.

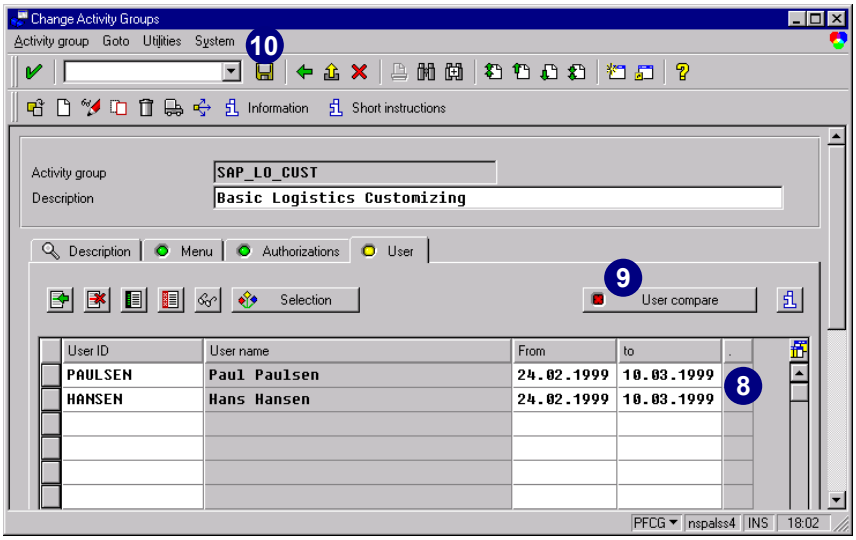


7. The users are being transferred from the customizing project/ project view to the customizing activity group with a default time period.

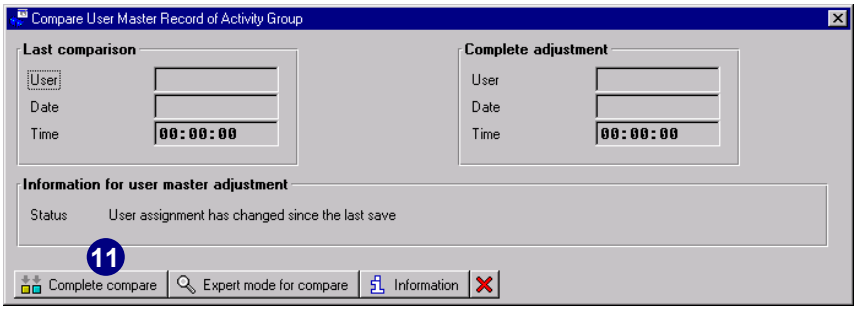


As customizing is executed project-related and for a limited period, you should maintain the end date for the user in the user assignment. This action prevents users who are assigned to the activity group from having authorization for the assigned projects or project views after the customizing project is complete.

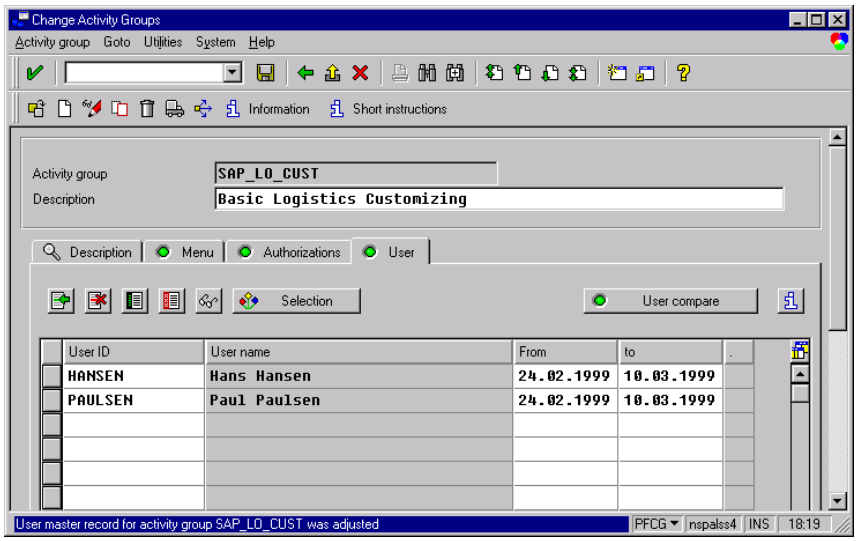
8. Enter the correct start and end date for the estimated customizing period.
9. Choose *Adjust user master* record.
10. Choose *Save.*



11. Choose *User master compare.*



12. Now you have transferred the users for the customizing project/project view.



Updating Profiles in the User Master Records

This section describes the steps involved in using report *PFCG_TIME DEPENDENCY* to update user master records. As you just learned, activity groups, their assignment to user master records, or PD objects can be delimited.

To ensure that only valid authorization profiles remain in the user master record each day, conduct daily profile comparisons. For the changes in the user master record to be effective, this comparison must take place before the user logs on.

To conduct a comparison, you can either:

I. Compare the user master data directly from within transaction **PFCG**

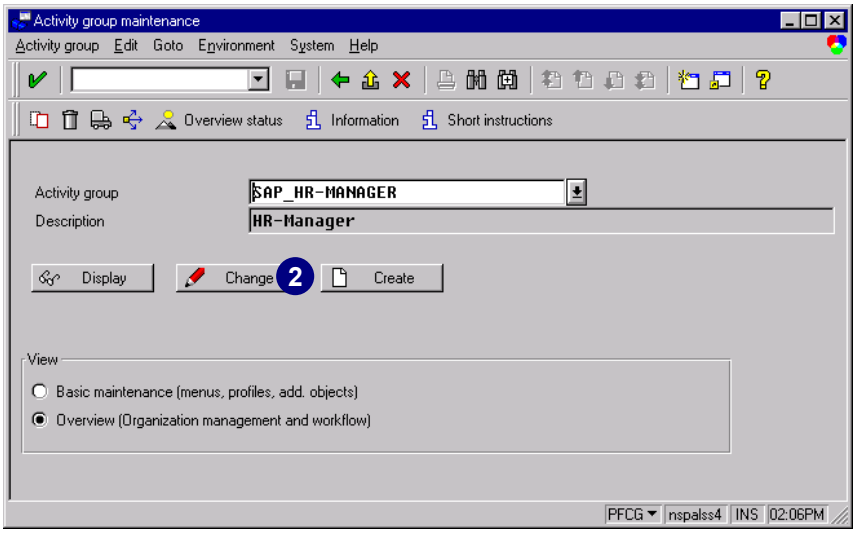
II. Use transaction **PFUD** (or within the PG *Goto* → *Mass compare*)

III. Run report *PFGC_TIME_DEPENDENCY* in a background job before the start of each day

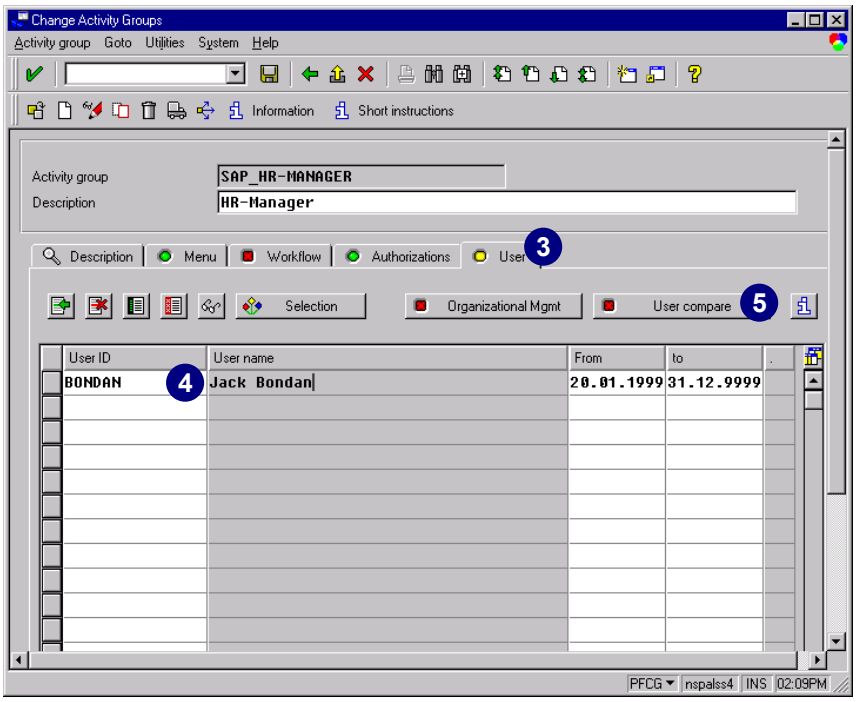
I. From Within Transaction PFCG

This technique immediately updates a specific user master after creating an assignment.

1. Start the *Profile Generator* and select an activity group that you created earlier.
2. Choose *Change*.

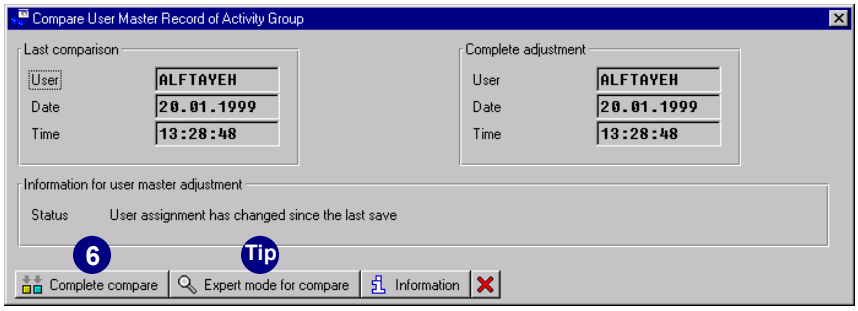


3. Choose the *User* tab.
4. In *UserID*, select a user with *possible entries*.



Status Display on the *User* Tab
The status display on the tab tells whether or not users are already assigned to the activity group. If the indicator is red, no users are assigned. If green, at least one user is assigned to the group. If yellow, this means that although users have been assigned to the activity group, the user master record comparison is not current.

5. Choose *User compare*.
6. Choose *Complete compare*.

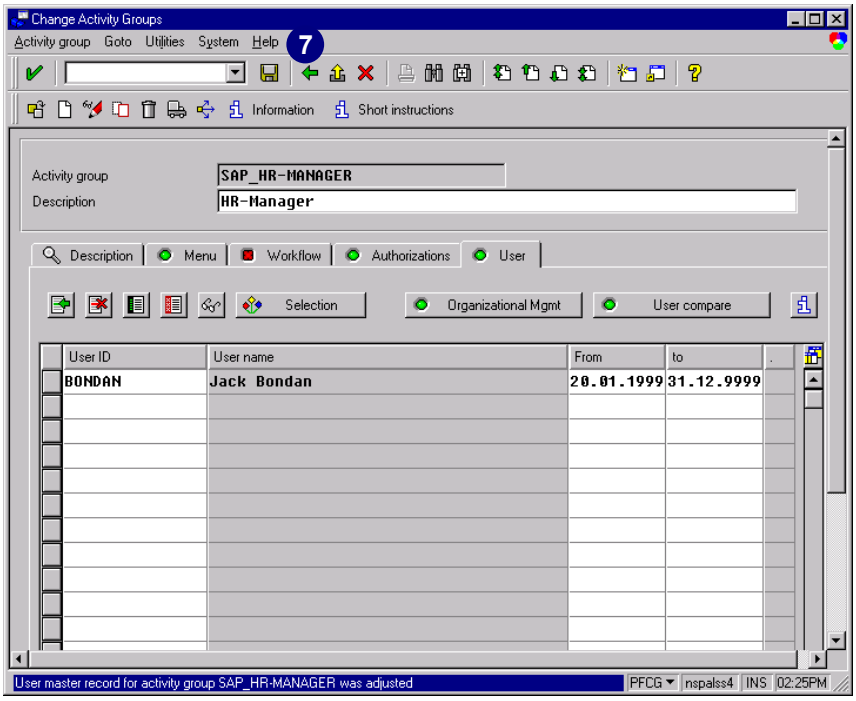


The expert mode displays exactly which profiles were inserted and removed for each user. As you have the option to restrict the selection of the profiles for processing, the status of *User compare* is not switched to green. This status is only the case if the comparison is executed by choosing *Complete compare*. If you choose *Expert mode for compare*, the status is not set to green.

The green indicator on *User compare* means that the comparison is complete.

7. Choose *Back*.

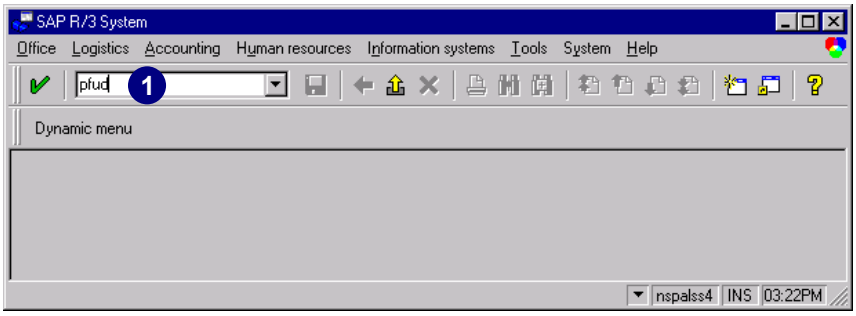
Remember that changes are first active with the next user logon.



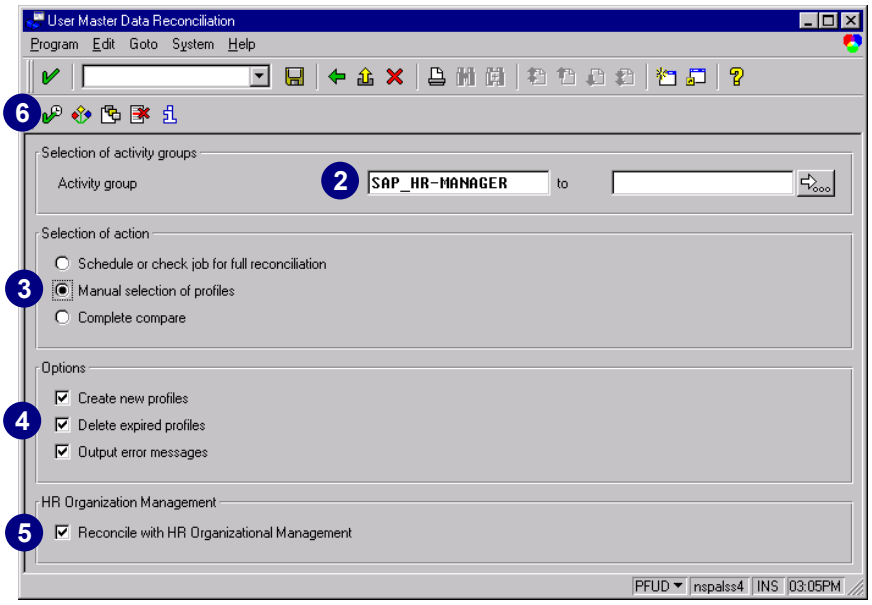
II. Using Transaction PFUD

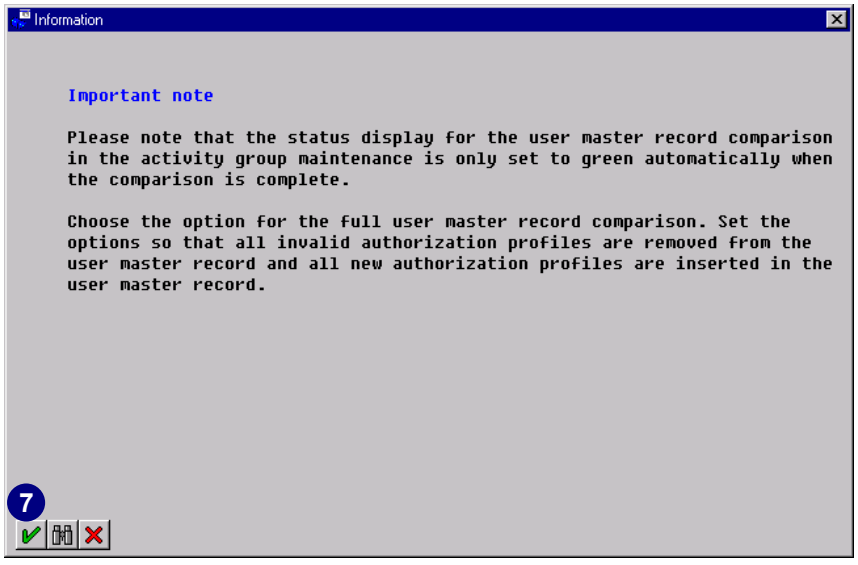
As an administrator, use the transaction **PFUD** (or within the PG *Goto* → *Mass compare*) regularly to check for background job errors.

1. In the *Command* field, enter transaction **PFUD** and choose *Enter* (or enter transaction **SA38** and use program **RHAUTUPD_NEW**).

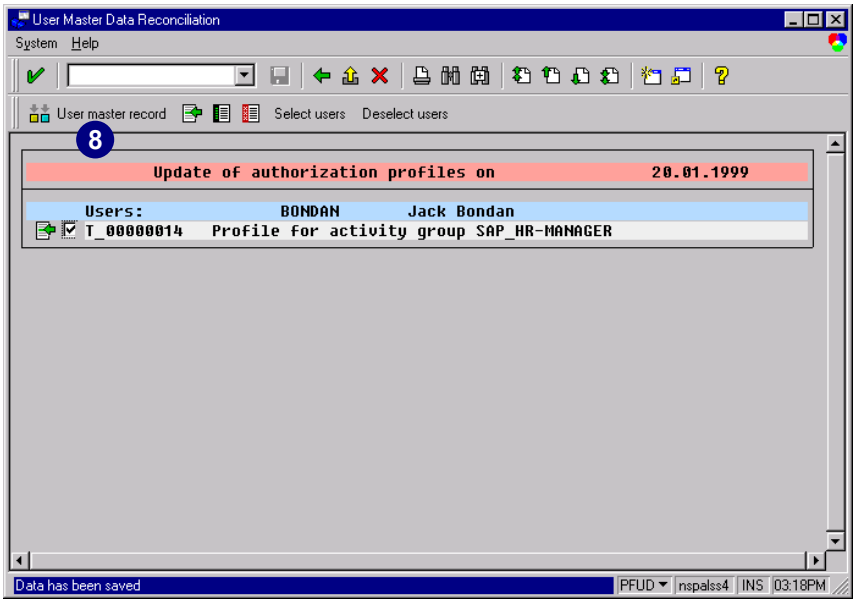


2. Choose the activity groups you would like to reconcile.
3. Select one of the following:
   - *Schedule or check job for full reconciliation*
     (see the next section)
   - *Manual selection of profiles*
     (for selected profiles)
   - *Complete compare*
     (to adjust user master record for all activity groups)
4. Under *Options*, select the desired settings.
5. If you would like to reconcile with organizational management, select *Reconcile with HR Organizational Management*.
6. Choose *Execute*.
7. Choose *Continue*.



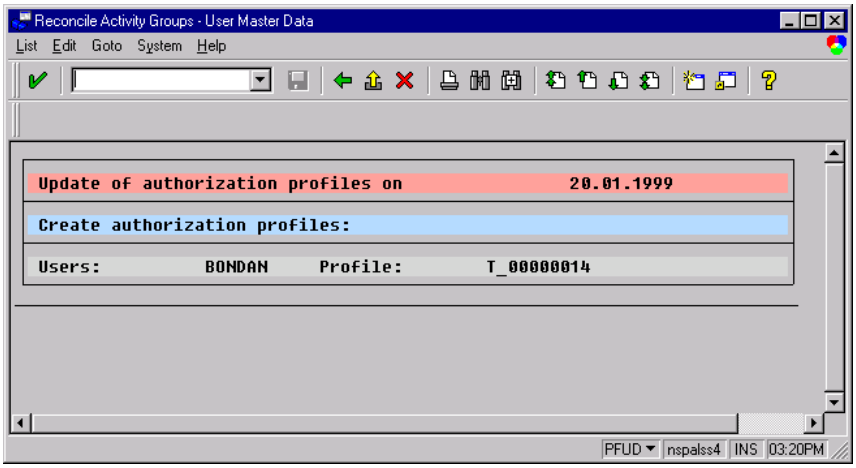


8. Choose *Reconcile user master record*.



The user master records have been successfully updated.

Remember that changes are first active with the next user logon.

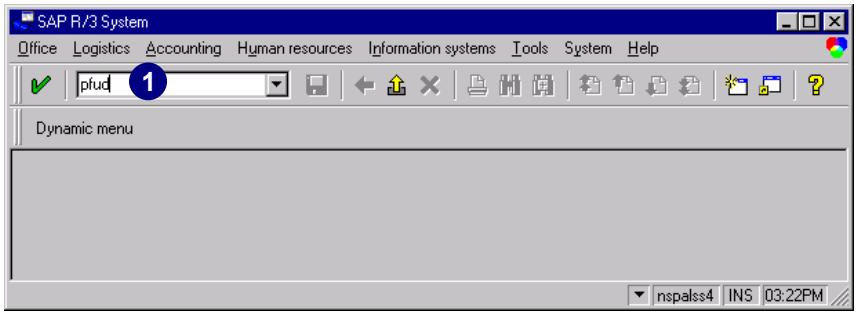


II. Running Report PFCG_TIME_DEPENDENCY as a Background Job

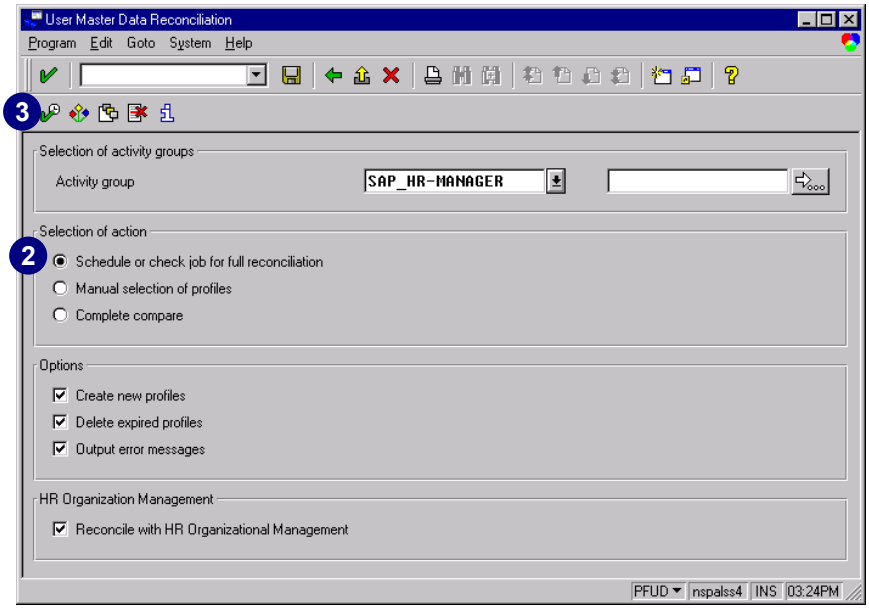
Time-Dependency of User Assignment and Authorizations
When you specify the users for the activity group, the system defaults to the current date as the start date of the user assignment, and 31.12.9999 as the end date. If you want to restrict the start and end dates of the assignment, for example if you want to define a temporary replacement for a user, the system automatically makes the changes to the user. This automatic adjustment of the user's authorizations is executed by report *PFCG_TIME_DEPENDENCY*. In this case, you should schedule report *PFCG_TIME_DEPENDENCY* daily, for example early in the morning, to run in the background (in transaction *SA38*, for example). This report compares the user master records for all activity groups and updates the authorizations for the user master records. The system removes authorization profiles from invalid user assignments and enters authorization profiles from valid user assignments.

If report *PFCG_TIME_DEPENDENCY* runs every night, assuming the job ran correctly, the authorization profiles in the user master will be updated each morning. The best procedure is to schedule this report in a periodic background job.

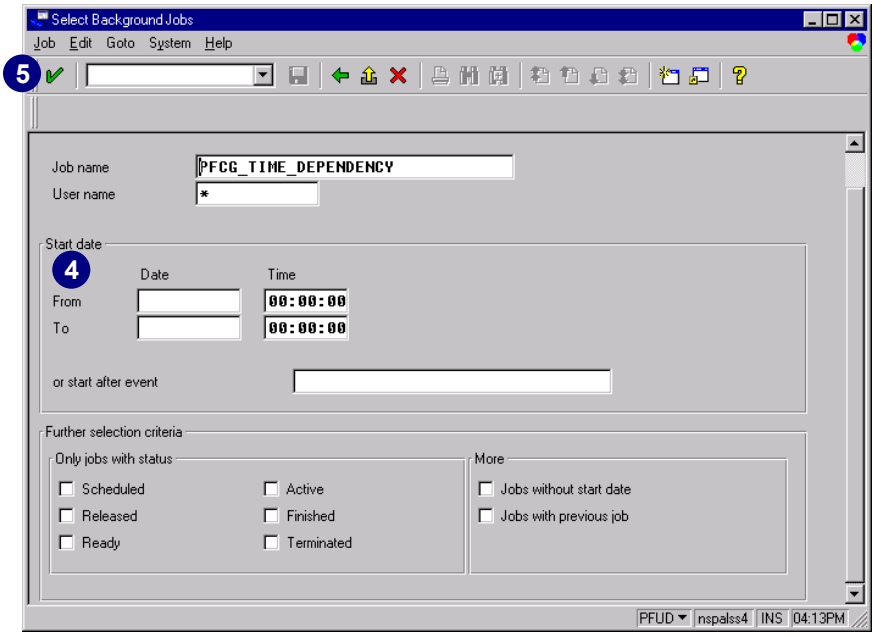
1. In the *Command* field, enter transaction **`PFUD`** and choose *Enter* (or enter transaction **`SA38`** and use program **`RHAUTUPD_NEW`**).



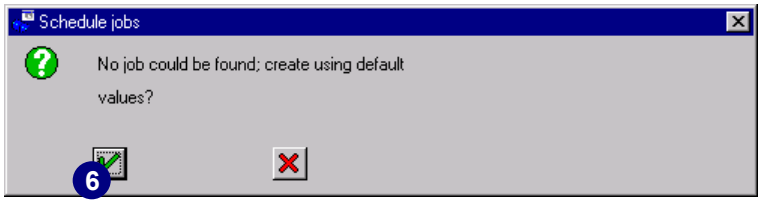
2. Select *Schedule or check job for full reconciliation*.
3. Choose *Execute*.



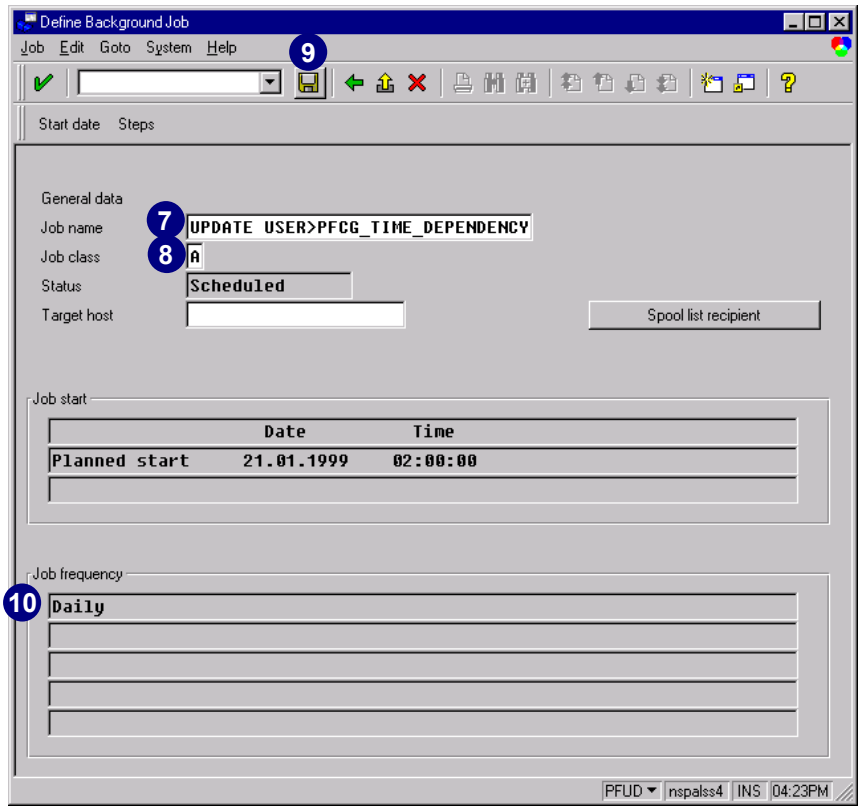
4. Select the date and time you want the report to run.
5. Choose *Enter*.



6. Choose *Enter*.



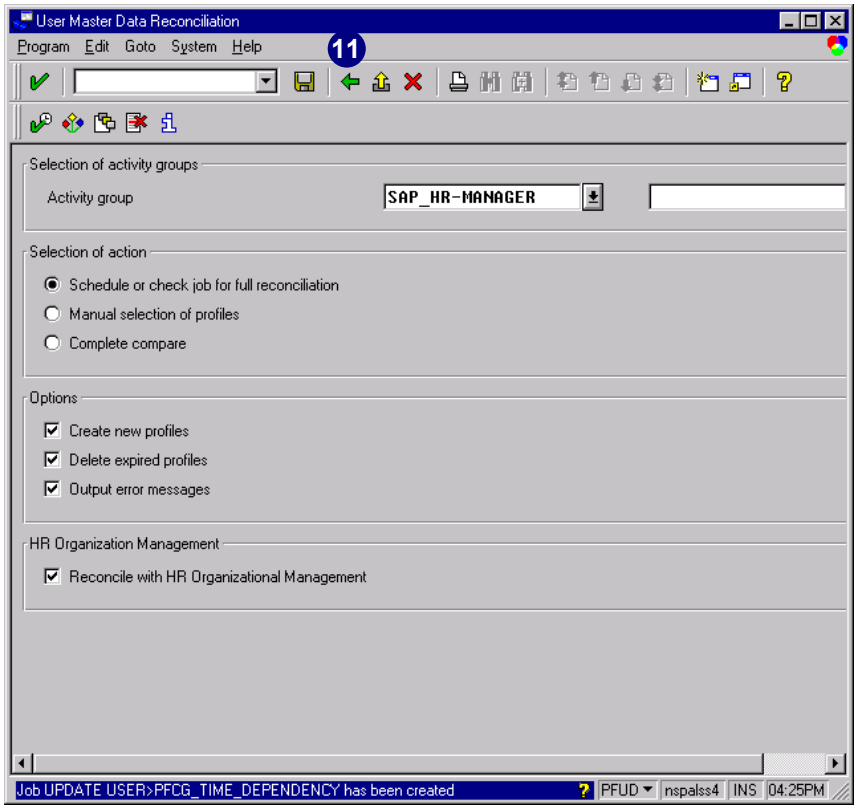
7. Enter a name in *Job name* or leave the default.
8. Enter **A** in *Job class*.
9. Choose *Save*.
10. All other data necessary to periodically schedule the report are automatically entered.



Report *UPDATE <USER> PFCG_TIME_DEPENDENCY* has been created and successfully scheduled.

11. Choose *Back* to exit *PFUD*.

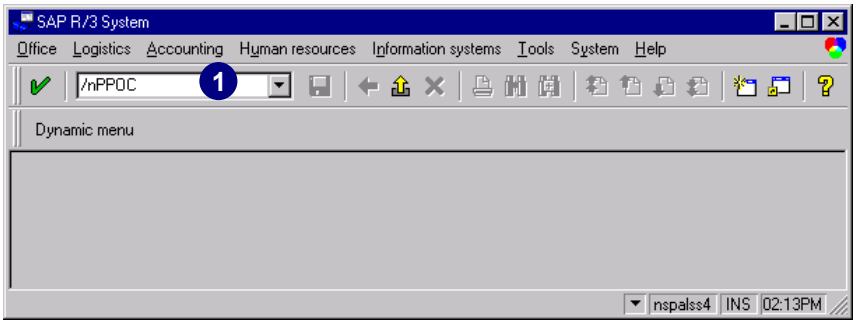
You can run transaction **SM37** is check the status of the scheduled job.



Creating a Sample Organizational Plan

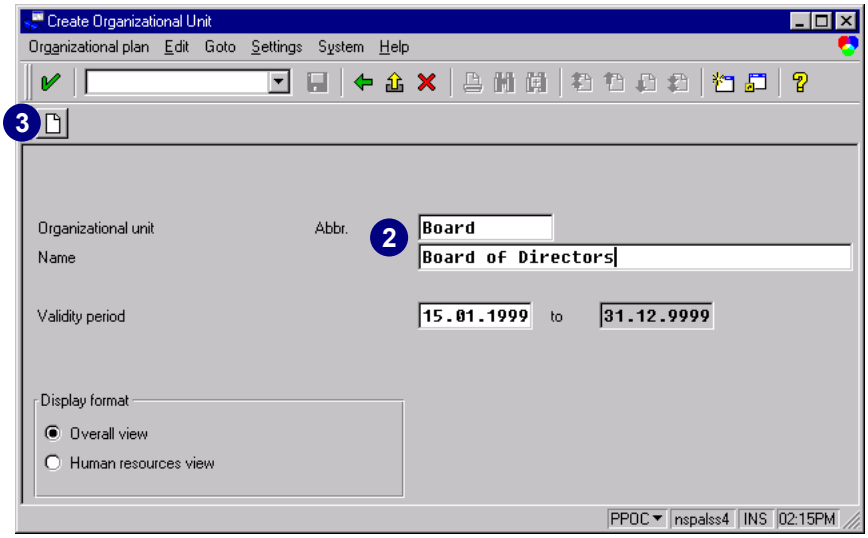
This section describes the steps to create a sample organizational plan for testing. This plan will not be complete but shows the required elements.

1. In the *Command* field, enter transaction **PPOC** and choose *Enter* (or choose *Human resources* → *Organizational management* → *Simple maintenance* → *Basic org. plan* → *Create*).

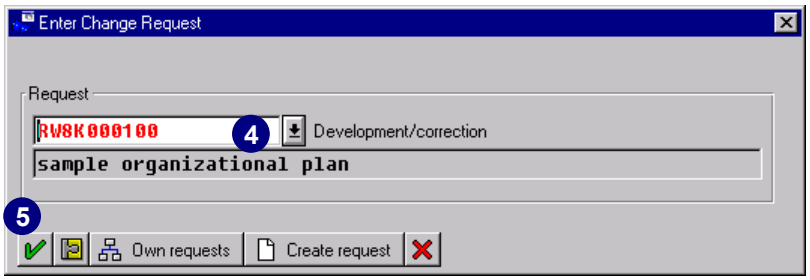


   To start a plan, first create a root organizational unit (the highest level in an organizational structure, for example the *Board of Directors*). Then build the organizational structure from the root organizational unit.

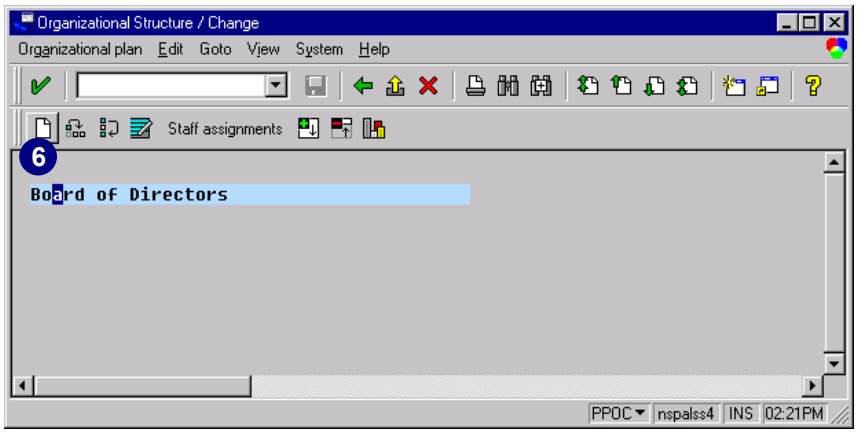
2. Enter the short and long name for the root organizational unit.
3. Choose *Create*.



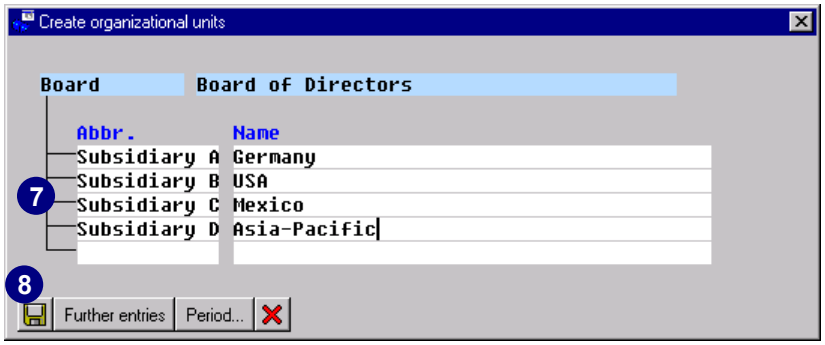
4. In the *Request* field, use *possible entries* to select a change request.
5. Choose *Continue*.



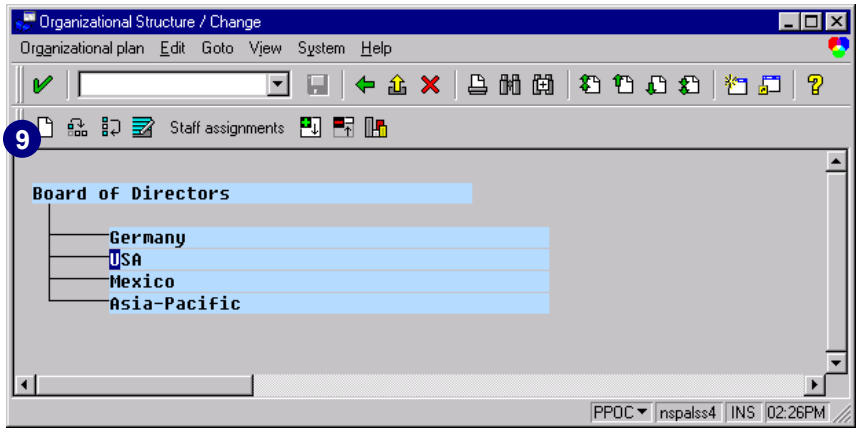
6. Choose *Create* to create the organizational units that follow your root unit.



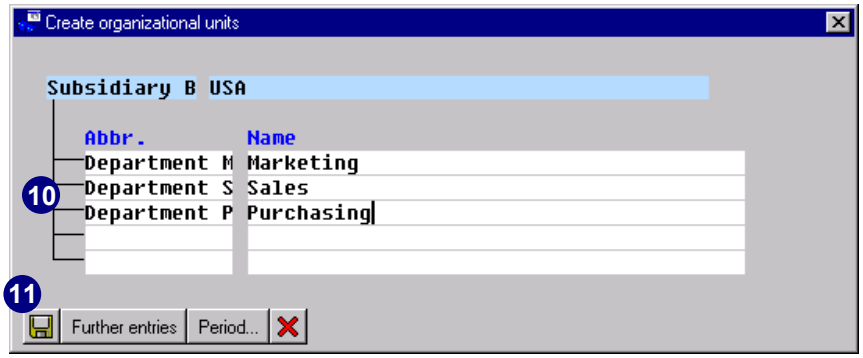
7. Enter the next organizational units under your root unit.
8. Choose *Save*.



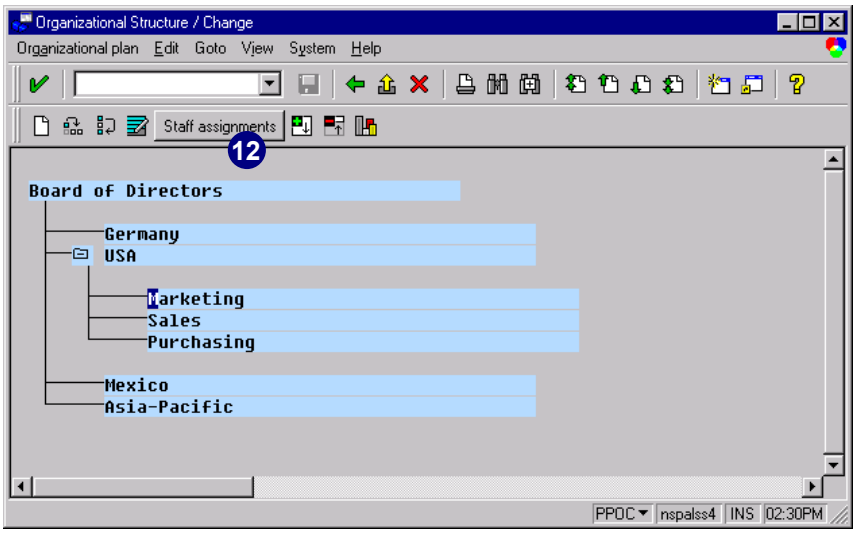
9. Select an organizational unit and choose *Create* to enter the next level of organizational units.



10. Enter the next organizational unit under *Subsidiary B*.
11. Choose *Save*.

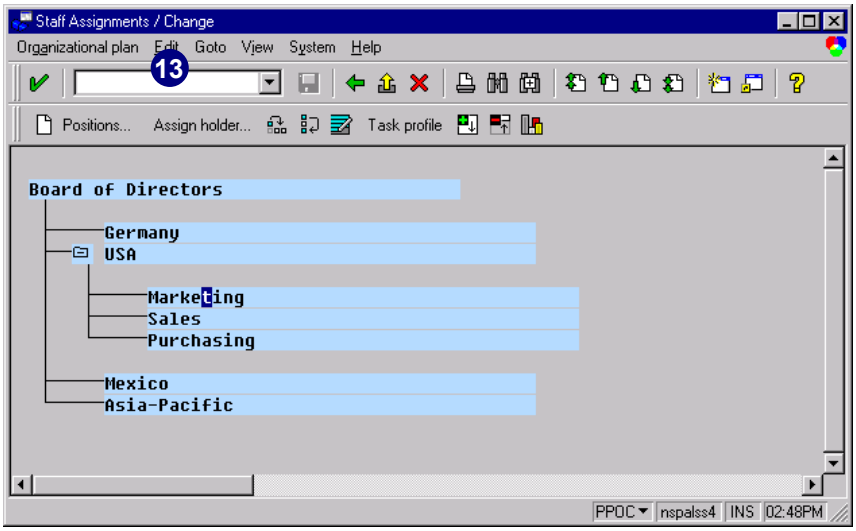


12. Choose *Staff assignments*.



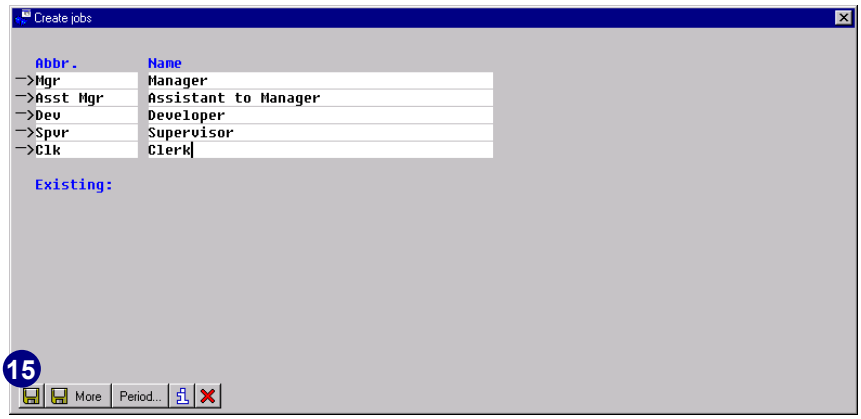
The *Staff Assignments / Change* window allows you to identify the fundamental staffing details required for an organizational plan. This step is achieved by creating jobs, and positions, and by assigning holders to positions.

13. Choose *Edit* → *Create* → *Jobs*

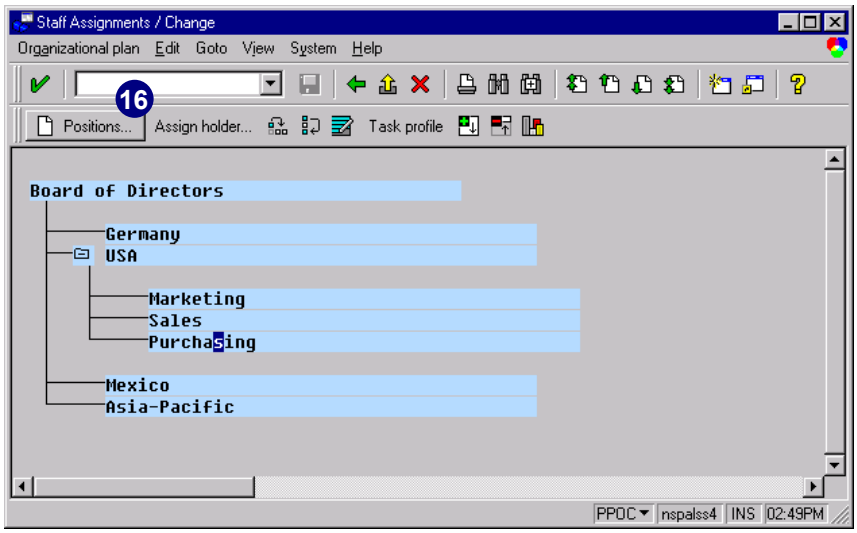


Jobs are one of the objects that make up an organizational plan. A job is a general classification, such as secretary, computer programmer, instructor, etc. You may create as many jobs as you want. Once a job is created, describe its attributes by defining infotypes. An employee automatically inherits the infotype settings, attributes, and properties of the job. (Positions are usually based on jobs.)

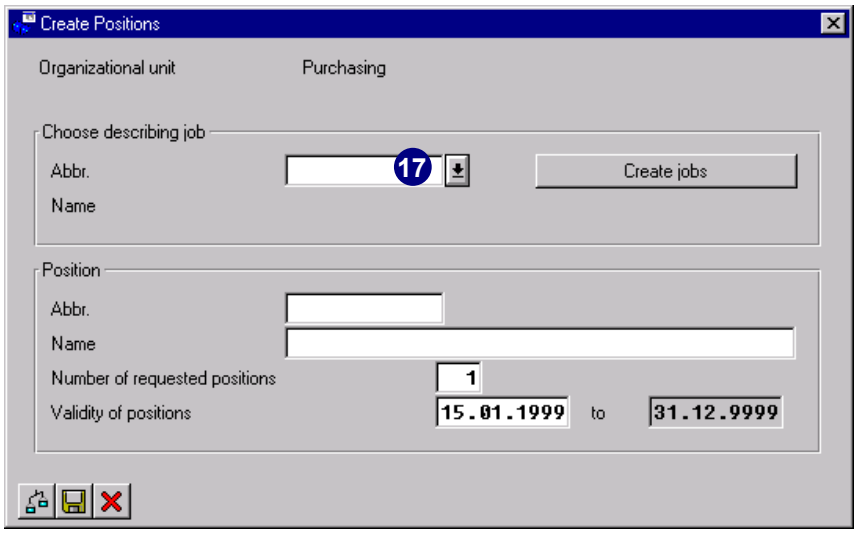
14. Enter the job information.
15. Choose *Create*.



16. Select an organizational unit, then choose *Create Positions*.



17. Choose *possible entries* for *Abbr*.

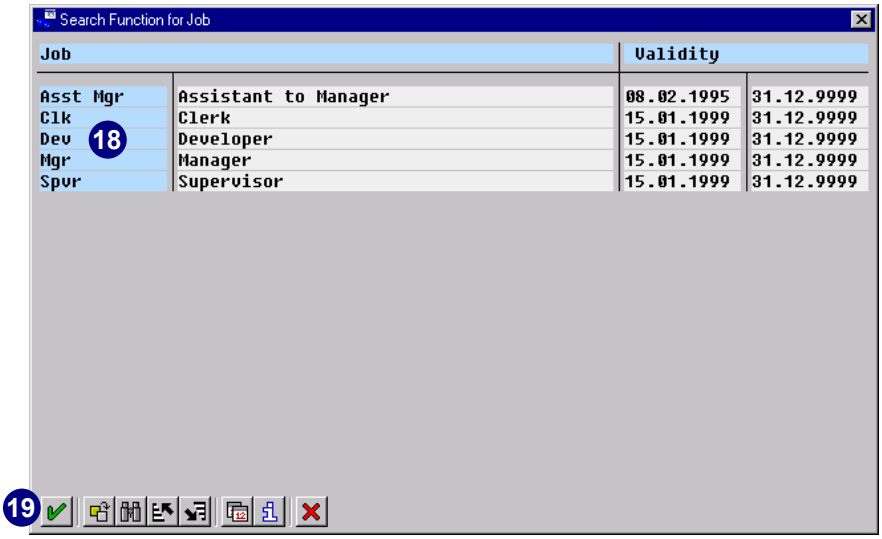


Positions are the individual employee assignments within a company for example:

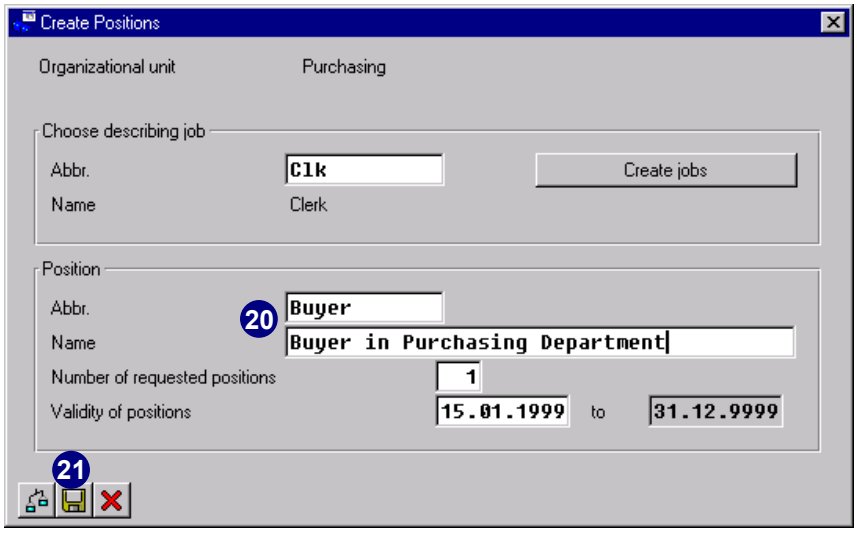
- Sales manager
- Marketing secretary
- Junior manufacturing engineer

By creating positions and creating relationships among the different positions, you can identify the reporting structure at your firm. Positions are usually based on jobs.

18. Select the appropriate job.
19. Choose *Enter*.

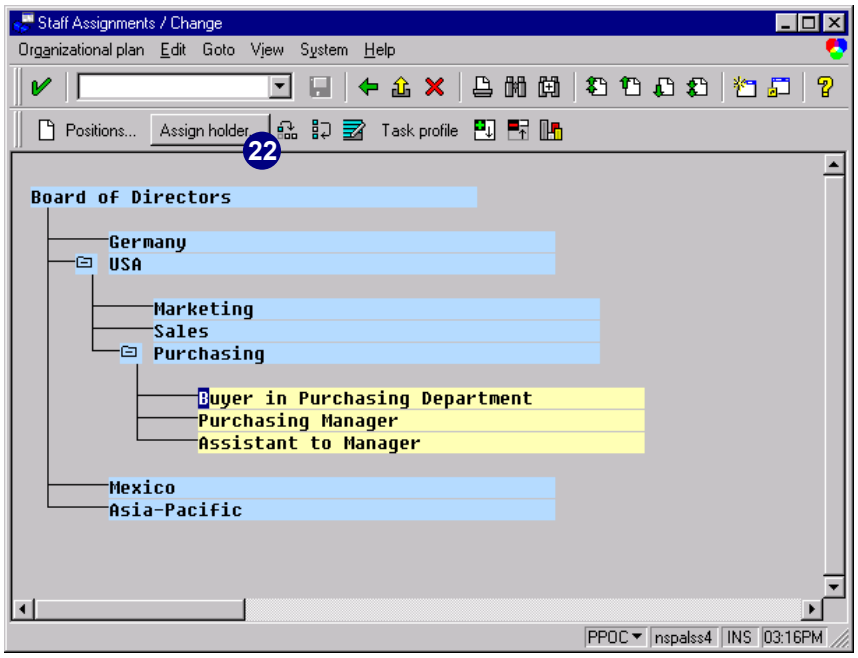


20. Enter information in the fields under *Position*.
21. Choose *Save*.



Repeat steps 16–21 to create additional positions.

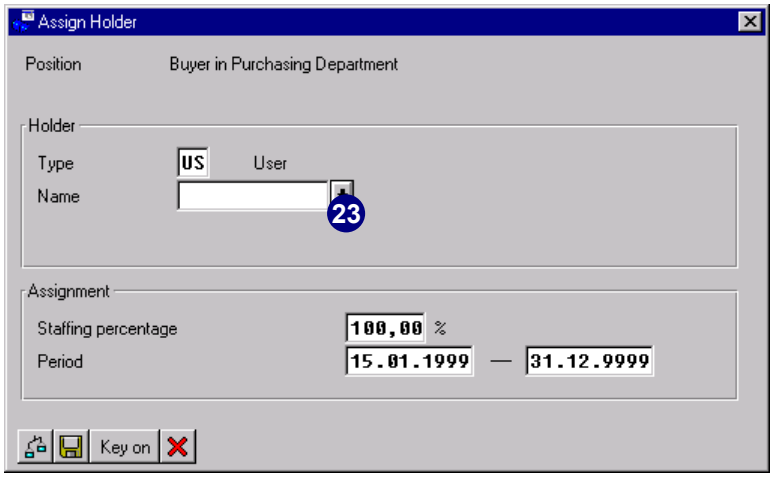
22. Select a position and choose *Assign holder*.



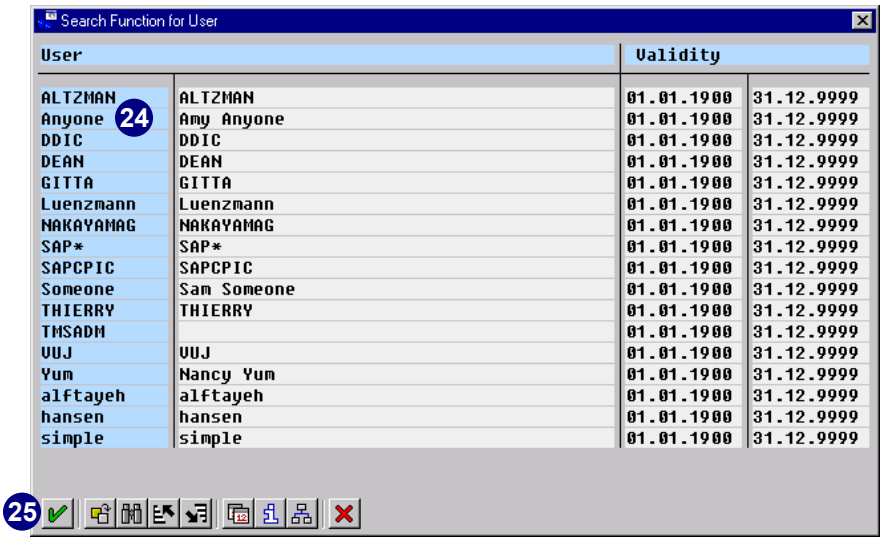
Assign holders when you want to identify who occupies, or fills, a specific position.

In *Simple Maintenance*, assign either an employee or R/3 user to a position. Workflow users assign R/3 users to positions. Personnel administration users assign employees to positions.

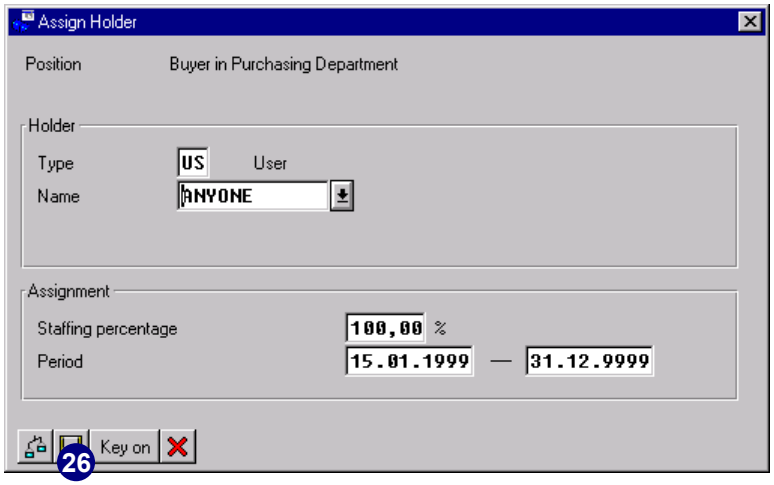
23. Choose *possible entries* to display the list of R/3 users already in your system.



24. Select the correct holder of the position from the user list.
25. Choose *Enter*.

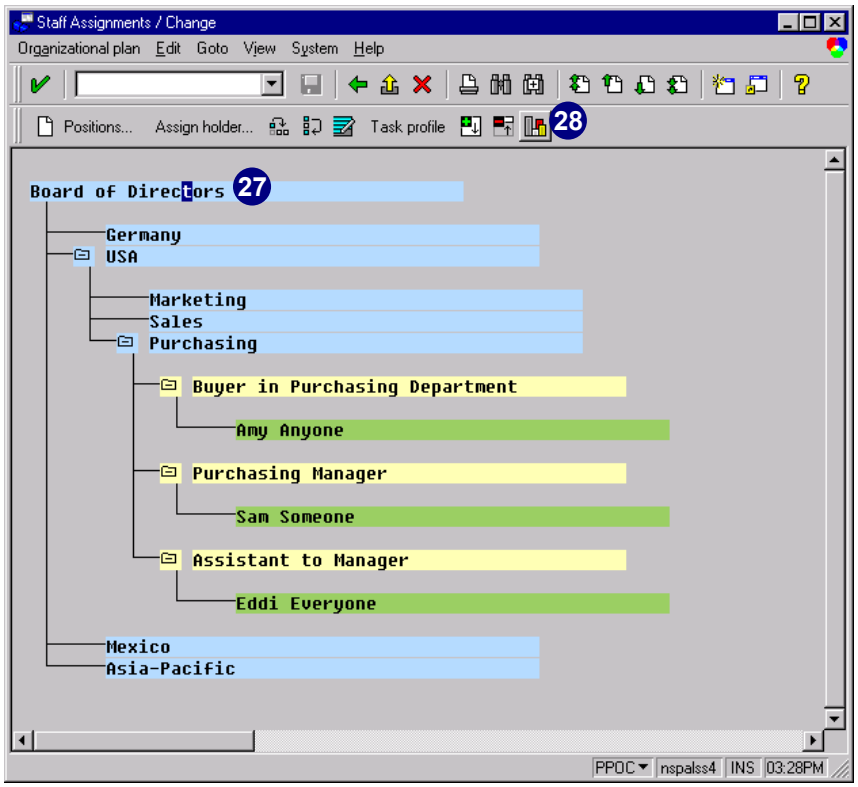


26. Choose *Save*.

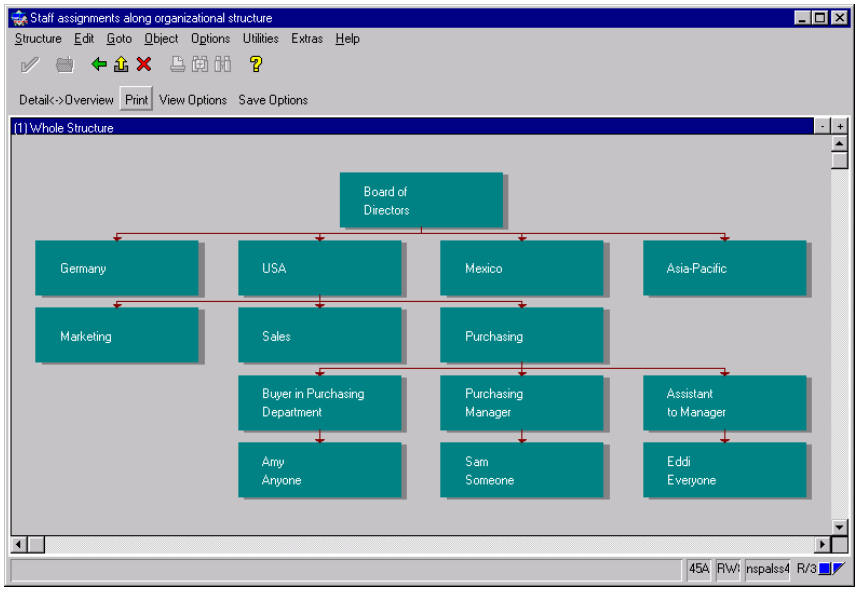


Repeat steps 22–26 to assign additional holders to positions.

27. Select the root organizational unit.
28. Choose *Structural graphics*.



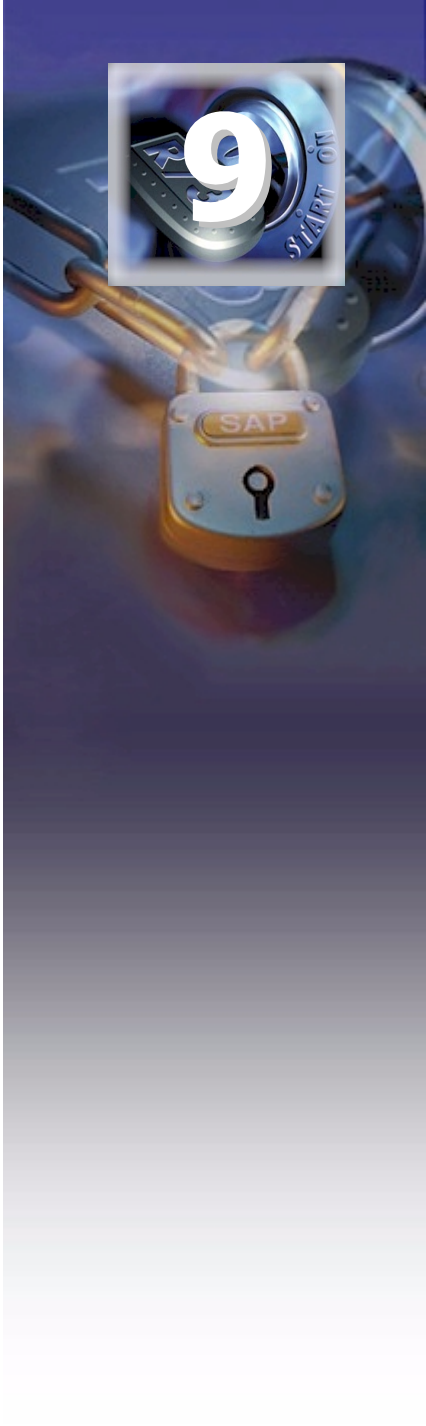
29. *Structural Graphics* allows you to view a graphical depiction of organizational plans and to create (and work with) objects in a graphical format. *Structural Graphics* is particularly helpful when you want to move objects within structures.



The structural graphics displayed are adapted to fit the screen using the available options under *View options*.

Simple Maintenance allows you to rapidly organize a basic framework for this plan. Procedures for creating objects are streamlined for quick and uncomplicated entry. However, not all PD functionality is available.

Simple Maintenance operates in a tree structure format, which makes it easier to view and understand the relationships between objects in your plan.



Chapter 9: Infosystem Authorizations

Contents

Overview

The *Infosystem Authorizations* function in R/3 provides the opportunity to evaluate and compare your:

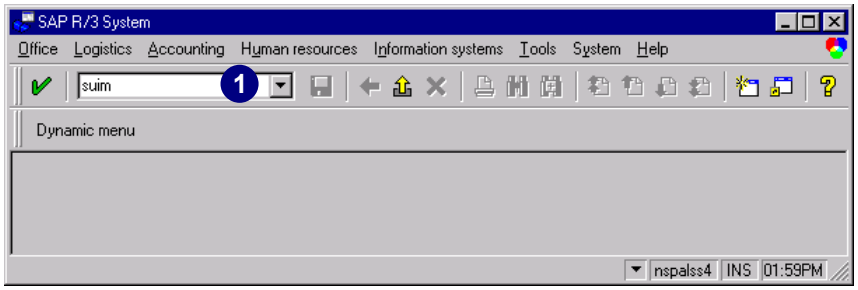
- Users
- Profiles
- Authorization objects
- Authorizations
- Activity groups
- Transactions
- Where-used lists
- Change Documents

You can search and evaluate this data using simple or complex criteria. Each generated output list allows you to drill down into more specific information on fields and values by clicking on the appropriate criteria.

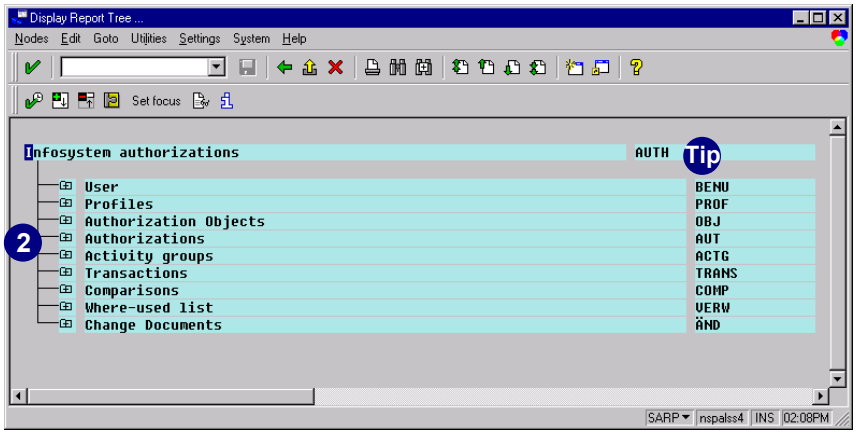
Displaying Information

To access the *Infosystem Authorizations:*

1. In the *Command* field, enter transaction **SUIM** and choose *Enter* (or choose *Tools* → *Administration* → *User maintenance* → *Repository Infosys*).



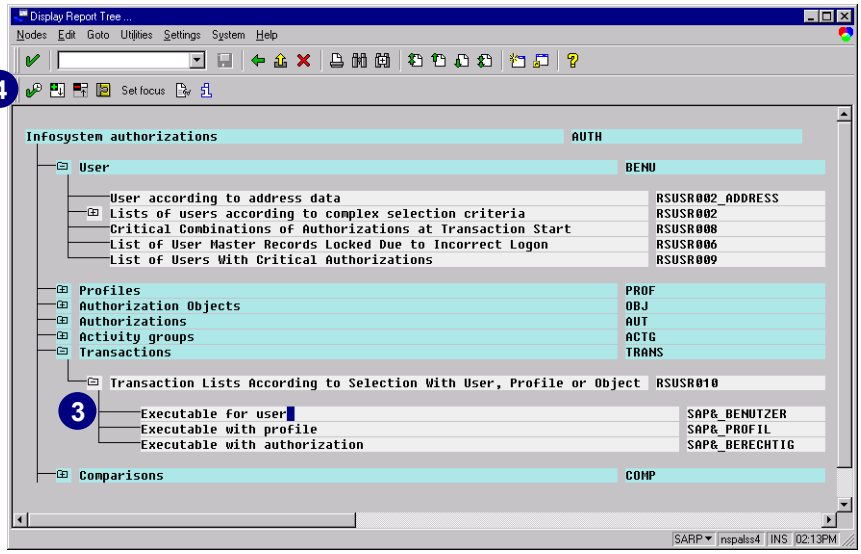
2. Select the area from which you would like to get information and expand the tree branch by clicking the node.



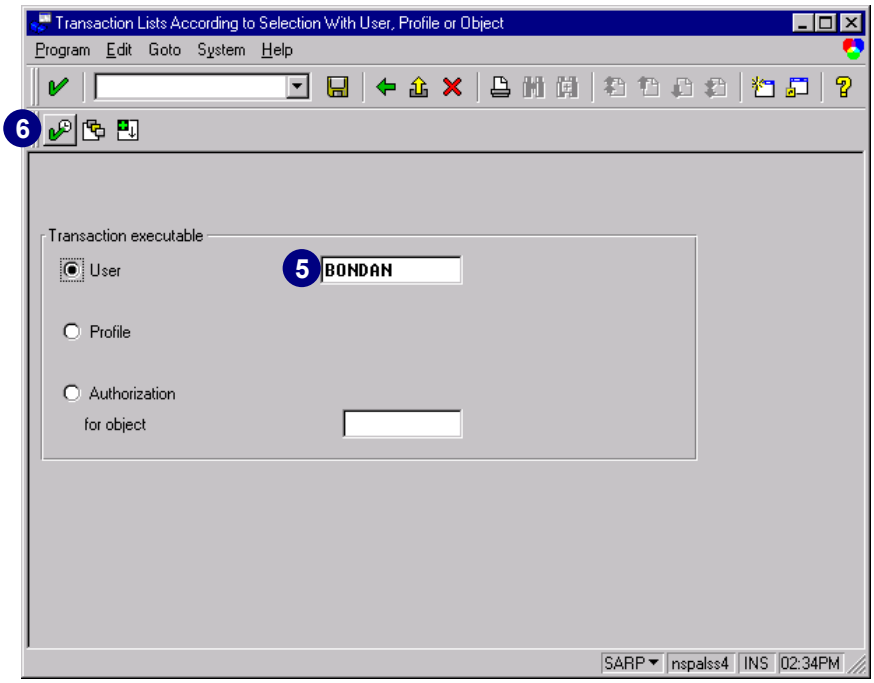
To view the technical names, choose *Settings* → *Technical names on/off.*

In our example, we chose the transactions that are executable by a specific user.

3. Select the desired report.
4. Choose *Execute*.

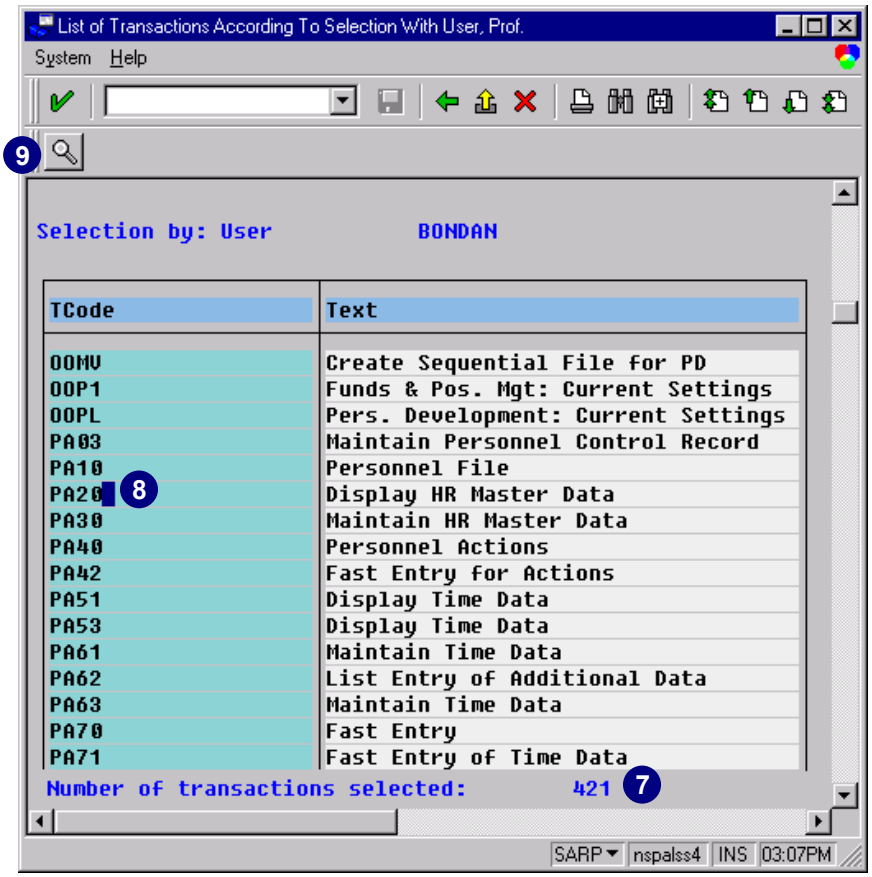


5. Enter the appropriate information in the report fields (for example, the user name).
6. Choose *Execute* to run the report.

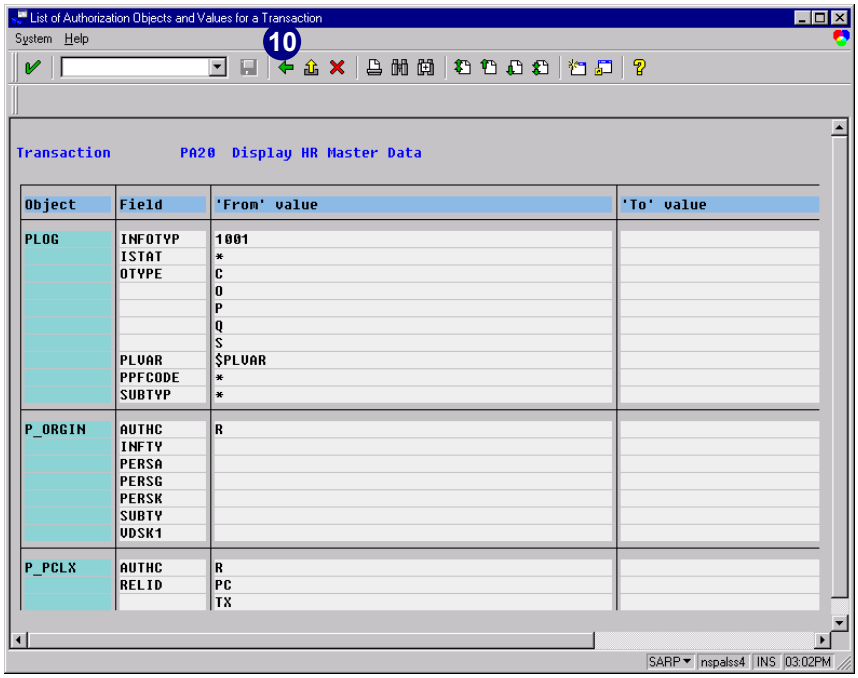


7. At the end of the list you can see the total number of transactions selected for this user (you may have to scroll down to view the entire list).
8. Click to select the transaction where you want to drill down for more detail.
9. Choose *Choose*.

   Expand the appropriate branches to display more information if needed.



10. Choose *Back*.

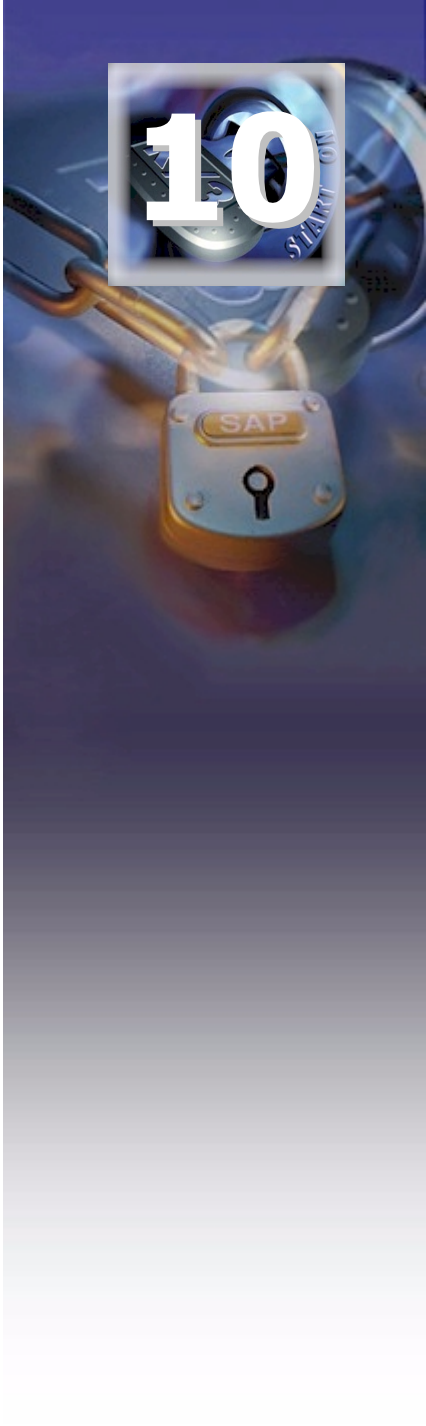


Drilling Down for Detailed Information

Double-clicking on a field in the output screen allows you, in most cases, to drill down for further information. This technique works for all reports in *Infosystem Authorizations.*

Additional Reports and Transactions

- Run transaction **`RE_RHAUTH00`** to evaluate structural authorization in HR.



Chapter 10: Predefined Activity Groups and Authorization Profiles

Contents

What Are Predefined Activity Groups

Predefined activity groups (PDAGs) are activity groups that have already been created by SAP. They can serve as templates for your user activity groups but they are not part of the standard R/3 Release 4.5A/B. PDAGs come as transport files that include the activity groups and the related profiles which need to be imported into your system. The PDAGs provide a foundation for further security configuration of a customer's specific requirements. PDAGs are easily adaptable to the customer's needs, and their user's current transaction and report access rights can be changed as needed.

Advantages of Predefined Activity Groups

There are several advantages of PDAGs:

- A reduction in R/3 security implementation time, cost, and complexity

  PDAGs can save a customer up to 15 days of security implementation time and reduce project costs. This time and expense reduction is made possible by predefining the most common job roles within a company. An activity group is created for each of these job roles; the roles that normally access these transactions and reports are preselected. Authorization data is also maintained for each activity group. All you have to do is import the data into the correct client and assign these PDAGs to users.

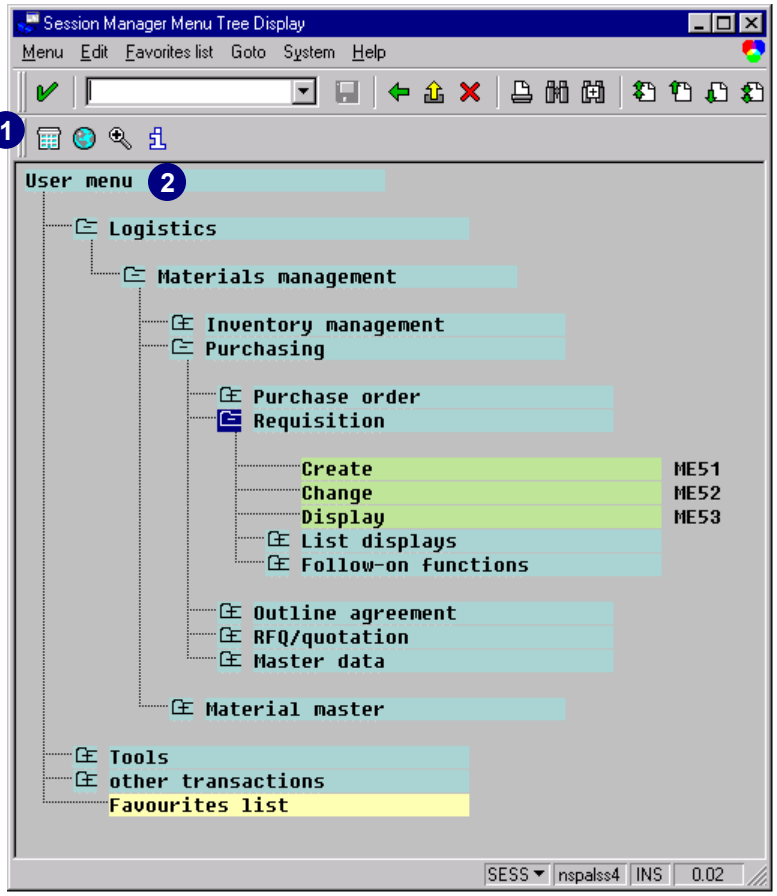
- Valuable customer benefits are felt immediately

  The most common job roles within an enterprise, such as a buyer or customer service representative, are predefined and operate out of the box. PDAGs also enable the customer to get a head start on learning about R/3. Once these groups are imported into the system and assigned to users or PD objects, these users can run standard R/3 business transactions.

To help you understand how a user can work immediately in his area using predefined activity groups, we created user *Wilson* in the following example:

1. User *Wilson* was assigned to the predefined activity group *BUYER*.

2. User *Wilson* logged on the R/3 System and ran transaction **SESS** *(Session Manager)*. *Wilson* can only see the functionality in R/3 he or she is allowed to use (*User menu*).



The benefits of predefined activity groups also continue during different project phases:

- During project kickoff, groups help the security administrators ensure that everyone has only the access rights they need, which will prevent data loss during configuration.
- During security implementation, the groups support the setup of security administrators and job roles.

Which Activity Groups Are Predefined

The following list contains the job roles that have PDAGs and, therefore, generated predefined authorization data. These predefinitions are based on feedback gathered from our American customers and experienced SAP consultants.

The activity groups are no longer identified by their object IDs, unlike previous releases. They are now identified by their abbreviation.

Financial Accounting (FI)

Activity Group Name	Activity Group Abbreviation
FI: Accounts Payable Clerk	F_A-Pclerk
FI: Accounts Payable Supervisor	F_A-Psuper
FI: Accounts Receivable Clerk	F_A-Rclerk
FI: Accounts Receivable Supervisor	F_A-Rsuper
FI: Accounting Clerk	F_AcctClerk
FI: Accounting Manager	F_AcctMgr
FI: General Ledger Accountant	F_Gen_Led_Acct
FI: Fixed Assets Accountant	F_FixAssetAc

Materials Management (MM)

Activity Group Name	Activity Group Abbreviation
MM: Buyer	M_Buyer
MM: Buyer with Reporting Authorization	M_Buyer_Reporting
MM: Inventory Management	M_Invent_Mgmt
MM: Inventory Management Supervisor	M_Invent_Mgmt_Super
MM: Physical Inventory	M_Phys_Invent
MM: Physical Inventory Supervisor	M_Phys_Invent_Super

Sales and Distribution (SD)

Name of the Activity Group	Activity Group Abbreviation
SD: Customer Service Representative	V_Cust_Ser_Rep
SD: Customer Service Manager	V_Cust_Ser_Mangr
SD: Delivery & Shipping Clerk	V_D&S_Clerk
SD: Delivery & Shipping Manager	V_D&S_Mangr
SD: Accounts Receivable Clerk	V_Acc_Rec_Clerk
SD: Account Receivable Manager	V_Acc_Rec_Mangr
SD: MIS	V_MIS

Basis Administration (BC)

Activity Group Name	Activity Group Abbreviation
BC: User Administrator	S_Admin_User
BC: Authorization Profile Administrator	S_Admin_Profile
BC: Authorization Data Administrator	S_Admin_Auth_Data
BC: Printing Authorizations (Spool)	S_Printing
BC: OSS Logon Authorization	S_OSS_Logon
BC: End-User Basis Authorizations	S_End_User_Basis
BC: Operator	S_Operator
BC: Developer	S_Developer
BC: Basis – Display Only	S_Basis_Show
BC: Standard SAPoffice Authorizations	S_SAP_office
BC: SAP_ALL Restricted	S_SAP_ALL
BC: Use Session Manager	S_Use_Sess
BC: Use Authorization Check SU53	S_Use_SU53

Predefined Data for the Activity Groups

We have already maintained the appropriate authorization profiles for each activity group, with all open authorization fields maintained as specifically as possible. Because we do not know your specific enterprise settings, all open customer-specific authorization fields, such as authorization group fields, material type fields, etc., are generically maintained with an asterisk (*). This way, you can work with the PDAGs right out of the box, and not lose the flexibility to alter them later. This chapter describes how to change activity groups and postedit authorizations. With this information at your disposal, you are prepared to use the system.

Adapting the Predefined Activity Groups to Your Specific Needs

If you want to use the predefined activity groups only as a template, you can copy them. This way you have the opportunity to create your enterprise-specific name for the authorization profile you plan to generate.

Installing the Predefined Activity Groups

After the new R/3 System has been installed, import the groups as a basis for further security implementation. Before beginning the import, we strongly recommend that you read chapters 1 and 2 of this guidebook.

The transport files can be obtained from one of two sources:

- The latest transport files are available from the Simplification Group web page: *http://www.saplabs.com/auth*
- From the CD on the inside back cover of this guidebook, you can find the transport files for Release 4.5A and 4.5B.

Copy or download the files on your server. You get two files for each release, a data file and a co-file.

Release	CD-Folder	Data file	Co-file
4.5 A	*PredefinedAG45\45a*	*R900051.X5A*	*K900051.X5A*
4.5 B	*PredefinedAG45\45b*	*R900158.D5B*	*K900158.D5B*

Data File	Co-File	Transport request	Description AG = Activity Group data; AP = Auth. Profile data
R900051.X5A	K900051.X5A	X5AK900051	BC 4.5x AG/AP Printing Authorizations (Spool)
R900158.D5B	K900158.D5B	D5BK900158	BC 4.5x AG/AP Logon to OSS Authorization
			BC 4.5x AG/AP End-User Basis Authorizations
			BC 4.5x AG/AP User Administrator
			BC 4.5x AG/AP Authorization Profile Administrator
			BC 4.5x AG/AP Authorization Data Administrator
			BC 4.5x AG/AP Operator
			BC 4.5x AG/AP Developer
			BC 4.5x AG/AP Basis – only Display authorizations
			BC 4.5x AG/AP Standard SAPoffice authorizations
			BC 4.5x AG/AP SAP_ALL restricted
			SD 4.5x AG/AP IT/SD Representative
			SD 4.5x AG/AP Accounts Receivable Manager
			SD 4.5x AG/AP Accounts Receivable Clerk
			SD 4.5x AG/AP Delivery & Shipping Manager
			SD 4.5x AG/AP Delivery & Shipping Clerk
			SD 4.5x AG/AP Customer Service Mgr
			FI 4.5x AG/AP Fixed Assets Accountant
			FI 4.5x AG/AP Accounts Receivable Clerk
			FI 4.5x AG/AP Accounts Payable Clerk
			FI 4.5x AG/AP General Ledger Acct
			FI 4.5x AG/AP Accounting Manager
			FI 4.5x AG/AP Accounting Clerk
			FI 4.5x AG/AP Accounts Payable Supervisor
			FI 4.5x AG/AP Accounts Receivable Supervisor
			MM 4.5x AG/AP Buyer
			MM 4.5x AG/AP Buyer with Reporting authorization
			MM 4.5x AG/AP Inventory Management
			MM 4.5x AG/AP Inventory Management Supervisor
			MM 4.5x AG/AP Physical Inventory
			MM 4.5x AG/AP Physical Inventory Supervisor

To install the PDAGs:

1. Download the transport files from the webpage or copy them from the attached CD onto your system.
2. Copy the predefined data and co-files in the appropriate directory on your server.
3. Import the objects from the transport files into the target client.

The following steps are written primarily for Windows NT and UNIX. If you are working in AS400, an additional step is necessary to format the file in *EBCDIC* (please refer to Online Service System note *62739*).

Obtain the passwords for the SAP user <*SAPSID*>*adm* (such as *devadm* if your R/3 System ID is DEV) and the R/3 user *DDIC* (client 000) from your system administrator, because you will need them later in the installation.

Before proceeding, verify that the *SAP Correction and Transport System* (CTS) was properly set up during your R/3 installation. Later, we show you how to check whether the CTS is working properly.

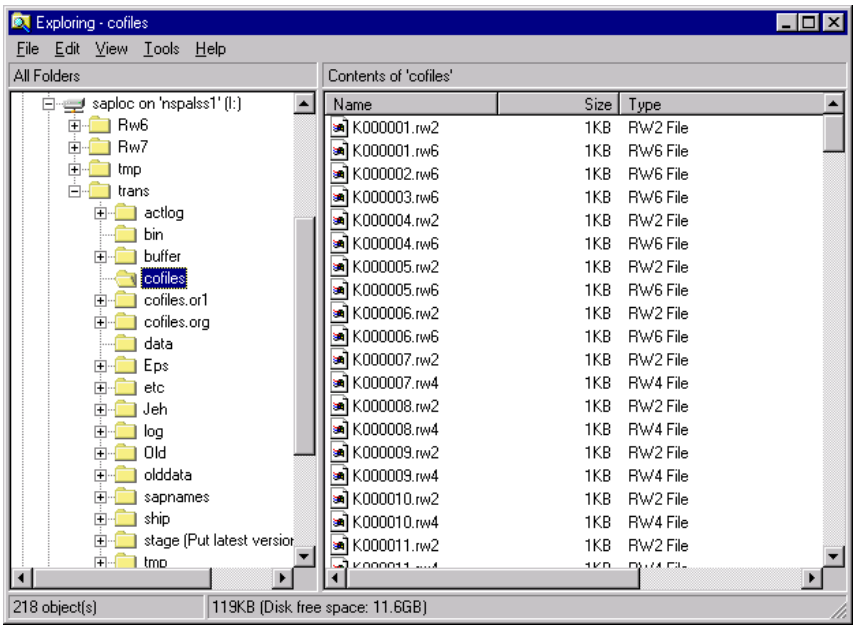
Copying the Predefined Data Files onto your System

Attached to this guide you will find the PDAG transport files for Releases 4.5A and 4.5B. You can also download them from the Simplification Group web page (see earlier this chapter).

1. Copy the appropriate file to a new directory on your machine.
2. Ensure that adequate space is available. You will need approximately 6 MB on your hard drive for the files, one starting *R900*… and the other *K900*….

1. Copy or ftp the files below into the */cofiles* subdirectory on your server. This subdirectory is usually located under *…/sap/trans/cofiles*.

   K900051.X5A Release 4.5A
   K900158.D5B Release 4.5B



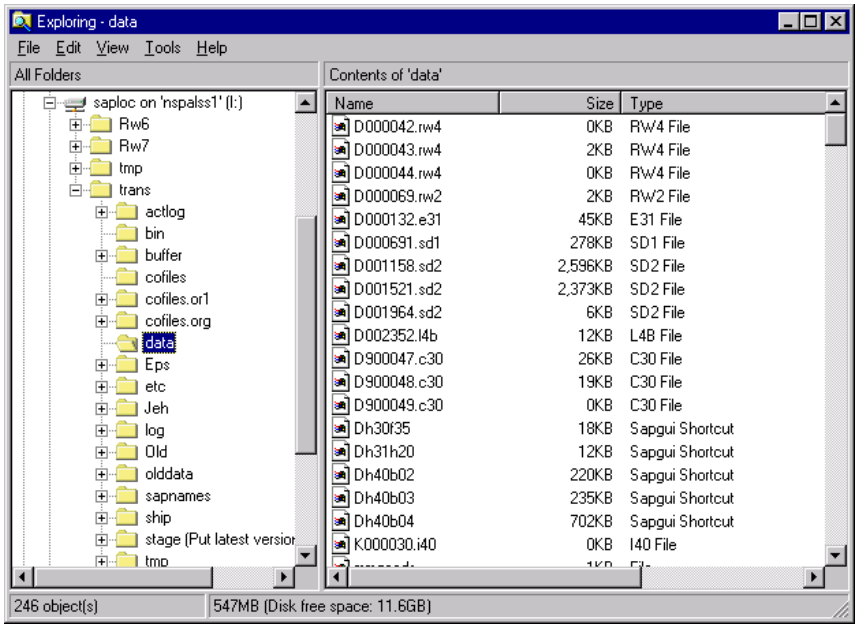
Caution

This screenshot does not contain the current valid transport number.

2. Copy or ftp the files below into the */data* subdirectory on your server. This subdirectory is usually located under *…/sap/trans/data.*

   R900051.X5A Release 4.5A

   R900158.D5B Release 4.5B



Caution

This screenshot does not contain the current valid transport number.

TechTalk

When copying the predefined data files onto your system, the differences among NT, UNIX, and AS400 are noticeable. Keep in mind the following:

- The screenshots above are taken from the Windows NT Explorer for an NT system.
- AS400 screenshots for this step are not available.
- In a non-Windows environment, the file structure will be the same as the AS400 structure.
- In UNIX use FTP for copying files, and in NT copy the files, for example with Windows NT Explorer.
- The TP commands are also the same, with the exception that under AS400, the body of the command must be enclosed in single quotes.

For example:

```
NT, UNIX:   tp checkbuffer x5a
AS400:      tp 'checkbuffer x5a'
```

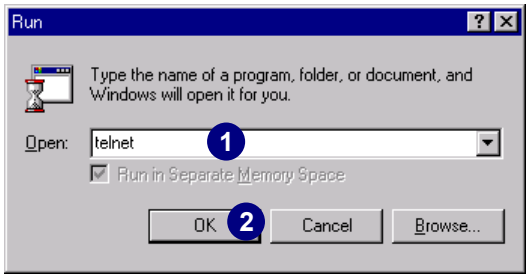
Importing Objects from the Transport Files into the Target Client

You need to know if your R/3 System is running on an NT-Server or UNIX-Server, because there are some differences in importing the transport files into the system (see above).

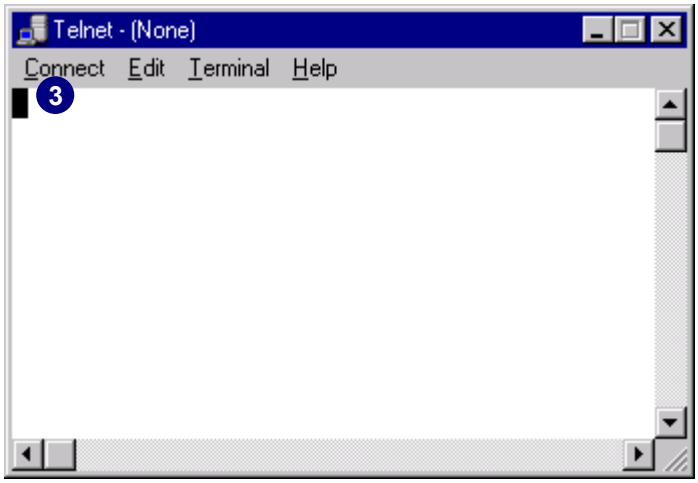
Importing onto a UNIX-Server

Start Telnet by choosing from the windows task bar *Start* → *Run* (or use a similar tool).

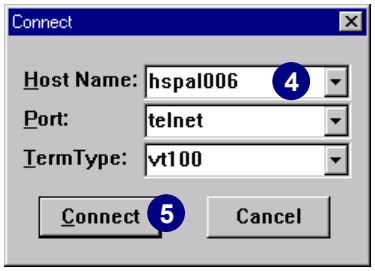
1. Enter **`telnet`**.
2. Choose *OK*.



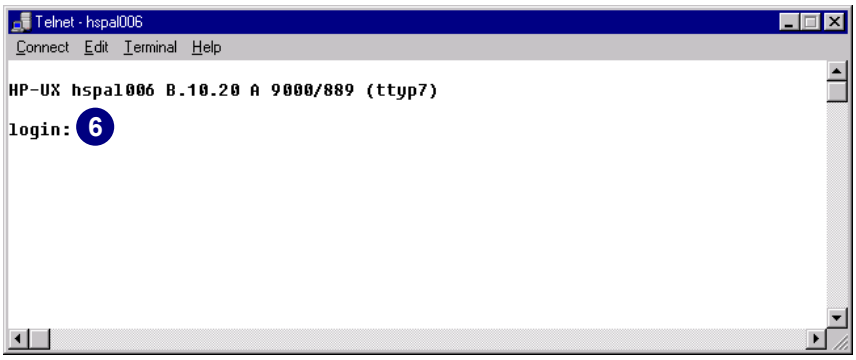
3. Choose *Connect* → *Remote System.*



4. Enter the server name to which you want to connect (for example, our server is called *hspal006*).
5. Choose *Connect*.

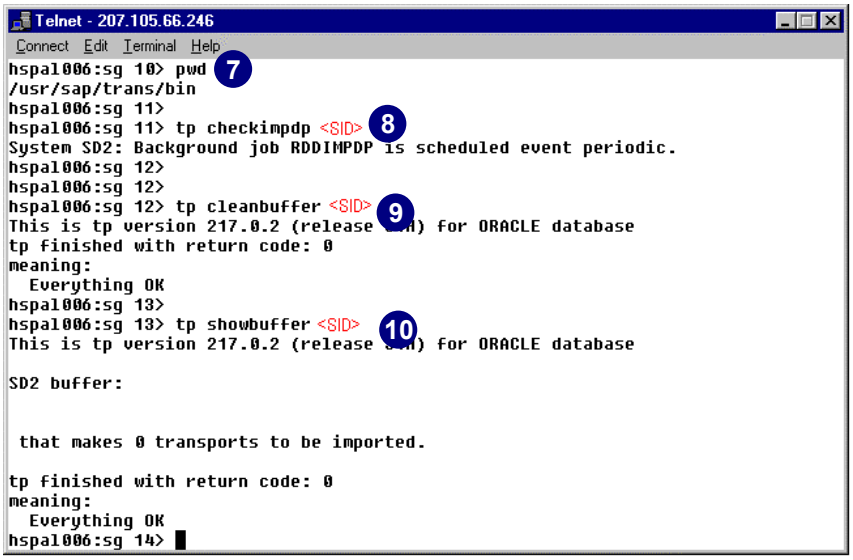


6. Log on to the operating system with an appropriate user and password, user **<SAPSID>adm** (for example, **devadm** if your R/3 System ID is *DEV*).



7. Switch to your transport directory, */usr/sap/trans/bin (our example)*. It might be on a logical drive.
8. Enter **tp checkimpdp <SID>,** replacing **<SID>** with the system ID number of your R/3 System. For example, if your ID is DEV, enter **tp checkimpdp DEV.**

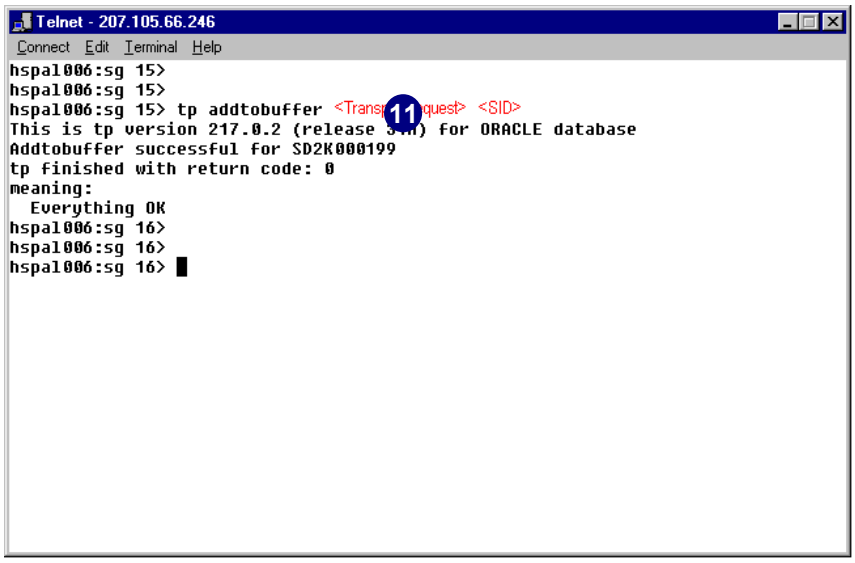
   If the response is anything other than *System <SID>: Background job RDDIMPDP is scheduled event periodic,* something is wrong with your transport system that must be fixed before you can continue.
9. Enter **tp cleanbuffer <SID>** to empty the transport buffer for your system. Remember to replace **<SID>** with your system ID.
10. Enter **tp showbuffer <SID>.** The output shows that the buffer is clean.



11. Enter **`tp addtobuffer <TransportRequest> <SID>`** to bring the first transport into the buffer. You must repeat this command for each transport request you would like to add to the buffer.

    Replace **`<TransportRequest>`** with the actual transport request number **`X5AK900051`** for release 4.5A, or **`D5B900158`** for release 4.5B, and replace **`<SID>`** with the R/3 System ID.

    For example, enter **`tp addtobuffer X5AK900051 DEV`** (This screenshot does not contain the current valid transport number).



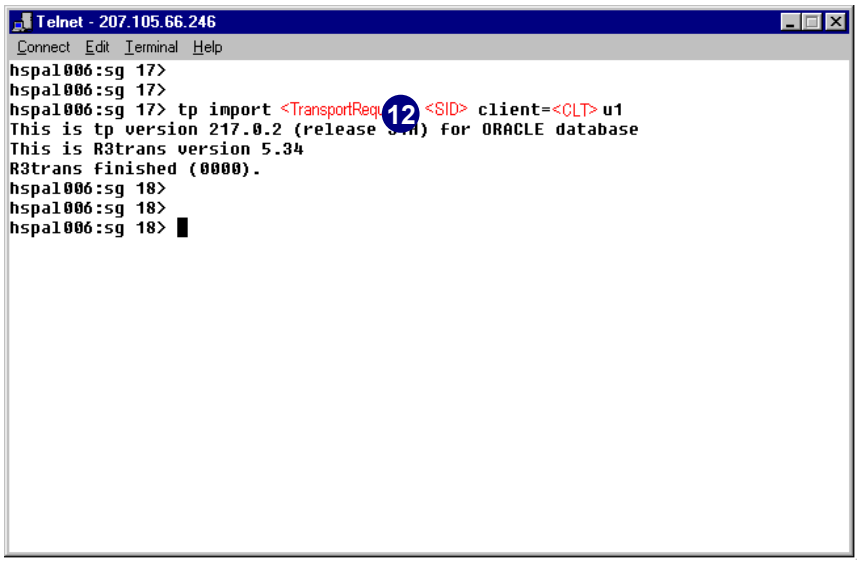
12. We are now ready to import. Enter **`tp import <TransportRequest> <SID> client=<CLT> u1.`** Make sure that you are importing to the correct client. Replace **`<CLT>`** with the client number (for example, **`220`**) to which you want to import the PDAGs.

    Depending on your system's speed and configuration, the import job could run for several minutes.

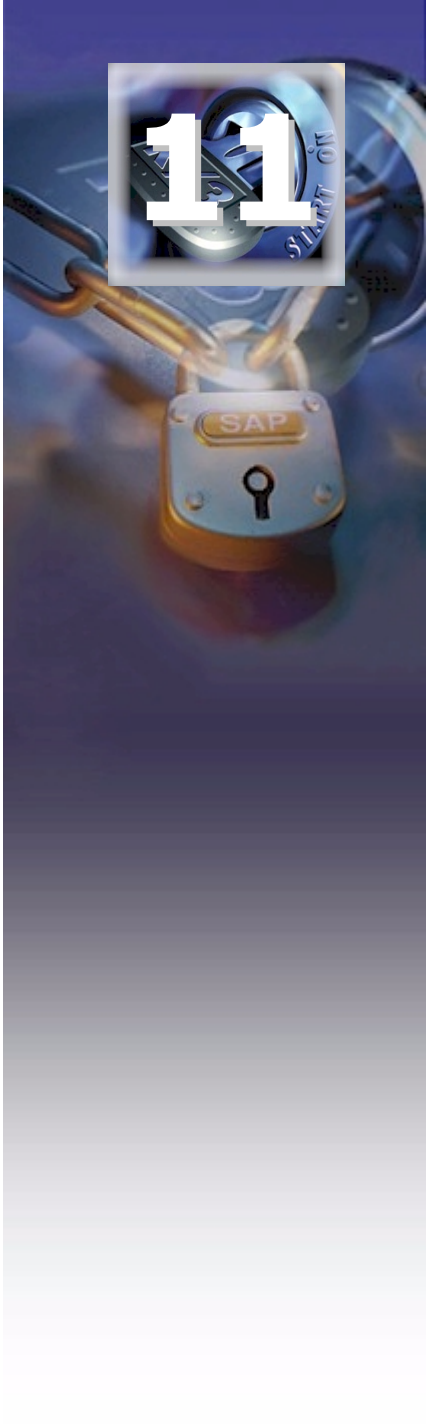
    For example, enter **`tp import X5A900051 DEV client=220 u1`**

    Congratulations. You just imported the PDAG.

    (This screenshot does not contain the current valid transport number.)



After completing the transport request import, all of the delivered PDAGs are within the activity group maintenance transaction *PFCG*. You do not have to regenerate the authorization profiles; only a user compare is required.



Chapter 11: Using the Session Manager

Contents

Overview

With the SAP Session Manager transaction *SESS*, you can display the various R/3 menus in your R/3 System and start your application from the menu. You can manage your sessions in one or more R/3 Systems and in different SAP clients. Users are usually only authorized to run functions from their user menu.

The following types of menus are available:

- User menus
- Company menus
- Standard SAP menus

Session Manager Benefits

The Session Manager is another way that SAP responds to R/3 customer feedback. This new tool offers two main benefits that allow R/3 users to easily navigate through the applications. The tool allows users to customize R/3 menus and provides a new user interface for interaction with R/3.

The most significant aspect of the Session Manager is its ability to narrow the menu scope. During a system implementation, a corporate menu is automatically generated with the R/3 functions a company actually uses. Based on this corporate menu, a user-specific menu is automatically created when activity groups are created. This menu contains the necessary application components and transactions. The Session Manager's user interface, transaction *SESS*, simplifies work with R/3 applications.

You can select any of these R/3 views:

- The complete SAP-Standard menu

  This menu furnishes a complete view of R/3.
- Your company menu

  This enterprise-specific menu contains only the transactions your enterprise actually uses.
- Your user-specific menu

  This menu contains only the transactions your user is authorized to use.

These selections substantially reduce clutter and help users focus on their immediate tasks. To begin a transaction, just double-click the menu entry. With the Session Manager, you can also individually configure your own interface, such as placing frequently used transactions in a "favorites" list. This way, the functions you most frequently need are at your fingertips.

The user menu is available on all machines when you log on to R/3. There are no locally stored settings, which reduces administrative overhead.

Menu Configuration

The company menu shows only those parts of the SAP standard menu that are actually used, while the user-specific menu displays only those parts needed by, or restricted for, the user. During an R/3 implementation, using the Implementation Guide (IMG) task *Generation of the Enterprise IMG*, you can select the application components that you need. These components automatically generate the company menu for the Session Manager (see chapter 2).

Generating the user-specific menu from the company menu takes place in two stages. The first stage involves setting up activity groups (see chapter 4). The company menu is presented as a tree, with submenus as branches and individual transactions as leaves. Individual menu branches are selected for specific job roles from the company menu by clicking on parts of them.

The second step involves generating appropriate authorization profiles and assigning activity groups to individual users (multiple assignments are also possible). User menus are then automatically generated. If the user administrator changes the activity group user allocation, the new menu is automatically generated the next time the Session Manager is started. Through menu configuration, the Session Manager provides new ways for users and administrators to more productively work with R/3.

Platforms and Availability

The Session Manager (transaction *SESS*) is platform independent.

How to Work with the Session Manager Transaction SESS

To benefit from the SAP Session Manager user menu, the following steps are required:

1. Set up activity groups (chapters 4).

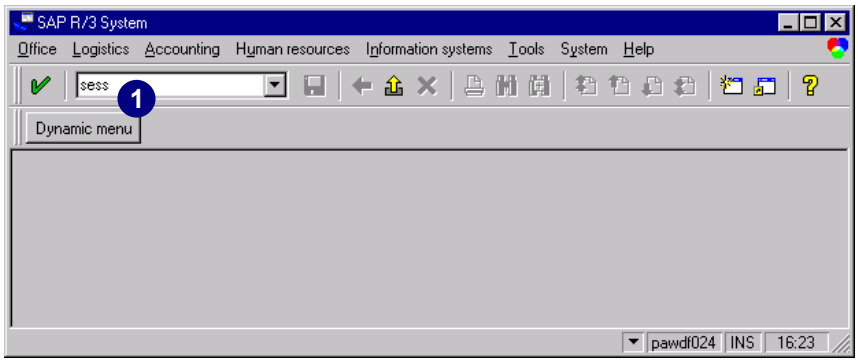
   Set up an activity group with access rights for transaction *SESS* and *SU53* and for other rights, such as printing. Each user who works with *SESS* should have permission to start *SESS*. Since transaction *SU53* is protected by the authorization check against object *S_TCODE*, we recommend that you provide all users access rights to this transaction. The transactions *SU53* and *SESS* can be found in the menu tree in the PG under *Other transactions*.

2. Generate the authorization profile(s) (chapters 5–6).
3. Assign activity groups to R/3 users or PD objects (chapter 8).
4. Assign the activity group that grants access rights for *SESS.*
5. Update the user master records (chapter 8).
6. Let the users log on to R/3, with transaction *SESS*, and test their access scope.

The screenshots on the following page show the different menus running transaction *SESS*. Users can choose between the:

- User menu
- Company menu
- SAP standard menu

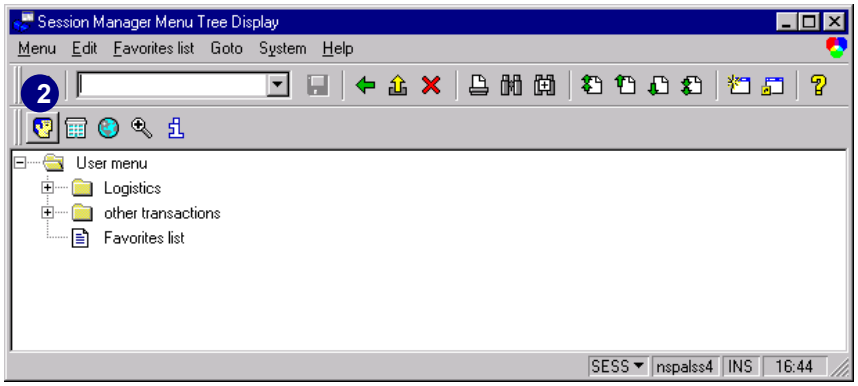
1. In the *Command* field, enter transaction **SESS** and choose *Enter* (or choose *Dynamic menu*).



To see the different kind of menus:

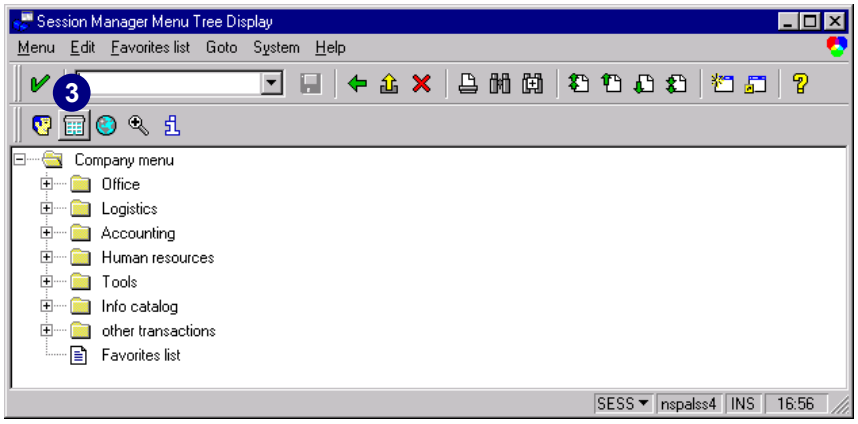
2. Choose *User menu*.

   The *User menu* contains the personal user menu.



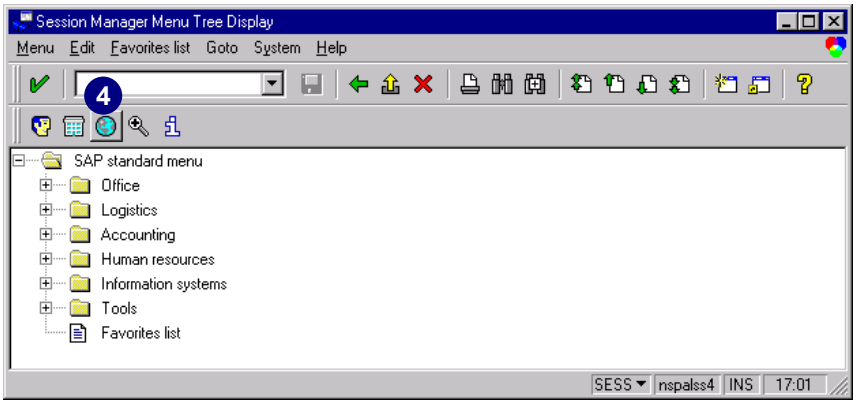
3. Choose *Company menu*.

   The *Company menu* contains a menu tree reduced to the company.

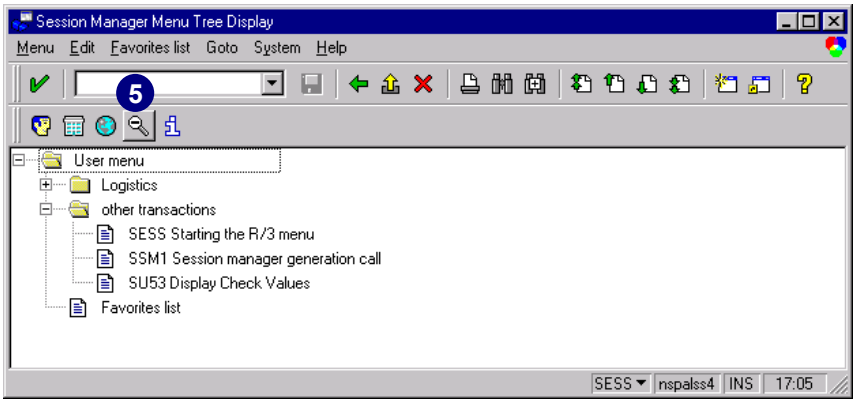


4. Choose *SAP menu*.

   The *SAP menu* contains the menu tree delivered by SAP.

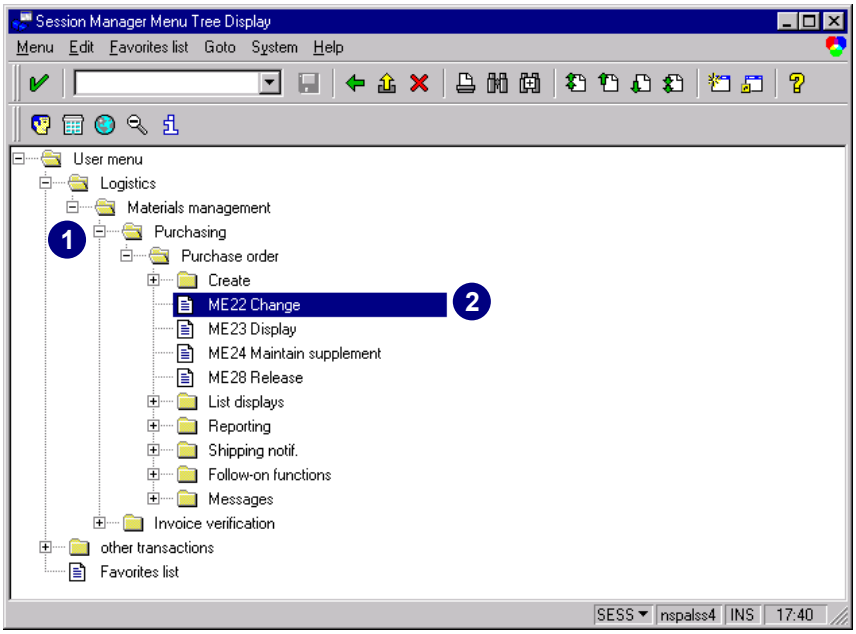


5. Choose *Technical names on/off* to switch the technical names on or off.

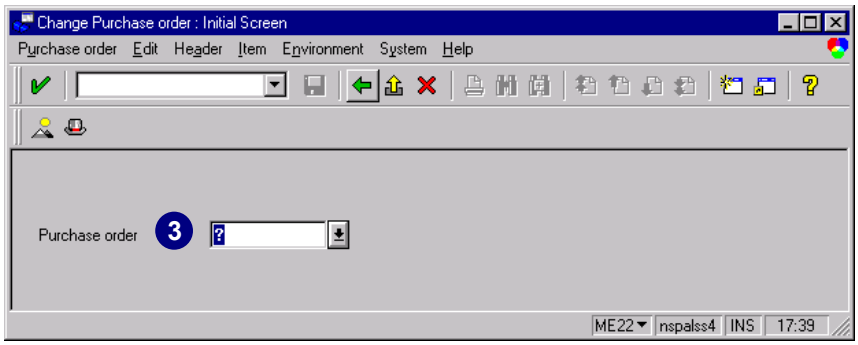


How to Start Transactions from the Menu Tree in Transaction SESS

1. Expand the appropriate menu branch by clicking the node (+).
2. Double-click the desired menu item, for example *ME22 Change (Purchase order)*.



3. The transaction starts in a new window.

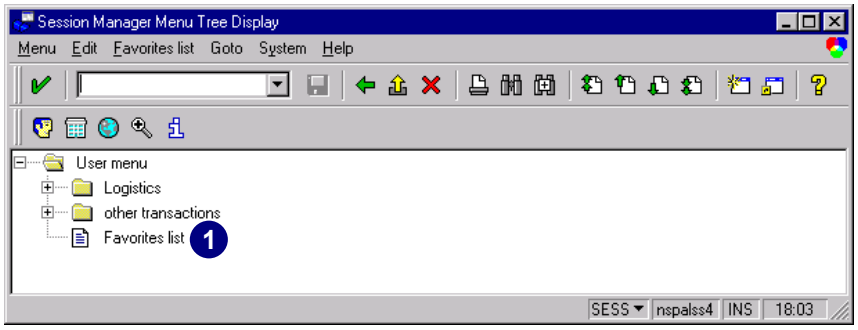


How to Maintain a Favorites List in Transaction SESS

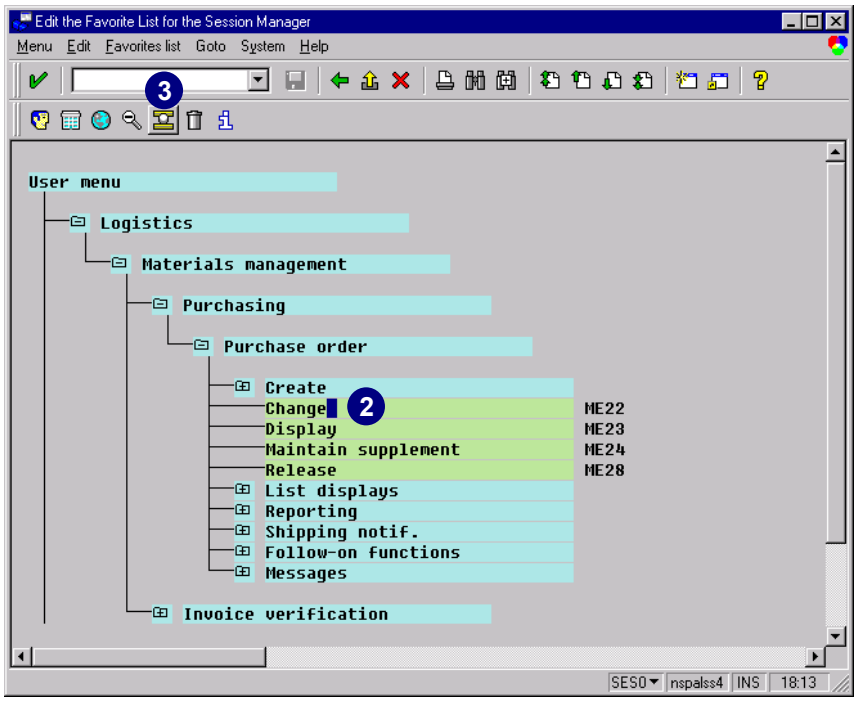
You can include heavily used menu options in a personal favorites list.

You can reach the favorites maintenance from every transaction with the relevant menu option *System* → *User profile.*

1. Double-click the item *Favorites list* (or choose *Goto* → *Favorite maint.*)

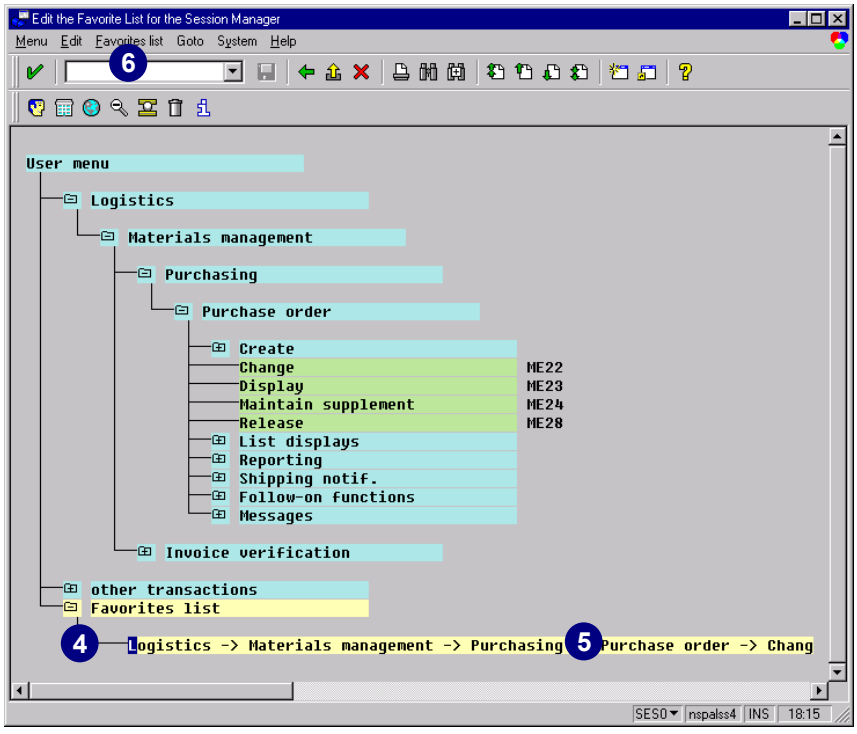


2. Expand the appropriate menu branch by clicking the node (+) and select the transaction you would like to add to your favorites list.
3. Choose *Create favorites*.

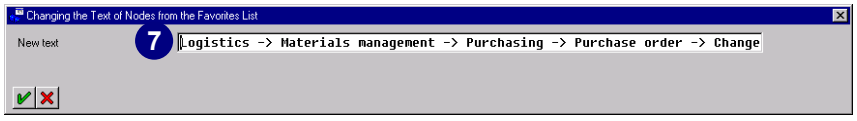


4. The new entry is created in the favorites list.

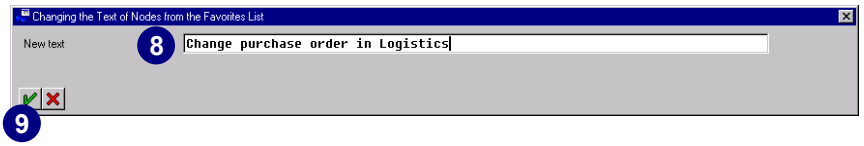
   (The following steps are optional and need to be performed only if you wish to change the default name in a shortcut into your own words.)
5. Select the new entry.
6. Choose *Favorites list* → *Change favorites*.



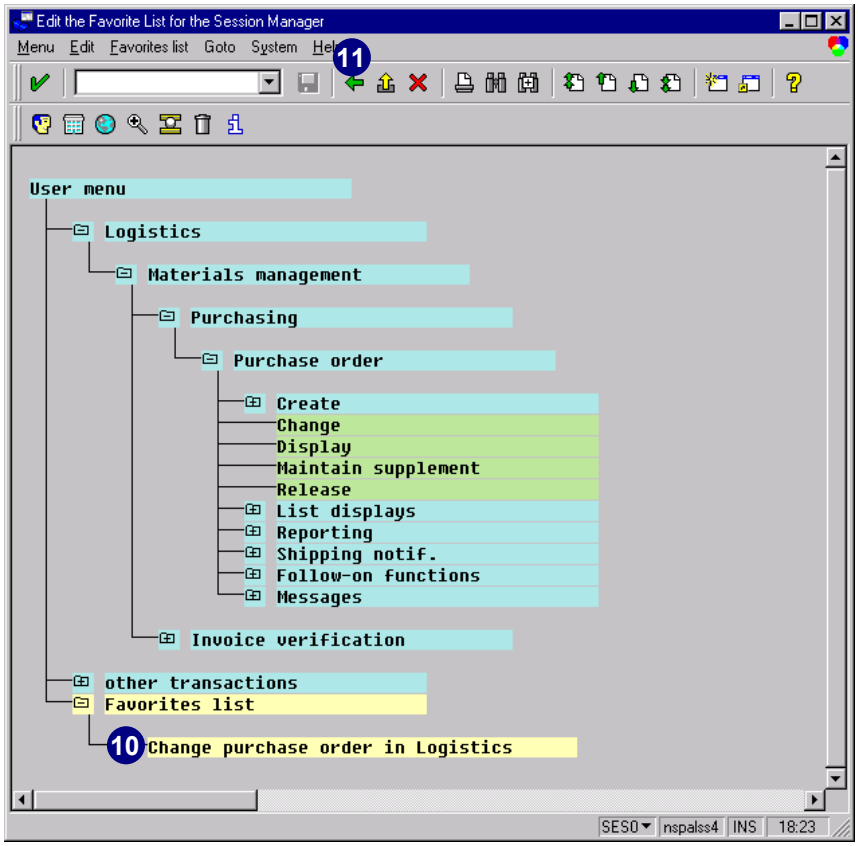
7. The SAP term appears.



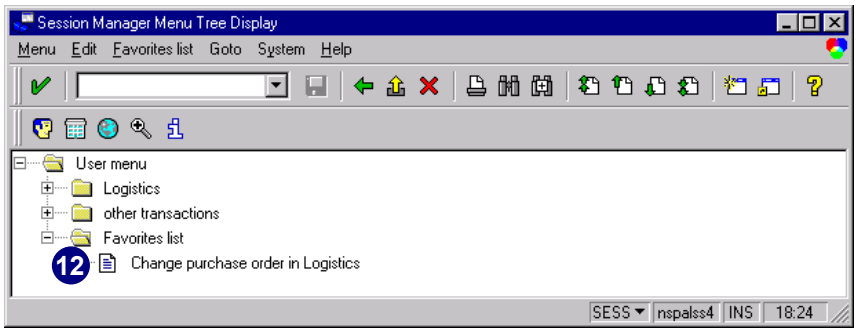
8. Now you can change the text for the shortcut as you like (we changed the text to *Change purchase order on Logistics*).



9. Choose *Enter*.
10. Your changes now appear.
11. Choose *Back*.

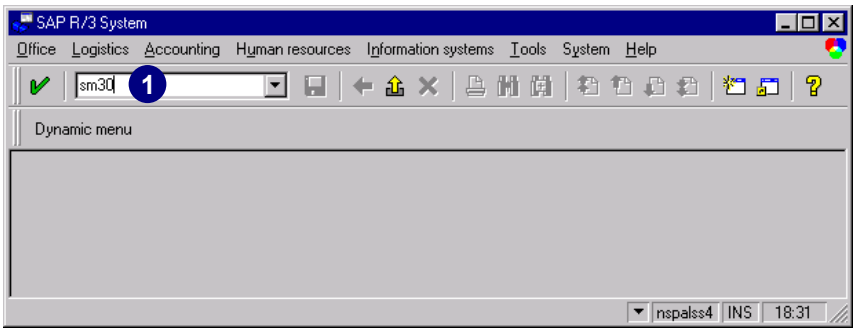


12. Now you can work with this newly created and renamed favorite in your *Session Manager* menu tree.

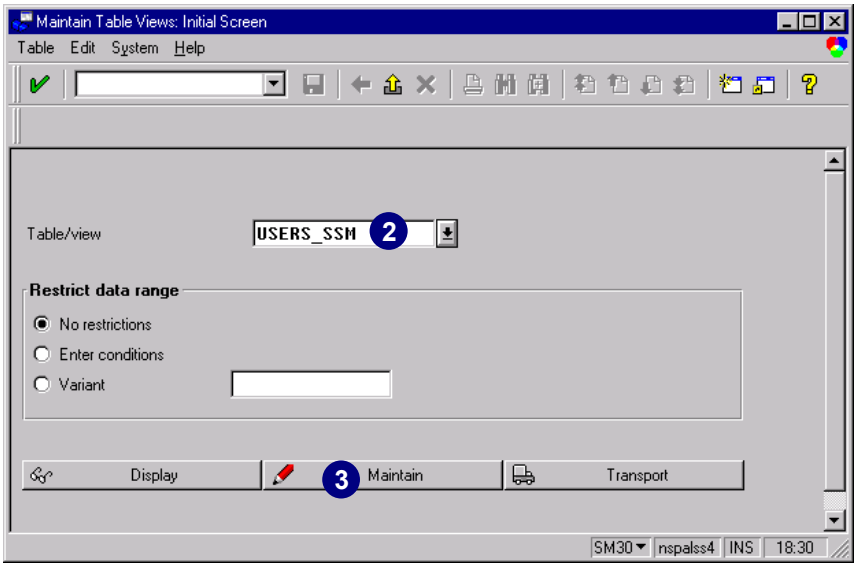


Customizing the Session Manager

1. In the *Command* field, enter transaction **SM30** and choose *Enter*.



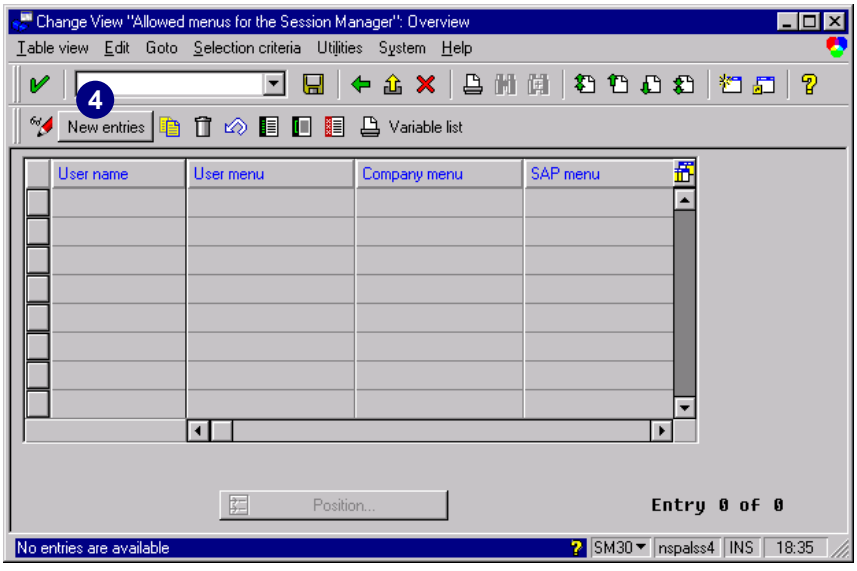
2. Enter **USERS_SSM** in the *Table/view* field.
3. Choose *Maintain*.



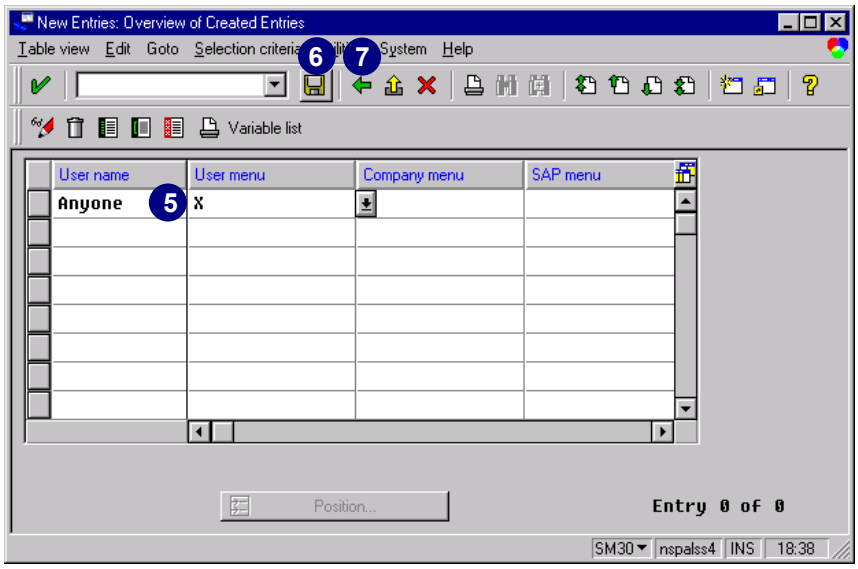
   In this view, you can maintain all users and determine how many menus they can see.

   The first time you maintain this view, it shows no entries.

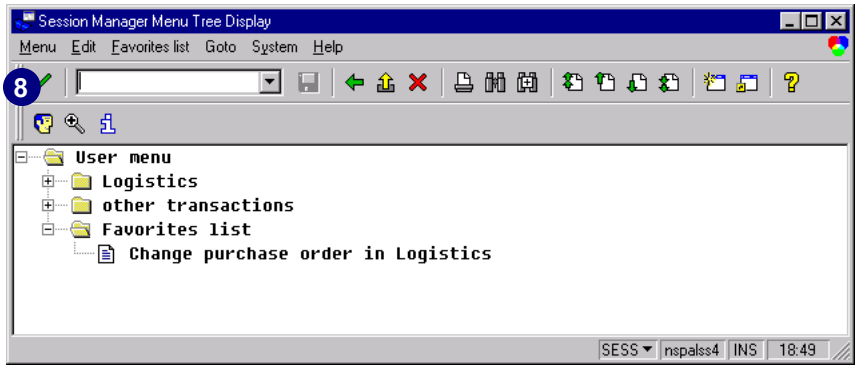
4. Choose *New entries*.

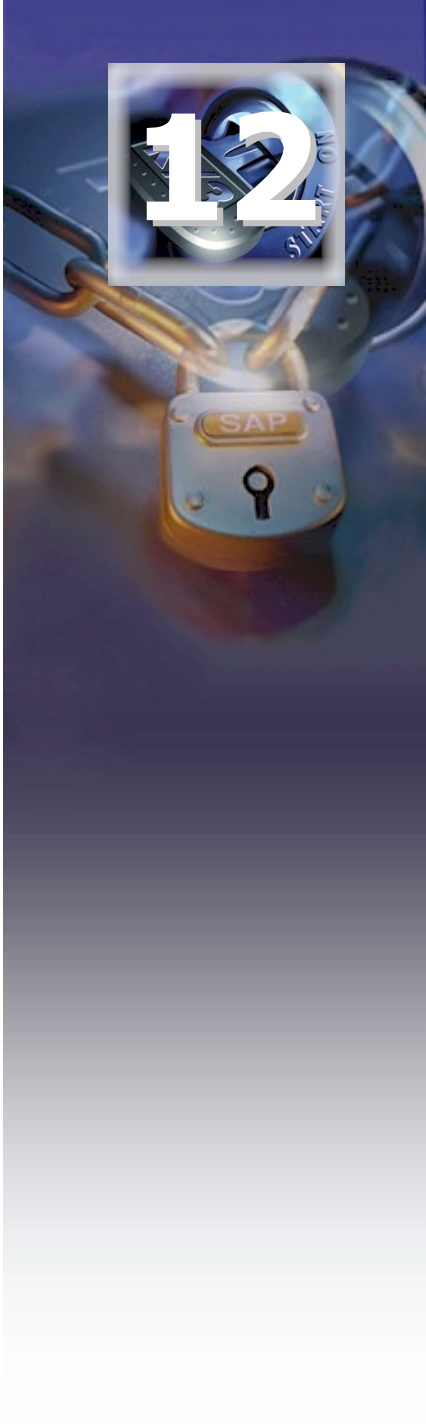


5. Enter a user name and an **`X`** (for "yes") in the appropriate menu column for the menu that this particular user should see when they log on. (We chose *User menu*, so Amy Anyone sees only the user menu when she logs on and no company menu or SAP menu.)
6. Choose *Save*.
7. Choose *Back* twice.



8. If user *Anyone* logs on and runs transaction **`SESS`**, she will see only the *User menu* icon.





Chapter 12: Transporting

Contents

Overview

Depending on the type of transport, you can transport the following items:

- Activity groups
- Authorization profile data
- Authorization data
- User master records

You can transport either between clients within an R/3 System, or between R/3 Systems.

Transports Between Clients

The items in the list above are client-dependent. Therefore, separate records, activity groups, profiles, and authorizations must be maintained for each R/3 client. Transaction *SCCL*, which must be run from the target client, transports user master records, authorization profiles, and authorizations between clients. As of Release 4.5A, activity groups are copied with Customizing.

When you carry out a transport, all user master records, profiles, and authorizations in the target system with the same names as items in the transport will be overwritten. Therefore, do not use *SCCL* if your target client contains authorizations and user master records that you want to keep. Only use *SCCL* to create a new client, with the objects *SAP_CUST* (users will be kept) or *SAP_UCUS* (users come from the source client).

Since activity groups belong to Customizing they are copied automatically during client copy. It is also possible to copy them manually (see below).

The transaction documentation contains additional information about the necessary authorizations. Use transaction *SCC1* to copy activity groups between existing clients manually.

To copy activity groups between clients:

1. Create transport request with the appropriate activity groups.
2. If you use transaction *SCC1*, do not release the transport.

   Transaction *SCC1* works with released and unreleased transports.
3. Log onto the other client.
4. Run transaction **`SCC1`**.
5. Choose the *Source client* and *Transport request* including the *task* number.
6. Execute.

The activity group(s) should now be active in transaction *PFCG*.

Transports Between R/3 Systems

You can transport authorization components, activity groups, and user master records between R/3 Systems. Components may be transported independently or with all of their associated authorizations.

Transporting Activity Groups

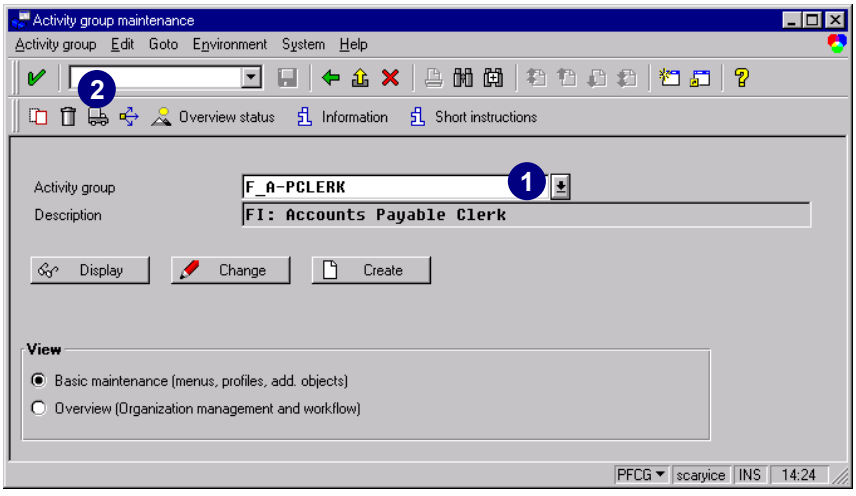
When you transport activity groups, this also transports the authorization profiles. Unlike previous releases, the profiles no longer have to be regenerated in the target system in transaction *SUPC*. However, you should compare the user master records when you import activity groups into the target system.

Once you have entered the activity group in a transport request, you should not make any more changes to the authorization profiles of that activity group. If you have changed profiles or generated them for the first time, you should enter the whole activity group in a transport request again.

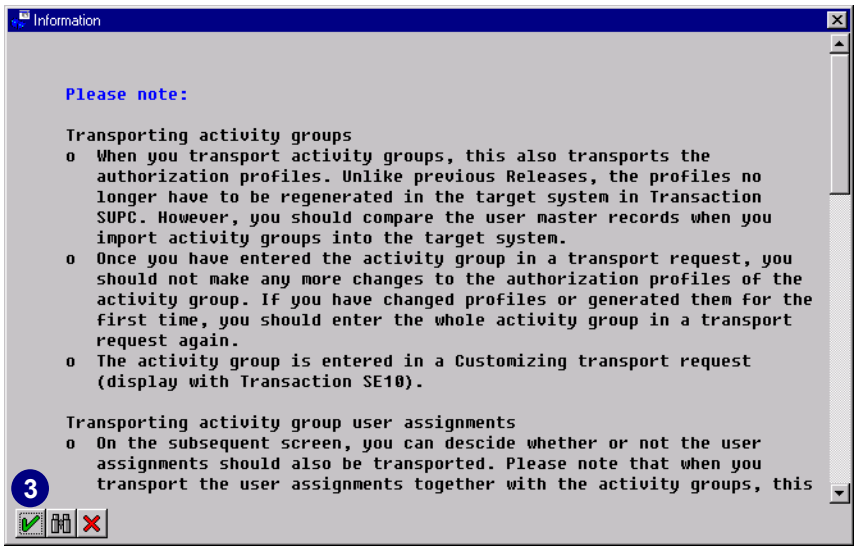
The activity groups entered in a transport request can be displayed with transaction *SE10*.

Transporting Single Activity Groups Using the Activity Group Maintenance Transaction

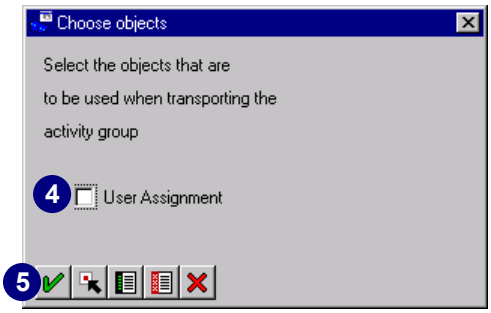
1. In the Profile Generator's (PG's) *Activity group maintenance* screen, select the activity group you would like to transport.
2. Choose the *Transport* button.



3. Choose *Continue*.



4. If you would like to transport the *User Assignment* as well, select *User Assignment*. If you do not want to transport the user assignment with the activity group, make sure it is deselected.
5. Choose *Continue*.



You can decide whether or not the user assignments should also be transported. Please note that when you transport the user assignments together with the activity groups, this action replaces the activity group user assignment in the target system.

If you are using the central user maintenance, you can only create user assignments in the central system. These can then be sent by request to the system group that you specified. If user assignments to activity groups were additionally transported, the central user administration display would be inconsistent. The users transported in this way would be removed at the next user distribution.

If you want to lock the system against importing user assignments from activity groups, you can specify this in the Customizing table *PRGN_CUST* (using transaction *SM30*). Enter a line with the identifier **USER_REL_IMPORT** and the value **NO**.

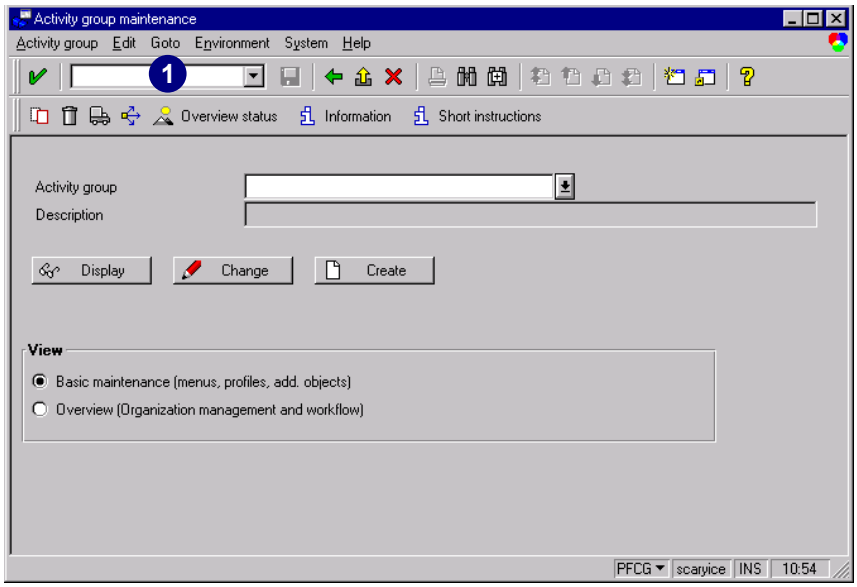
6. In the *Enter Change Request* dialog box, choose the correct *Request* number.
7. Choose *Continue*.

The activity group was inserted in the appropriate transport request.

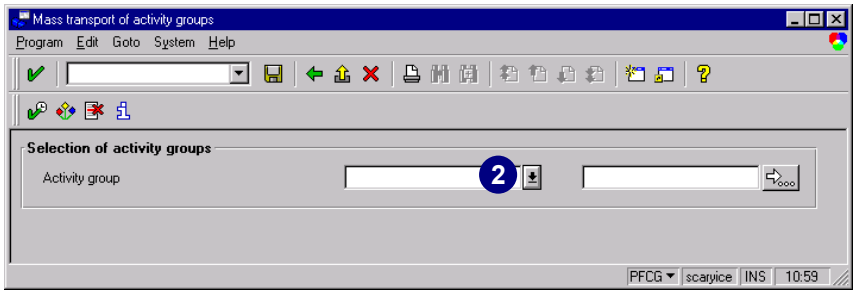
Mass Transport of Activity Groups

To transport a set of activity groups all at once, use the mass transport function inside the PG.

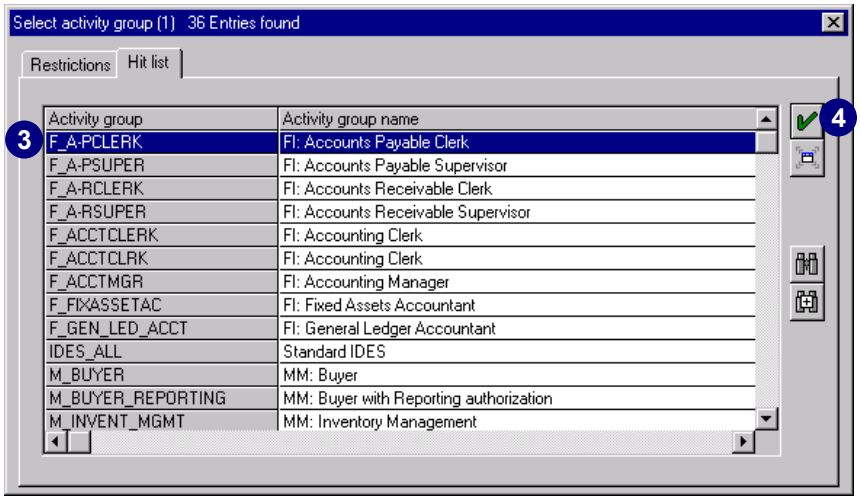
1. In the PG's *Activity group maintenance* screen, choose *Goto* → *Mass transport.*



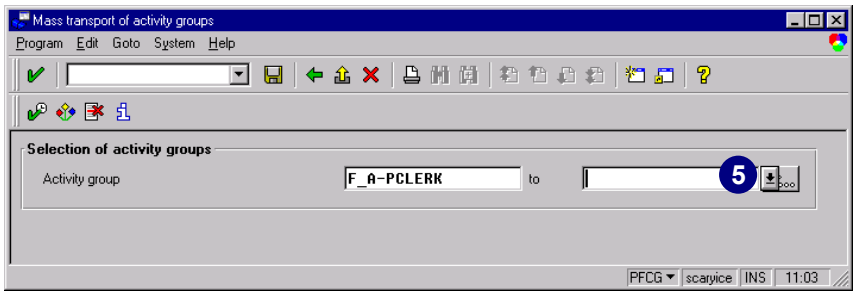
2. To select the activity groups you would like to transport, choose *possible-entries* to display all currently existing activity groups, or enter the name of the first activity group directly into the first field.



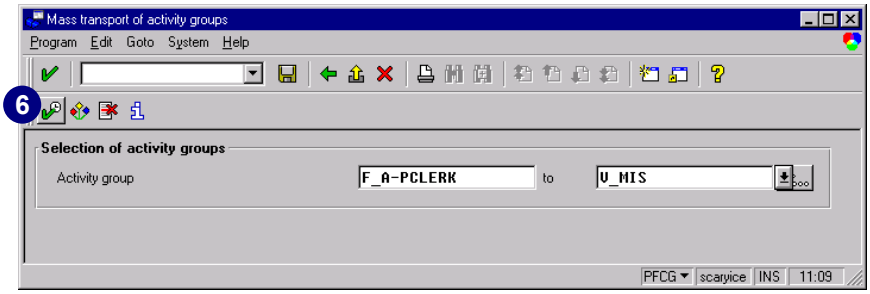
3. Select the first activity group to be transported.
4. Choose *Continue*.



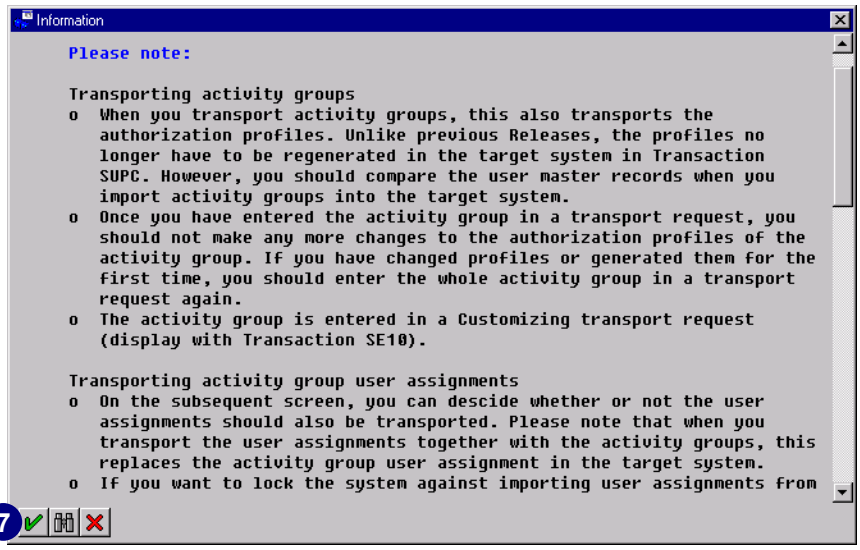
5. To select the last activity group of the set, use *possible entries* to select it from the list, or enter the name of the last activity group to be transported directly into the second field.



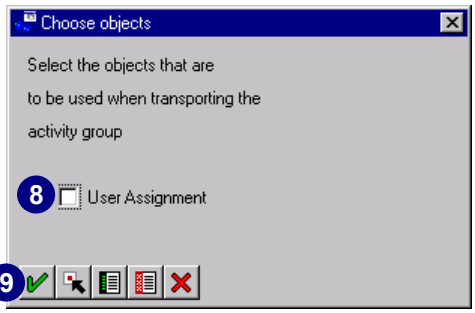
6. Choose *Execute* .



7. Choose *Continue*.



8. If you would like to transport the user assignment as well, select *User Assignment*. If you do not want to transport the user assignment with the activity group, make sure it is deselected.
9. Choose *Continue*.



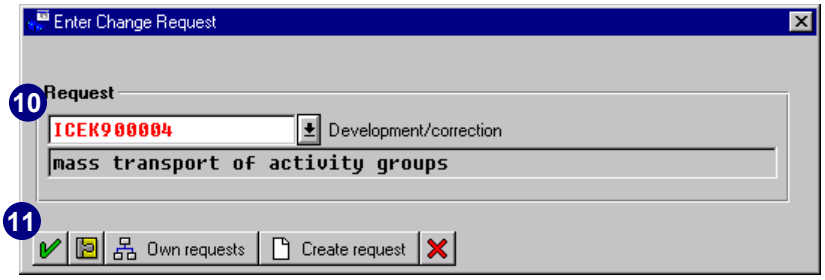
You can decide whether or not the user assignments should also be transported. Please note that when you transport the user assignments together with the activity groups, this action replaces the activity group user assignment in the target system.

If you are using the central user administration, you can only create user assignments in the central system. These can then be sent by request to the system group that you specified. If user assignments to activity groups were additionally transported, the central user administration display would be inconsistent. The users transported in this way would be removed at the next user distribution.

If you want to lock the system against importing user assignments from activity groups, you can specify this in the Customizing table *PRGN_CUST* (using transaction *SM30*). Enter a line with the identifier **`USER_REL_IMPORT`** and the value **`NO`**.

10. In the *Enter Change Request* dialog box, use *possible entries* to choose the correct *Request* number.
11. Choose *Continue*.

    You have just created a transport request that contains all the activity groups that will be transported to another client. Release the transport and import it into the other client.



User Master Record Comparison After Import into the Target System

Once the activity groups have been imported into the target system, you should compare the user master records of the activity groups concerned. You execute this comparison using report *PFCG_TIME_DEPENDENCY*, which you should schedule periodically. You can therefore wait until the next time that the report runs in your target system.

If you do not want to wait that long and want the activity groups in the target system to be immediately consistent, compare the activity groups by choosing *Goto* → *Mass comparison* in transaction *PFCG*. In the *Activity group* field, choose the activity groups concerned. Select *Complete compare* in the *Selection of action* field and start the report by choosing the *Execute* button. The activity groups in the target system are then made consistent.

Using the Organizational Management (HR-Org)
When you use Organizational Management, note that the links made in this step are not automatically transported. Use the transport function in Organizational Management to transport the changes that you made there. In Organizational Management you can enter changes automatically in a transport request, or use report *RHMOVE30*. If you use this report, enter the activity groups as the object type, *A007* as the evaluation path, and 2 as the display level. Fill the remaining parameters according to the data that is to be transported.

Automatic Recording of Personnel Planning and Development Data

Recording for activity groups is an active, standard setting after an R/3 installation. To deactivate automatic recording for activity groups, call transaction **OOCR** and set the value of entry **TRSP CORR** to **X.**

Transporting Check Indicators and Field Values

Transaction *SU25* (*Copy initial defaults*) copies the supplied SAP defaults concerning check indicators, field values, tables *USOBX*, and *USOBT*. This procedure imports both the SAP check indicator defaults for authorization objects in a transaction, and the authorization field values for the PG into the customer tables *USOBX_C* and *USOBT_C*.

Whether you run transaction *SU25* initially, or change the defaults later with transaction *SU24*, the process will be recorded in the correction and transport systems. By carrying out the corresponding transport request, you distribute your check indicators in the system.

The <*Transaction name*> corresponds to normal SAP transaction names, such as *VA01*. The check indicators and field values are included in the transport. Check indicators are saved in table *USOBX_C* and field values for the PG are saved in table *USOBT_C*.

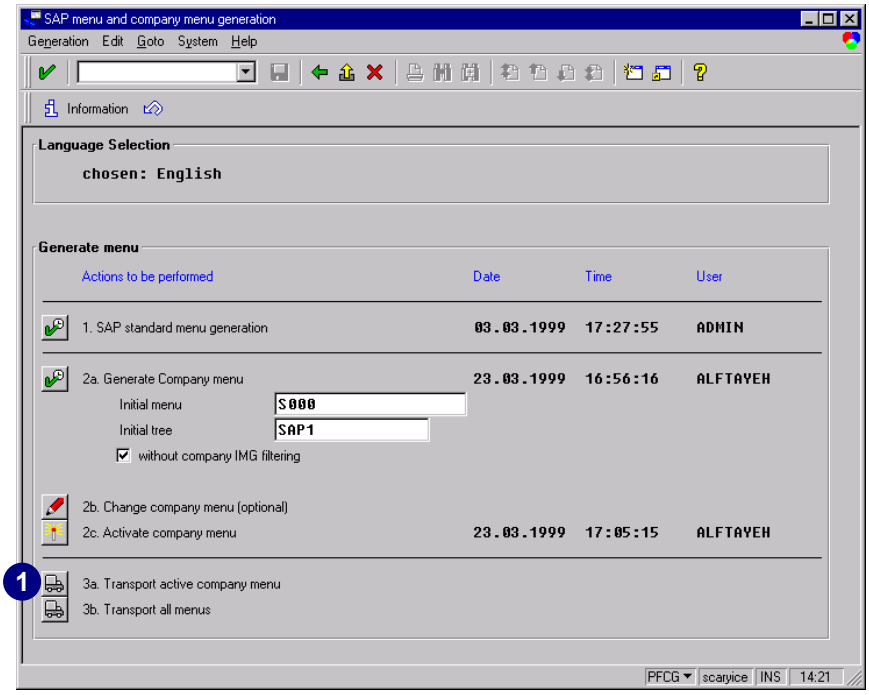
Transporting the Company Menu

Using IMG transaction *SSM1* you can generate, edit, and activate your company menu. (For more information on this issue, please see chapter 2.)

The first screen in transaction *SSM1* allows you to choose the type of transport for the company menu:

1. Choose *3a. Transport active company menu*.

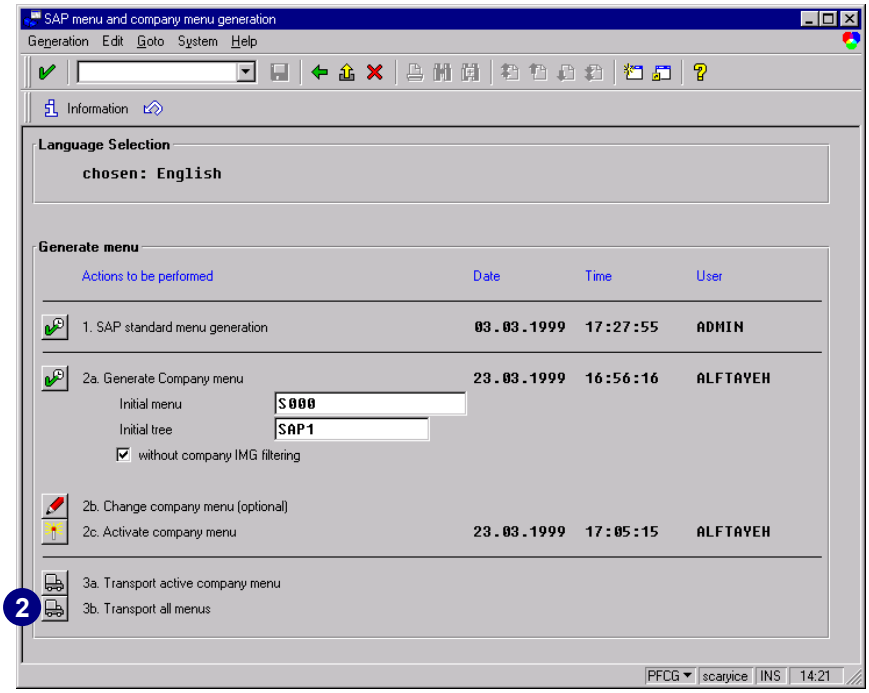
   In the target system, you cannot edit the active company menu, but you can edit and activate the inactive company menu.



2. Choose *3b. Transport all menus*.

   This transport involves the following objects:

   - SAP Menu
   - Inactive version of the company menu
   - Active version of the company menu
   - Details of generation and changes



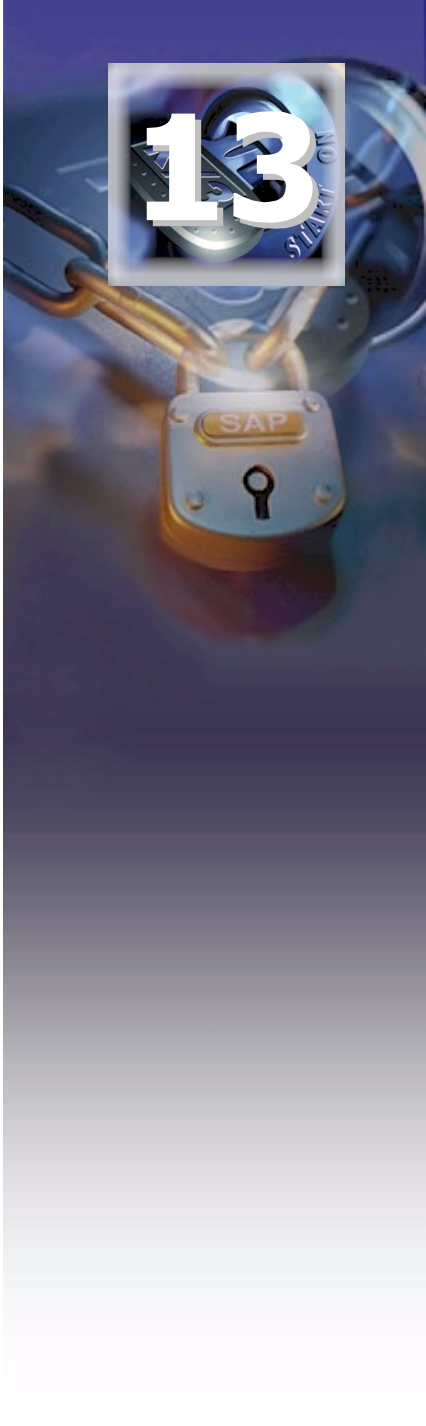
Transporting Authorization Templates

After an upgrade, all SAP-delivered templates will be identical in all systems. You cannot change these templates, you can only copy and alter them. You can, however, create your own templates. When you compare activity groups, unlike SAP defaults changes, template changes are not automatically passed on to the appropriate authorization profile(s) where the template was inserted. Once you have changed a template that was previously inserted in an authorization profile for an activity group, you must manually update that profile with the same changes that were made to the template. Changes to your own templates are recorded by the correction and transport systems. To carry out the transport request, objects in the request must contain the following syntax:

```
R3TR SUSP <Template Name>
```

Transporting User Master Records

To transport user master records between clients, run the client copy transaction **SCCL** and select profile *SAP_USER*. For transporting user master records between R/3 Systems, use transaction **SCC8** with profile *SAP_USER*.



Chapter 13: Tips and Troubleshooting Management

Contents

Overview

When users execute an R/3 transaction or report, they may see the system message, *You are not authorized to use Transaction XXXX.* This message means that either their current authorization profile does not contain the required authorization to execute the transaction, or the values maintained for the profile's authorization are insufficient. Authorizations can be located either by tracing authorizations with transaction *SU53* or with the system trace transaction *ST01.*

Tracing Authorizations with Transaction SU53

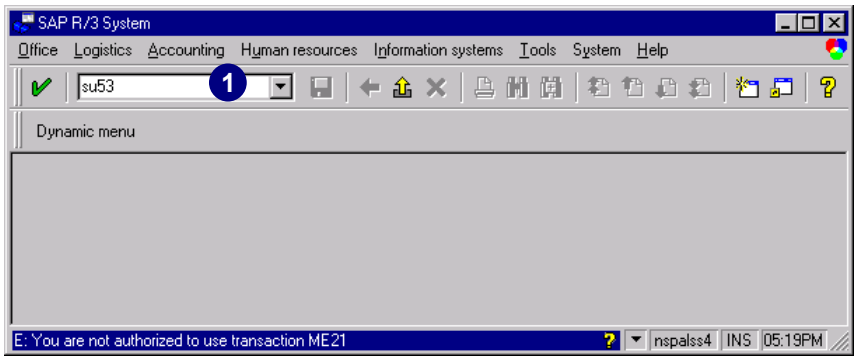
By entering **`SU53`** in the *Command* field, you can, at any time, analyze an authorization-denied error in your session. Transaction *SU53* can be accessed from any of your sessions, not just the one where the error occurred. You cannot, however, analyze an authorization error in another user's logon session from your own session.

At the transaction start, transaction *SU53* is protected by authorization object *S_TCODE.* You should give all users access rights to transaction *SU53*. Thus, in case of a problem, your help desk can easily analyze problems that use transaction *SU53.*

If you are using structural authorizations (see chapter 7), *SU53* is not very useful if the transaction where you are receiving messages "no authorization for…" is an HR transaction or a transaction that calls HR objects. This happens because *SU53* only reveals the last authorization check failure based on the ABAP code statement Authorization-Check. However, structural authorizations do not use the Authorization-Check statement in determining accesses. Therefore, if extensive structural authorizations are used, the system trace (transaction *ST01*) will be of more benefit than *SU53.*

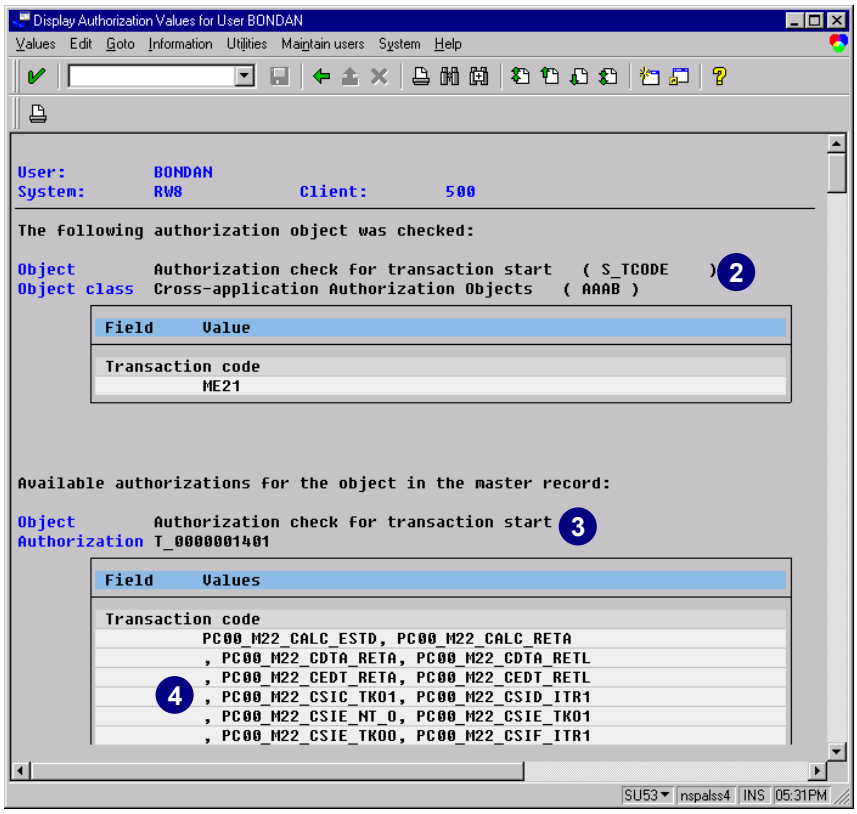
If the error message *E: You are not authorized to use transaction xxxx* (or something similar to it) appears in the status bar:

1. In the *Command* field, enter transaction **SU53** and choose *Enter* (or choose *System* → *Utilities* → *Displ. auth. check*.).



In the screen at the right, you can see:

2. The authorization object checked by the transaction with the required field values
3. The current authorization in your assigned authorization profile
4. The authorization field values for this authorization



To add the missing authorization to your current authorization profile by using the Profile Generator (PG) please see chapter 6. Also refer to Online Service System notes *23342, 67766,* and *18529*.

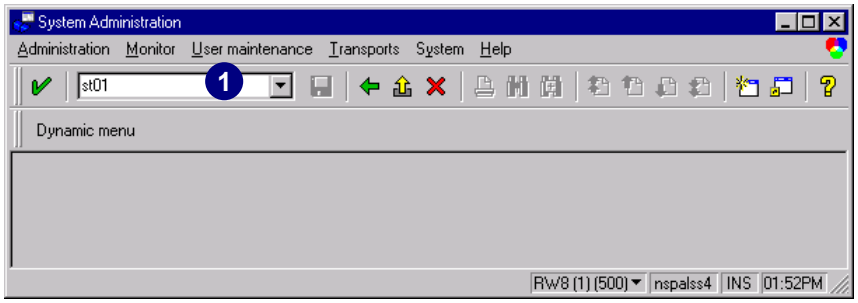
System Trace Using Transaction ST01

You can use the system trace to record authorization checks in your own session and other users' sessions. Start transaction **ST01** and run the transaction you are having authorization problems with. As soon as you get stuck, stop your trace. Everything you have done in the R/3 System, that requires authority checks is recorded in the trace with the object's fields and the tested values.

Using **ST01** impacts system performance; it slows your system down.

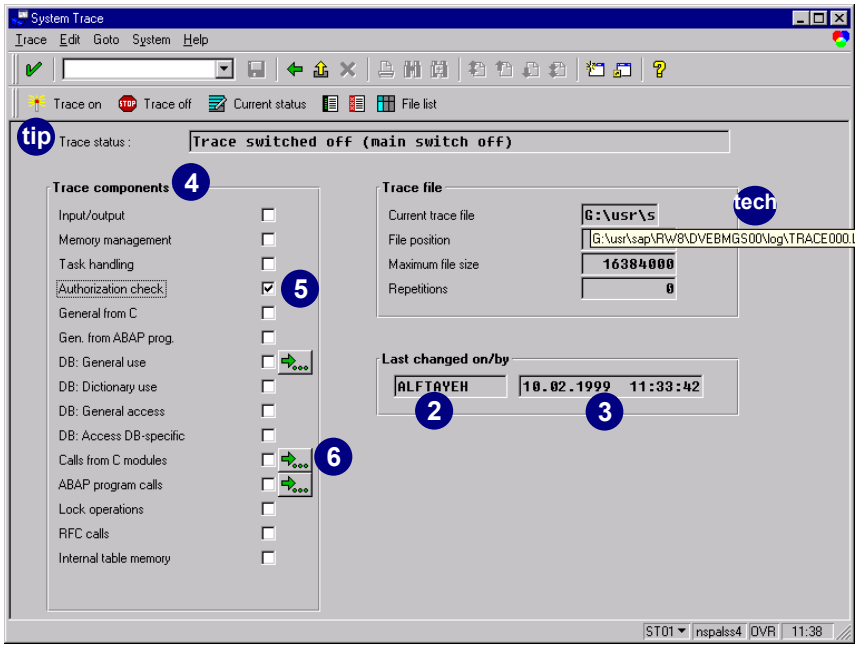
To start the trace:

1. In the *Command* field, enter transaction **ST01** and choose *Enter* (or choose *Tools* → *Administration, Monitor* → *Traces* → *System trace*).



2. You can see if another user has used the trace system.
3. You can also see when the trace was last activated.

Check *Trace status*. If the trace is active, do not interfere, because there is only one trace system for each R/3 instance.

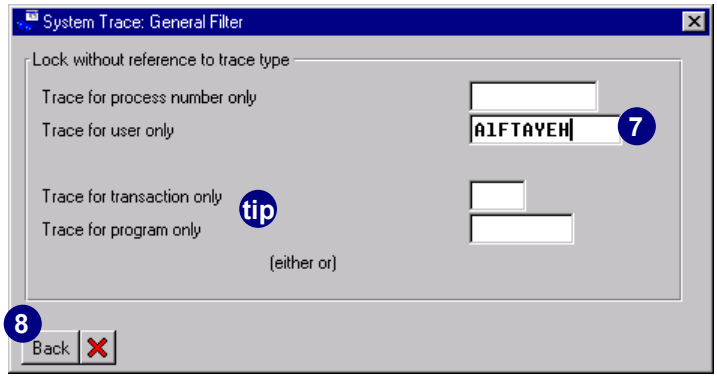


4. Many different *Trace components* exist and each is switched on with its own flag (and filter).
5. Some flags are directly visible in the checkboxes. Ensure that only *Authorization check* flag is selected.
6. Other flags are grouped and might contain only partial selections. Check all *Filter* icons to ensure that nothing is selected.

The trace file's name and storage location is shown in the field *Current trace file*. The trace is added to the existing file until the maximum file size is reached. Then a new file needs to be created (see later in this section).

To restrict the trace to your sessions, on the *System Trace* screen, choose *Edit* → *Filter* → *Shared*.

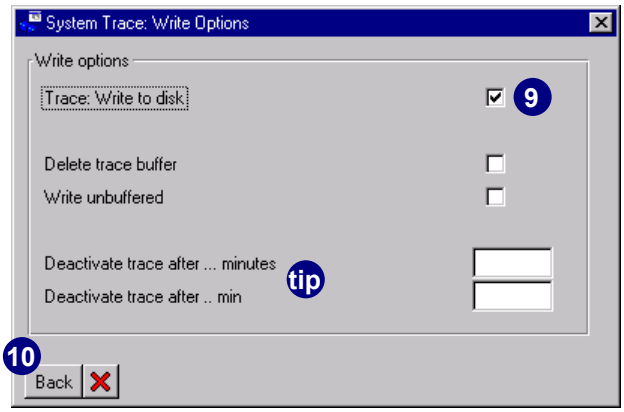
7. Enter your user ID in the proper field (for example, **`AlFTAYEH`**).
8. Choose *Back*.



You have also the option to filter the data for a certain transaction or a certain program only.

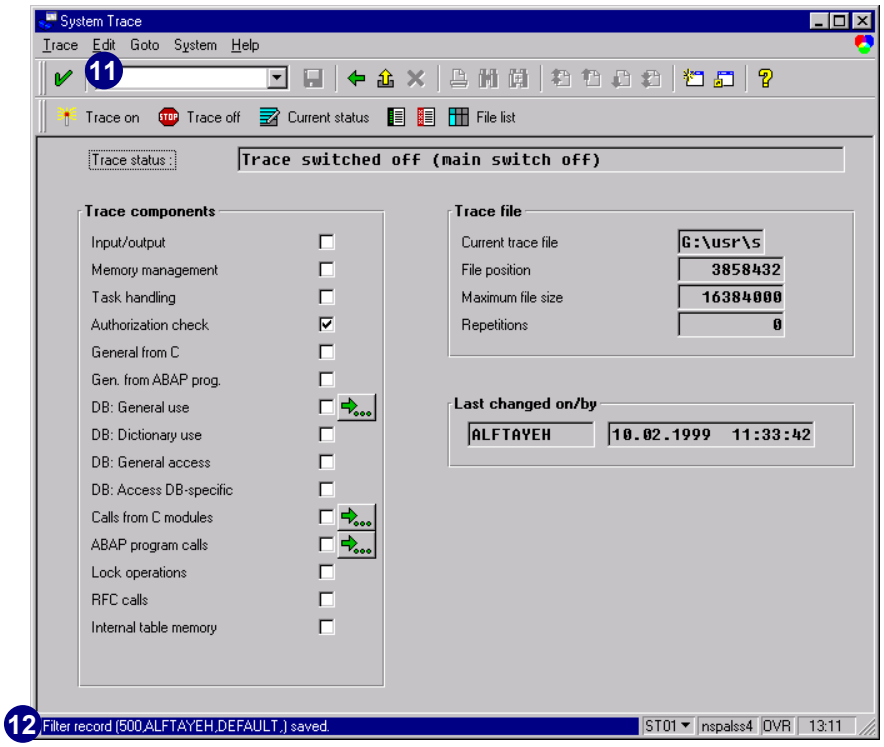
On the *System Trace* screen, choose *Edit* → *Write options*.

9. Set the *Write options* by selecting *Trace: Write to disk*.
10. Choose *Back*.



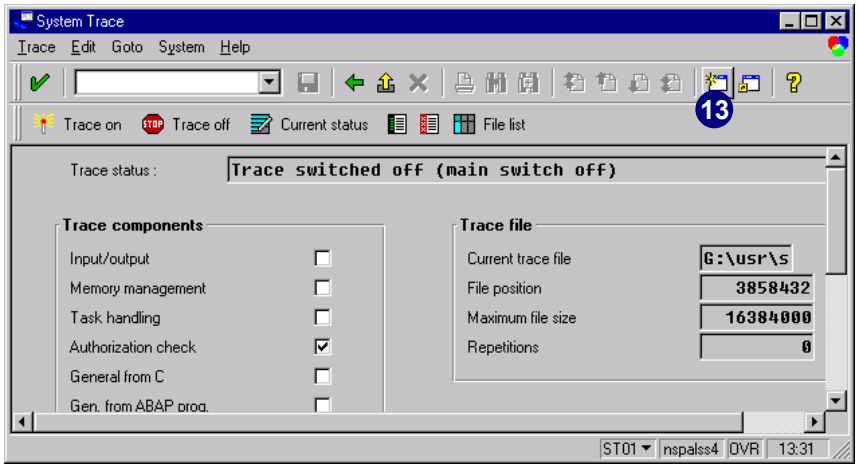
You have also the option to either define a time frame for the trace to run or use the buffer.

11. To save your settings for the next time you use the trace, choose *Edit* → *Settings* → *Write to database.*
12. Your data are saved with the following settings [*client, username, default*].

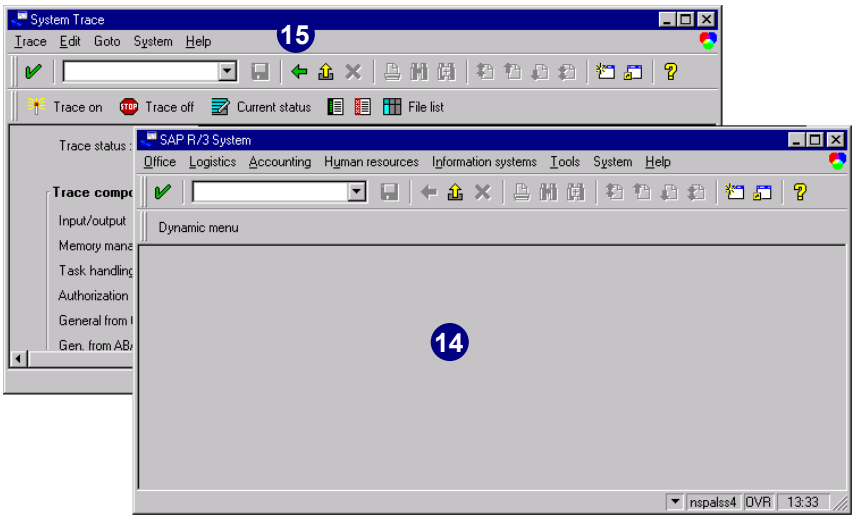


To use your individual settings the next time you start the trace, choose *Edit* → *Settings* → *Read from database.* All the checkmarks you set will appear in the corresponding checkboxes.

13. The system is now ready to begin the trace. At this time, we recommend that you open a new session or choose *System* → *Create session.*

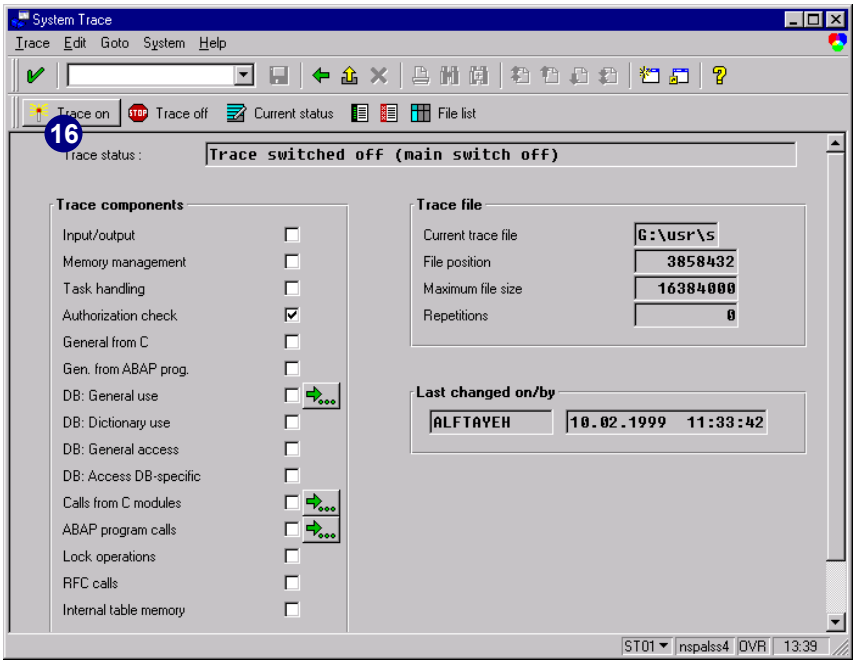


14. A new session (R/3 window) appears in which we will perform an example.
15. Return to the trace session.



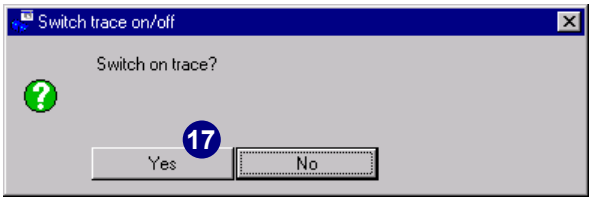
16. Switch the trace on.

    You can now trace authorization checks in any of your sessions. In our example, we use the second session to run transaction **SM31**.

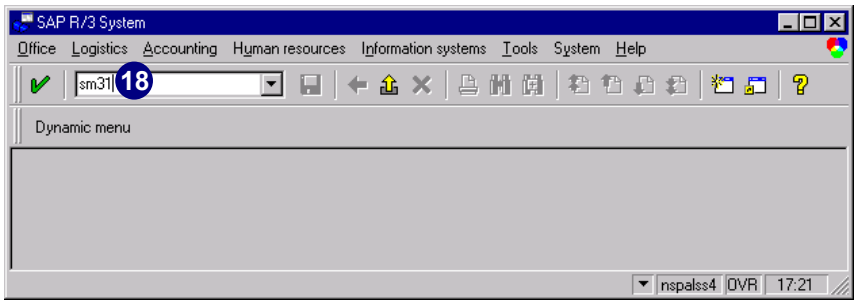


17. Choose *Yes*.

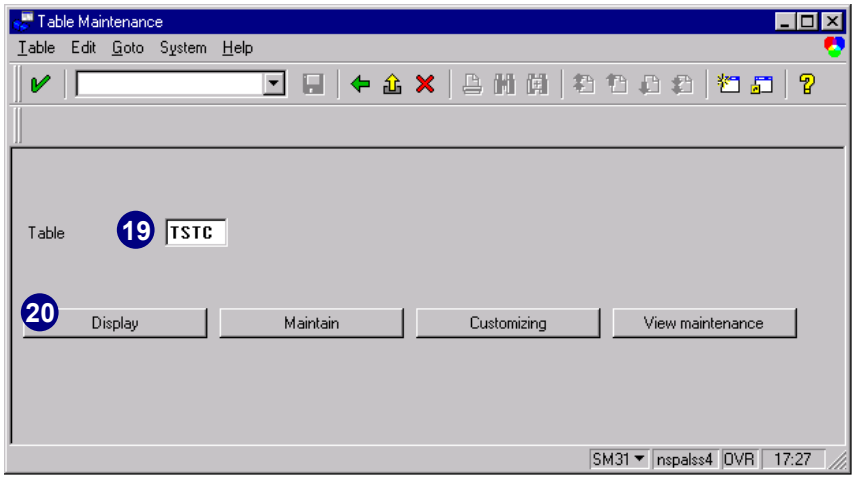
    Switch to the second session.



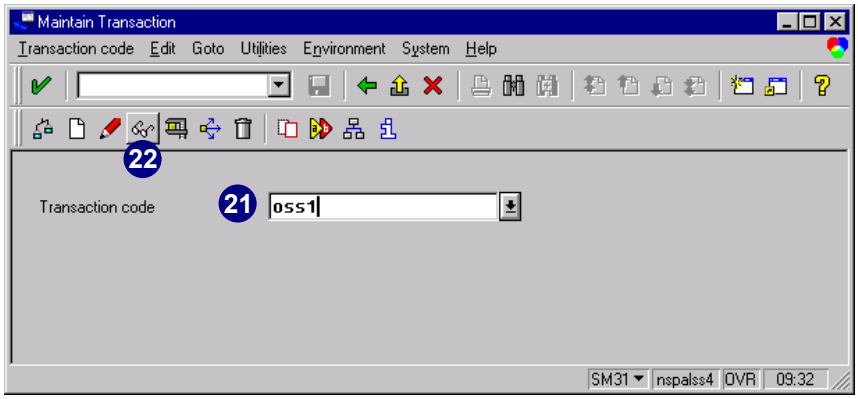
18. In the *Command* field, enter transaction **SM31** and choose *Enter*.



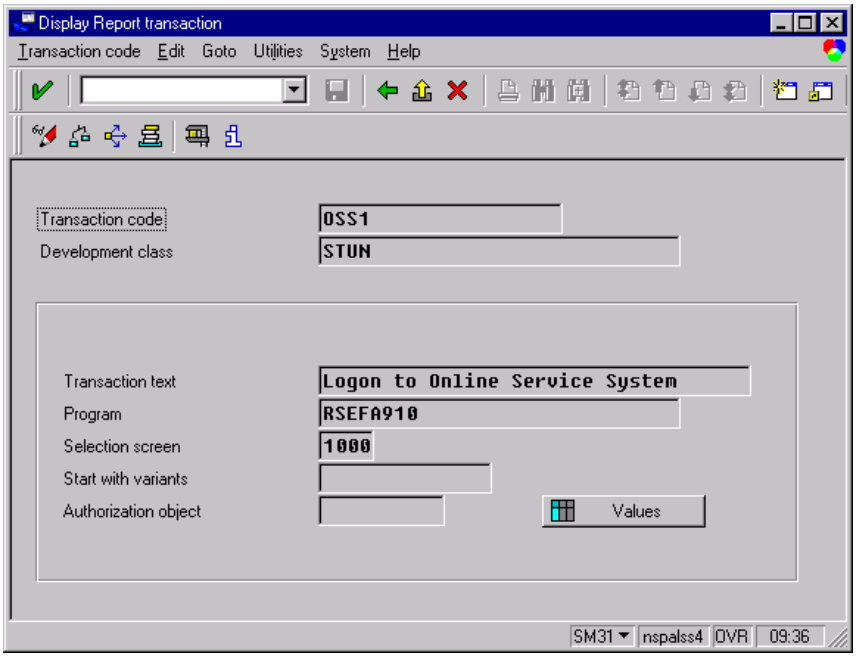
19. Enter **TSTC** in the *Table* field.
20. Choose *Display*.



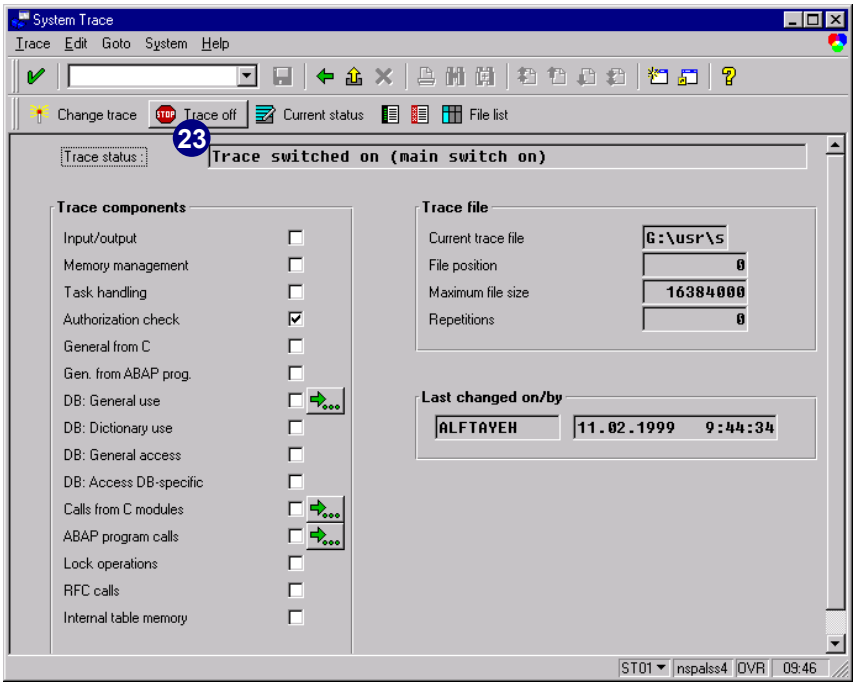
21. Enter a transaction code in the field *Transaction code,* we choose **OSS1** as an example.
22. Choose *Display*.



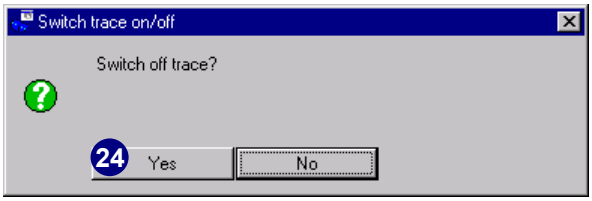
We have now completed our example. Return to the trace session.



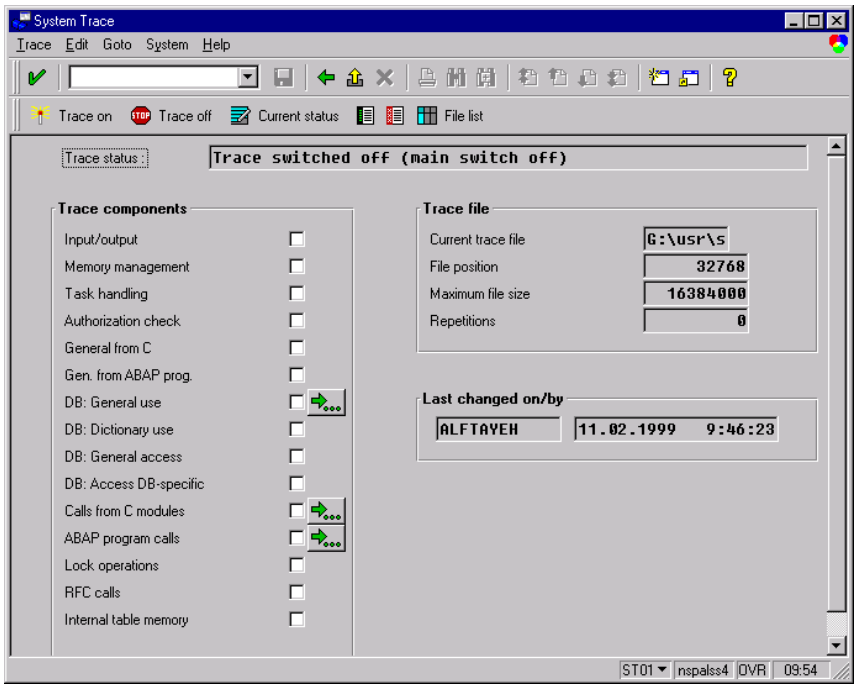
23. On the *System Trace* screen, choose *Trace off* to stop the trace.



24. Choose *Yes*.

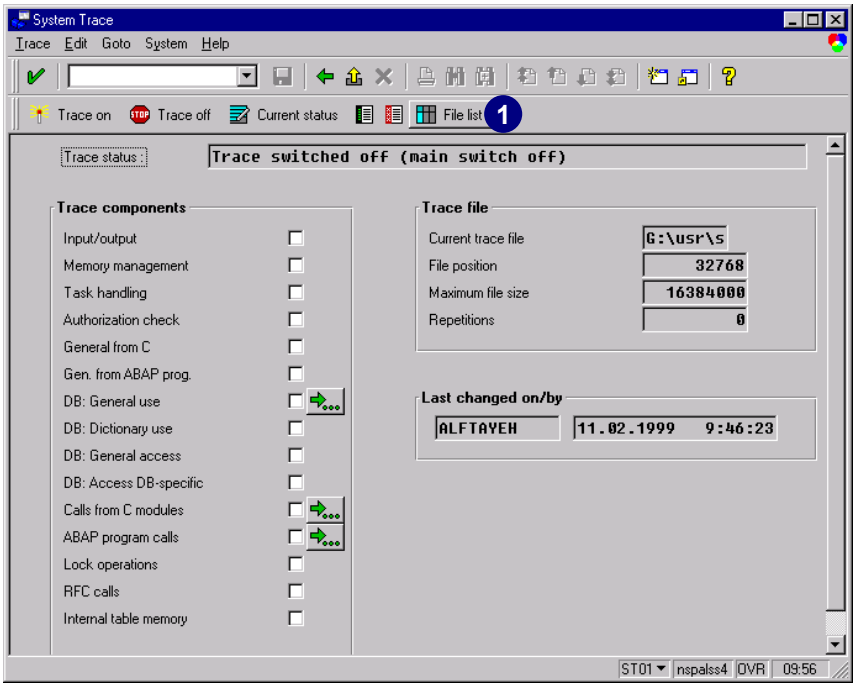


25. The trace has now stopped and is ready to analyze.

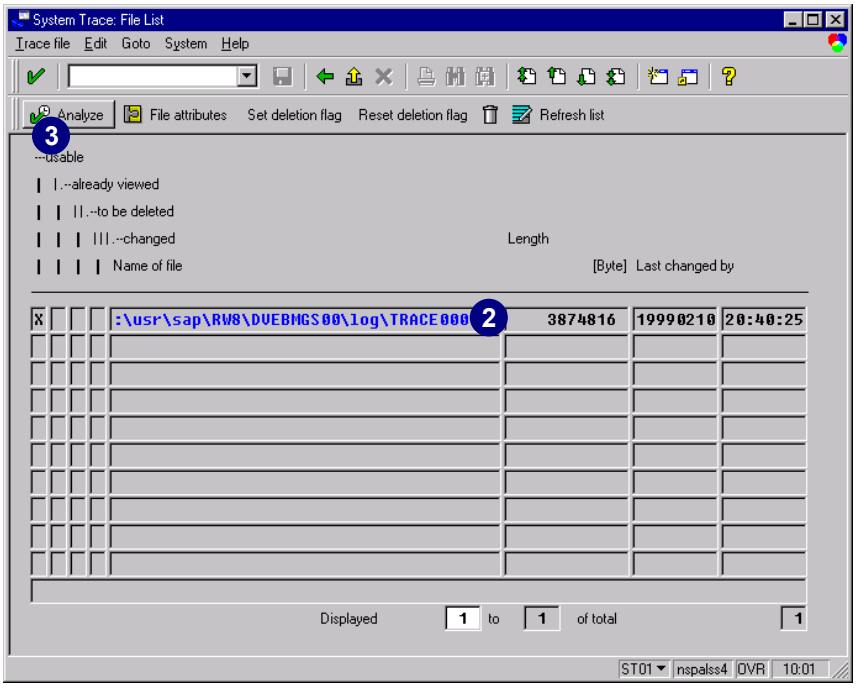


Evaluating a Written Trace File

1. To display the trace results, from the *System Trace* window, choose *File list* or *Goto* → *Files/Analysis*.



2. Select your trace.



The trace name has been given at the beginning (see *TechTalk* on page 13–4).

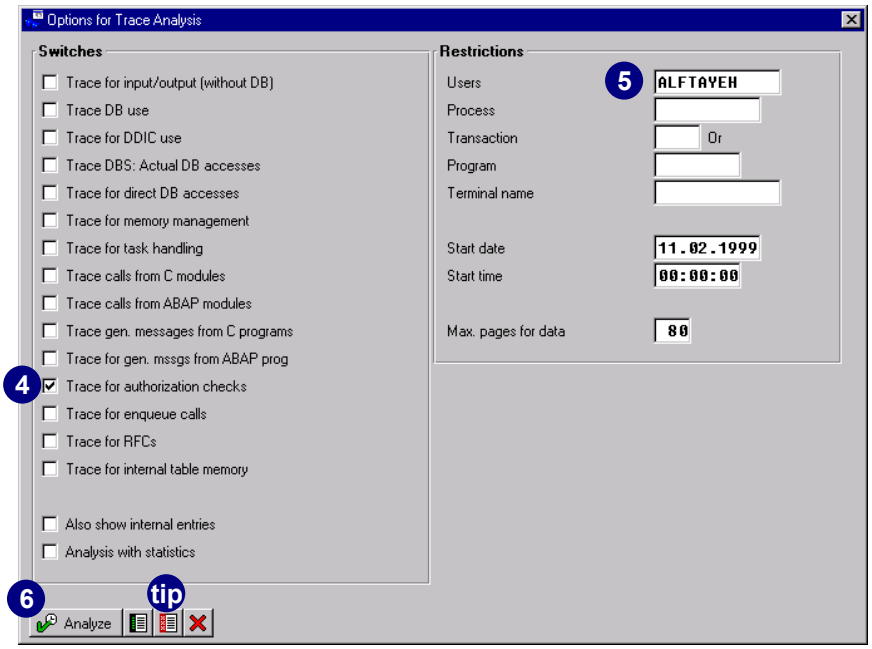
3. Choose *Analyze*.

You can now select all the options you would like to consider in your analysis.

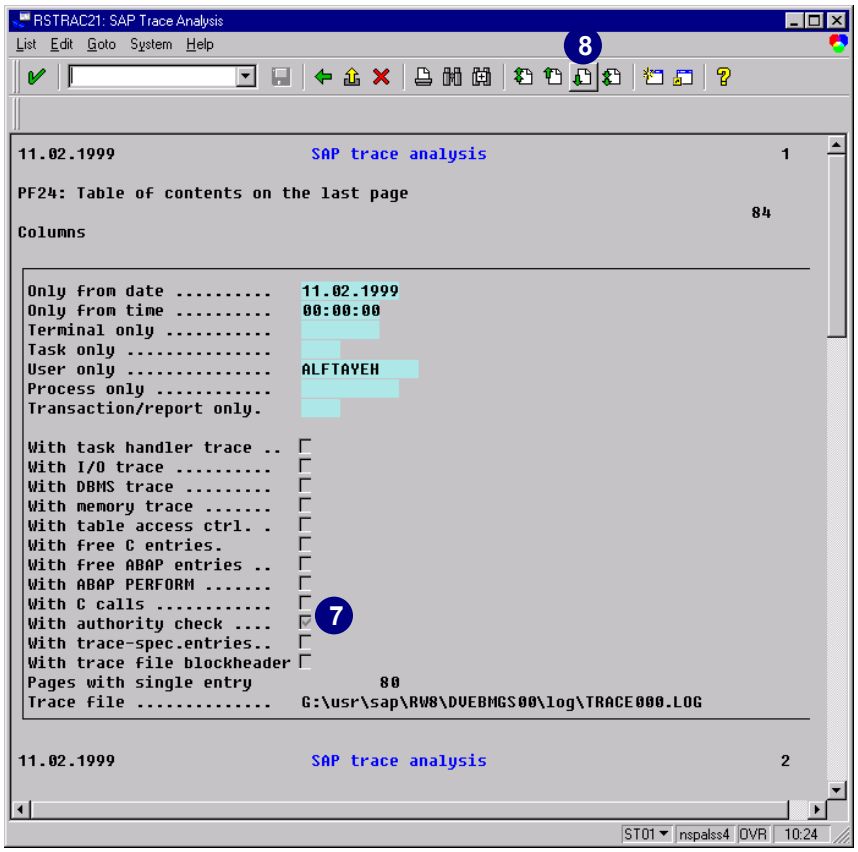
4. Select *Trace for authorization checks*.

If everything is selected, it might be easier to choose *Deselect all* first and then just reselect *Trace for authorization checks*.

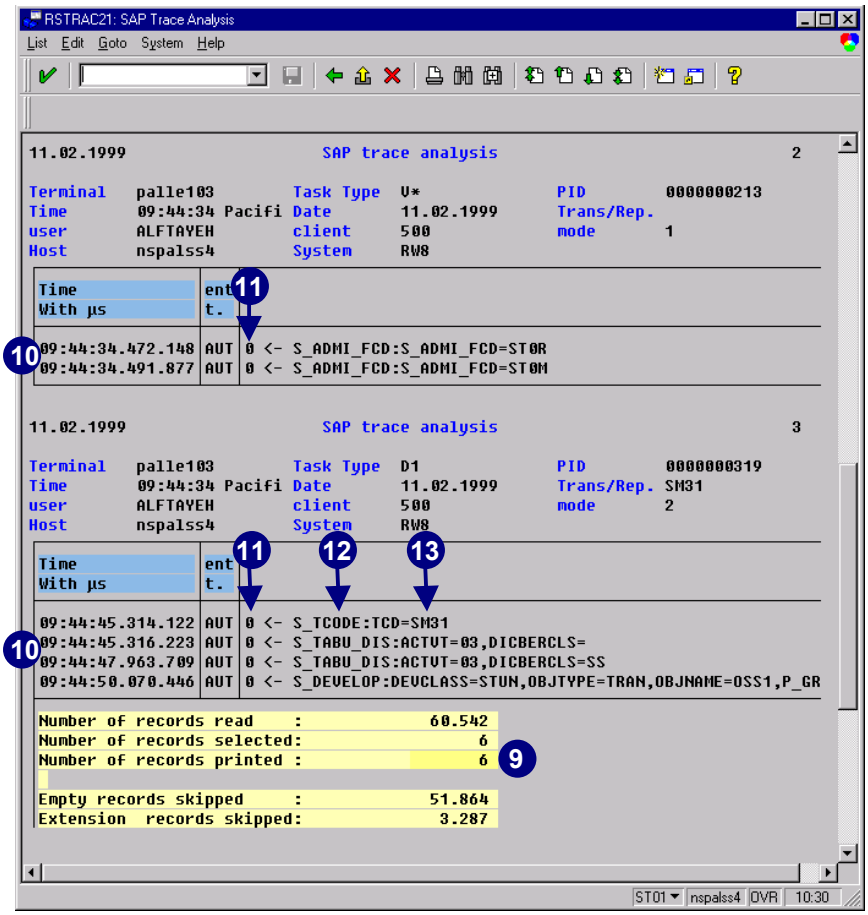
5. Enter the desired user.
6. Choose *Analyze*.



7. The first page of the trace file appears. By default, *With authority check* should be selected.
8. Choose *Next page*.



9. Since trace lists can be very large, the output is compressed. The *Number of records printed* is the number of lines currently displayed.
10. These lines appear in the box(es) above the *Number of records printed*. In our example, all the authorizations checked with the required field values have appeared. This is the information you are looking for!
11. The return code for each of these authorization checks also appears.
12. Object that has been checked
13. Transaction code that has been checked

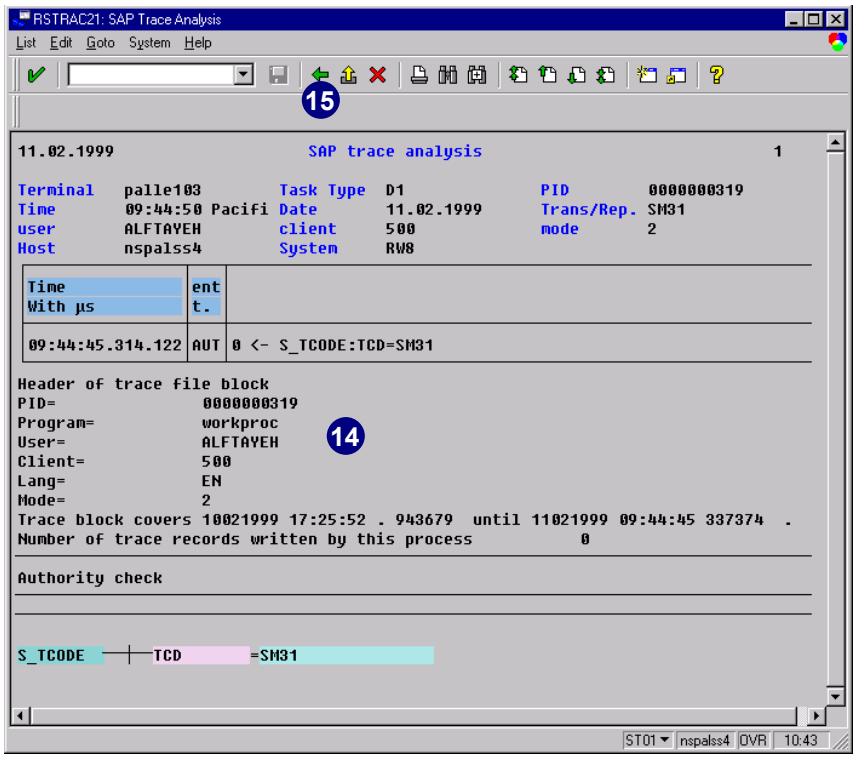


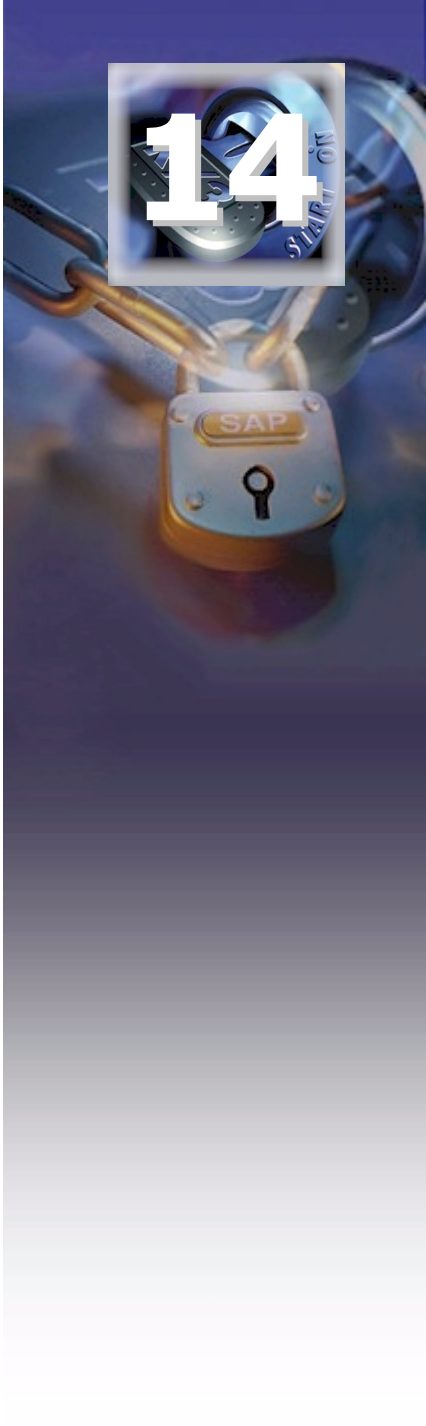
If the return code is:

- Equal to *0*, the authorization check is okay
- Greater than *0*, the authorization check is **not** okay

If you double-click on a record line, you can get more detailed information, for example we chose the *S_TCODE:TCD=SM31* line.

14. The detailed information for the particular authority check appears.
15. Choose *Back*.





Chapter 14: Upgrades

Contents

Overview

Before Doing Any Upgrade

Before doing any upgrade, you should:

1. Review the Online Service System regarding what notes already exist for the version you are upgrading to.
2. Review release notes related to authorizations for **all** versions between the version you are currently using and the version you will be implementing. For example, if you are upgrading from 3.1H to 4.5B you would want to read the release notes for versions 3.1I, 4.0A, 4.0B, 4.5A and 4.5B. To review the release notes, choose *Help* → *Release notes* on your system. Select the *Complete list Rel. 4.0* and then choose the specific release you would like to get the information on. In the tree structure that appears, use the search function and perform a search on the words "authorization," "checks," and "security." Also, you will want to read the section on the tree beneath *Basis* → *Computer Center Management System* → *Users and Authorizations*. Review the release notes because they will tell you what new functionality is now available, as well as changes to existing functionality that you may need to consider in the new upgraded environment.
3. Devise a backup and disaster recovery plan for authorizations. Be realistic. If you have done extensive modifications or changes to standard SAP R/3 logic, these changes may cause problems after the upgrade. You may want to create a temporary group of activity groups that can be used in the interim so operations can continue. Discuss your backup plan with the project management or system administrators. A good idea is to create these temporary activity groups immediately when you get access to the new system.
4. Make certain that the Basis team recognizes and appropriately allocates in the upgrade timeline plan that the authorization person is an **integral** part of the upgrade procedure and that the upgrade, from a technical perspective, is not complete until the authorizations portion is also complete.
5. If you have made **any** changes with *SU24*, then it is very advisable to download to a local file (and save outside of the R/3 System) the contents of the two tables *USOBT_C* and *USOBX_C* from the version you are upgrading from. These tables may be needed in the event that a disaster recovery needs to be performed.

In this chapter, we show you the steps required after an R/3 System upgrade. This information is extremely useful immediately after your upgrade. Make sure you read this chapter before continuing your work with the Profile Generator (PG) in a new release.

The specific steps involved after the upgrade depend on the source and target release you are coming from.

Upgrade from a Release Before 3.1x to 4.5

Read chapter 2 if:

- You are upgrading from a release before 3.1G
- In the release before 3.1G, you could not or did not use the PG
- You want to work with the PG now

You face two main questions:

- Do you convert the authorization profiles created with transactions *SU02* and *SU03* into profiles that can be maintained by the PG?
- Do you re-create the authorization profiles from scratch using the PG?

The following sections provide some hints to answering these questions.

Converting Existing Authorization Profiles for the Profile Generator

First, create and save a new activity group for each job role. Rather than selecting business transactions from the company menu tree, choose the *Authorizations* tab in the *Change Activity Groups* screen. Then follow the steps described in chapter 6, *Inserting Authorizations from a Profile*.

The advantage to this method is that you can work with existing, well-tested profiles. If object *S_TCODE* does not have an authorization, manually insert one. Maintain the permitted transaction for each activity group as authorization values for object *S_TCODE* in the profile you will generate for this activity group. You can, of course, maintain an asterisk (*), but this is a disadvantage, because users would receive more access than you want to give them. The other disadvantage is that since the user-specific menu is missing, you cannot re-create the information saved in an activity group. You may convert your old profiles and work with them until you need to re-create and delete them.

Re-create the Authorization Profiles from Scratch Using the Profile Generator

Follow the instructions in chapters 4, 5, and 6.

Upgrade from Release 3.0F to 4.5A or 4.5B

After your 4.5 upgrade, if you create activity groups and generate profiles in release 3.0F with the preliminary version of the PG, then:

1. Make sure that the instance profile parameter *auth/no_check_in_some_cases* is still active.

   Follow the instructions in chapter 2, the section *Running the RSPARAM Report and Checking the Instance Profile Parameter*. If the parameter is inactive, follow the instructions in chapter 2, the section *Setting the Required Instance Profile Parameter* to activate it.

   The PG is already active in Release 4.5 though.

   Apply the appropriate advance corrections for Release 4.5 or any available Hot Package by referring to chapter 2, the section *Applying Advance Corrections to your R/3 System*.

2. Because there were no customer tables *USOBX_C* and *USOBT_C* in the Release 3.0F version of the PG, copy the SAP defaults in these customer tables.

   To copy these defaults, run transaction *SU25* and perform the steps in chapter 2, the section *Work on SAP Check Indicator Defaults and Field Values*. In transaction *SU25,* perform the first step *Initially fill the customer tables*.

   Also read chapter 2, the section *Reducing the Scope of Authority Checks* to learn more about the new functionality. Then decide whether you need to perform additional steps on the check indicator settings for the transactions you are using.

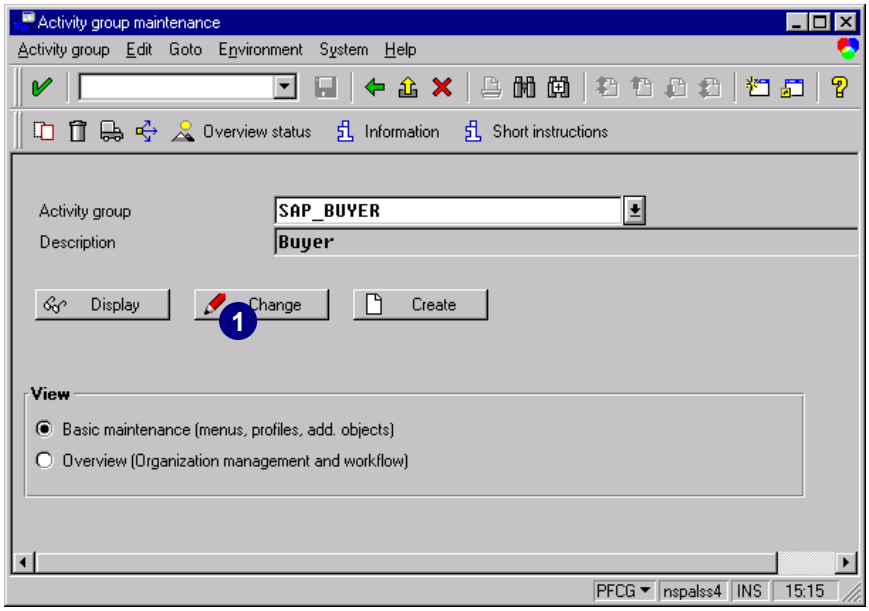
4. Due to new transactions in the menu tree, regenerate the SAP standard and company menu in the following fashion:
   - Reset the generation by choosing *Generation* → *Reset* in transaction *SSM1*.
   - The languages for which the menus are to be generated can be reselected after the generation is reset.
   - To regenerate the menus, see chapter 2, the section *Generating the SAP Standard Menu and Company Menu*.

5. After the upgrade to Release 4.5x, a profile matchup is required for all profiles generated in Release 3.0F. After the upgrade, the PG does not automatically inform you that a comparison is necessary for these profiles. (In transaction *PFCG*, the light on the *Authorizations* tab remains green for the profiles created in Release 3.0F, and transaction *SUPC* does not indicate whether a matchup is actually required.) Nevertheless, SAP has improved the SAP default data for check indicators and field values in the new release, so that a profile matchup is essential to ensure proper working profiles after the upgrade.

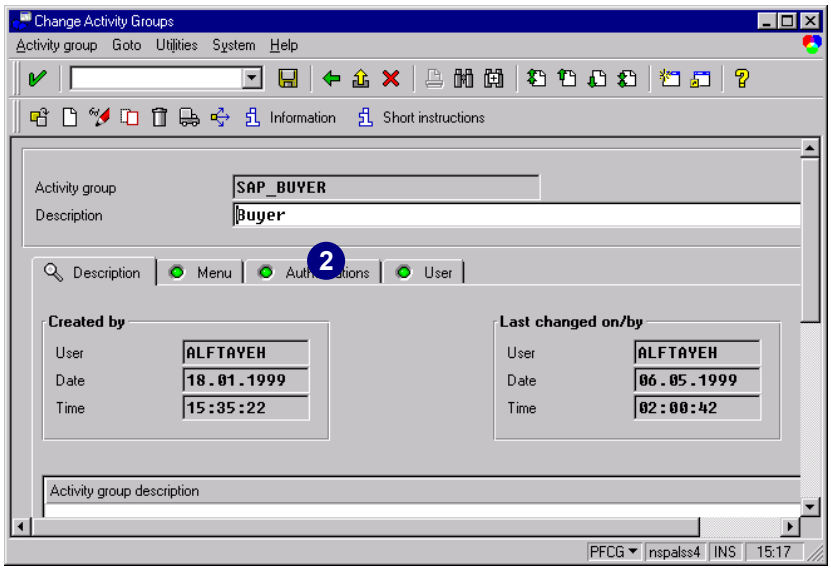
To perform a profile matchup:

Run transaction **PFCG** and select each activity group created in Release 3.0

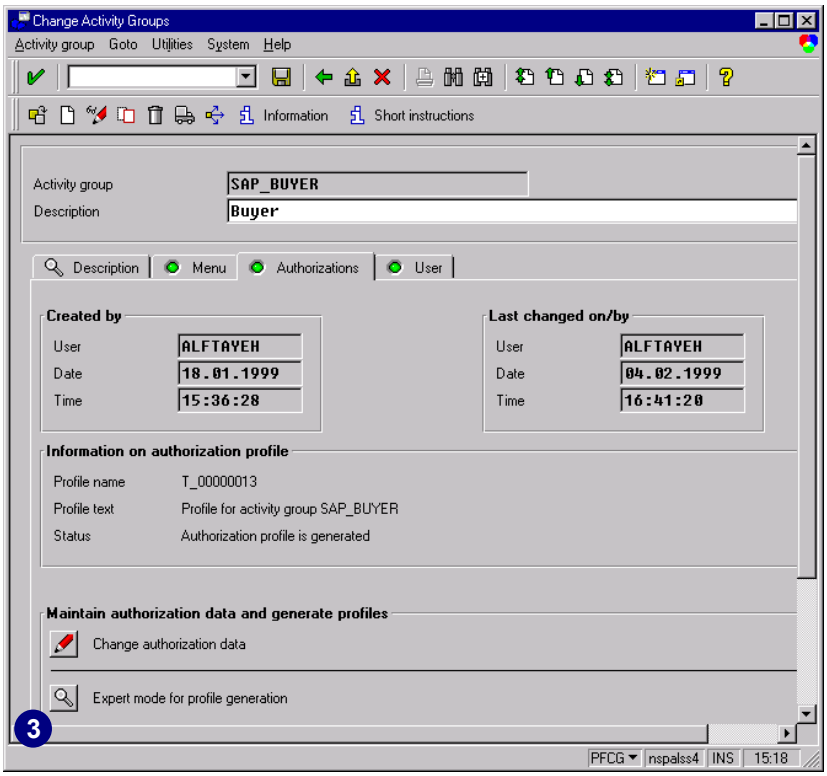
1. Choose *Change*.



2. Choose the *Authorizations* tab.

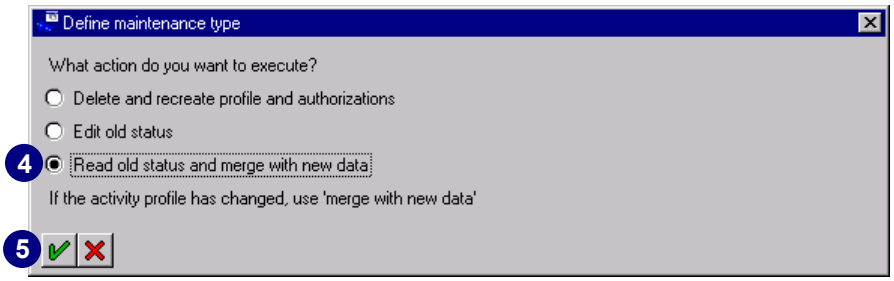


3. Choose *Expert mode for profile generation*.



4. Although the PG suggests that you choose *Edit old status* as the maintenance type, select *Read old status and merge with new data* as the correct maintenance type.

5. Choose continue and postmaintain any open authorization fields on the next screen, if required.



Due to changes in the SAP defaults for check indicators and field values in Release 4.5x, the PG may create some new authorizations. If you see new authorizations created where you have already maintained authorizations, deactivate or delete them.

The system includes the new required authorizations without checking for existing ones. This feature may sound unusual but offers improved system performance. To postmaintain all open authorization fields, follow the instructions in chapter 5, *Regenerating the Authorization Profiles after Making Changes*.

Menu options may appear under a new folder with the description *cannot be assigned* while you are maintaining the selection of business transactions for an activity group. If you see this description, please refer to Online Service System note *85565* for more detailed information.

6. After regenerating all the profiles, you have completed the upgrade steps for authorization profiles created in Release 3.0F.

No user master comparison is required for profiles already assigned to users, but remember that changes become active with the next system logon.

The procedure above has to be performed for each activity group seperatly. To speed that process up, use transaction *SUPC*, where you get a list with all activity groups. There you select the activity group that needs to be maintained by double-clicking on it.

Upgrade from Releases 3.1G, 3.1H, 3.1I to 4.5x

Once you upgrade to Release 4.5x, after creating activity groups and generating profiles in Releases 3.1G, 3.1H, 3.1I, 4.0A or 4.0B with the PG:

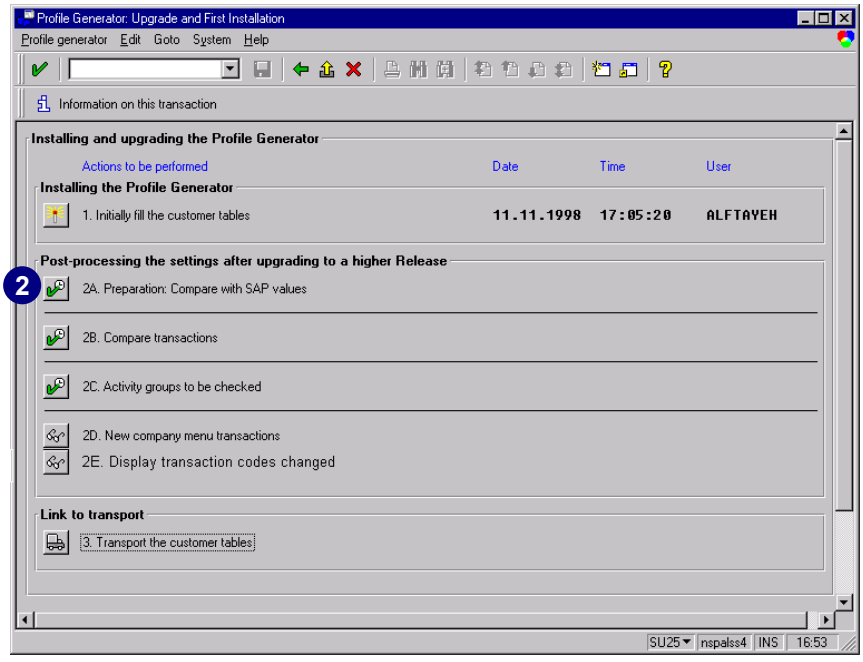
1. Make sure that the instance profile parameter *auth/no_check_in_some_cases* is still active.

   To do so, follow the instructions in chapter 2, the section *Running the RSPARAM Report and Checking the Instance Profile Parameter*. If the parameter is not active, follow the instructions in chapter 2, the section *Setting the Required Instance Profile Parameter* to activate it.

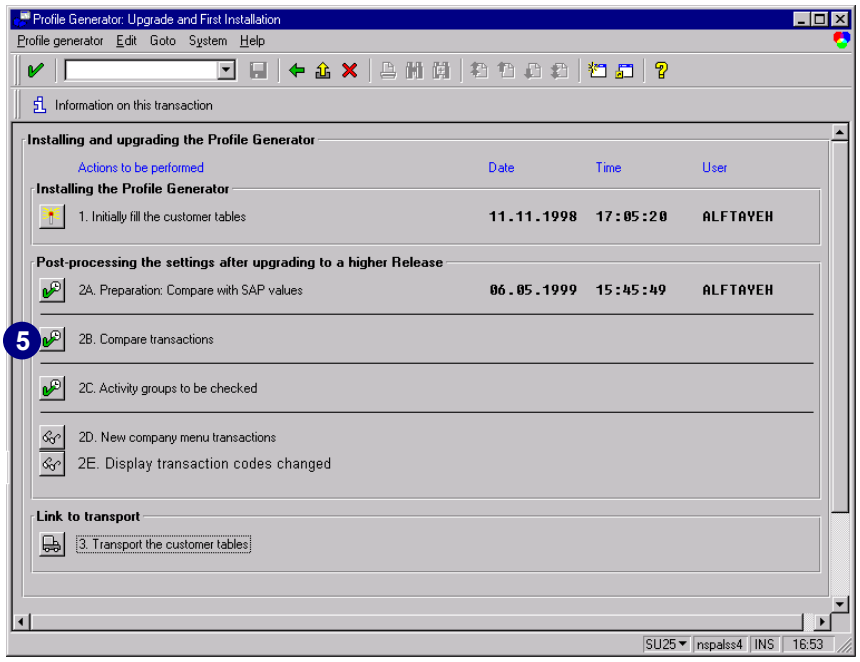
   The PG is set active in Release 4.5 though.

   Apply the appropriate advance corrections for Release 4.5 or any available Hot Package by referring to chapter 2, *Applying Advance Corrections to your R/3 System*.

2. Run transaction **`SU25`** and perform step *2A. Preparation: Compare with SAP values*. This step is used to prepare for steps *2B* and *2C*.



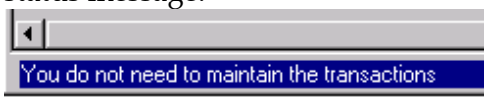
5. Choose *2B. Compare transactions*.

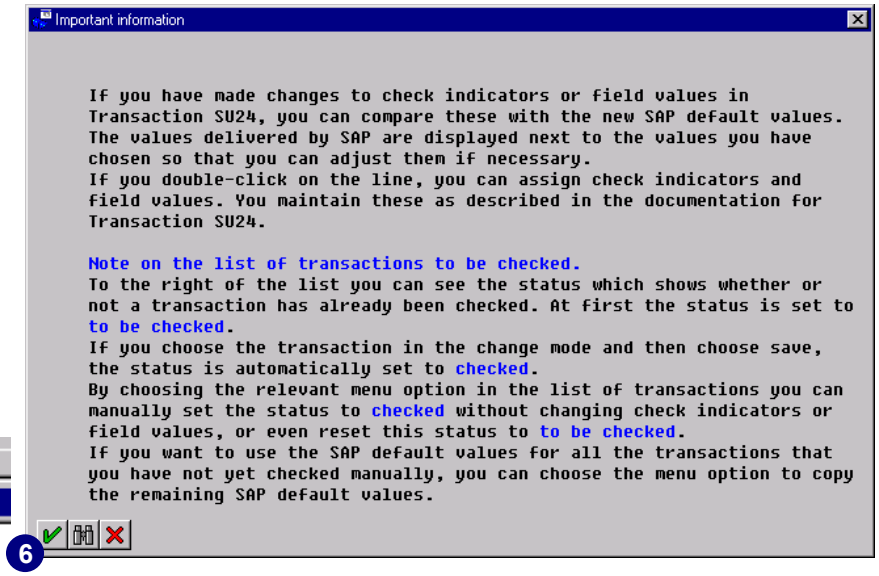


6. Choose *Enter*.

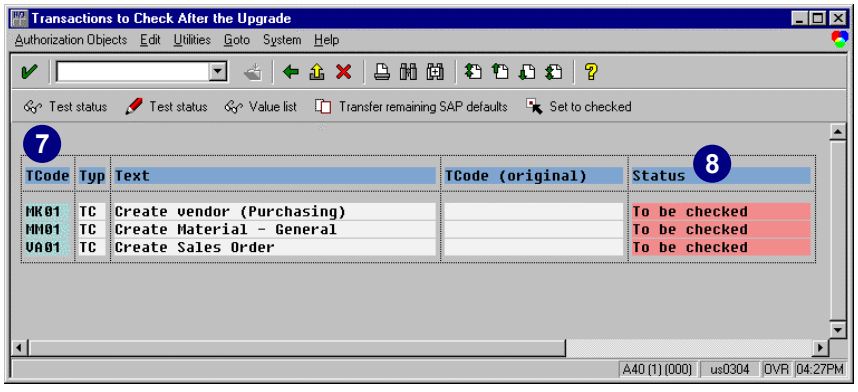
   The upgrade report you started in step *2A.* updates customer tables *USOBX_C* and *USOBT_C,* but does not overwrite the entries you changed in releases before 4.5x.

   If you have not changed check indicators and field values with transaction *SU24* in releases before 4.5x, you will see the following status message:



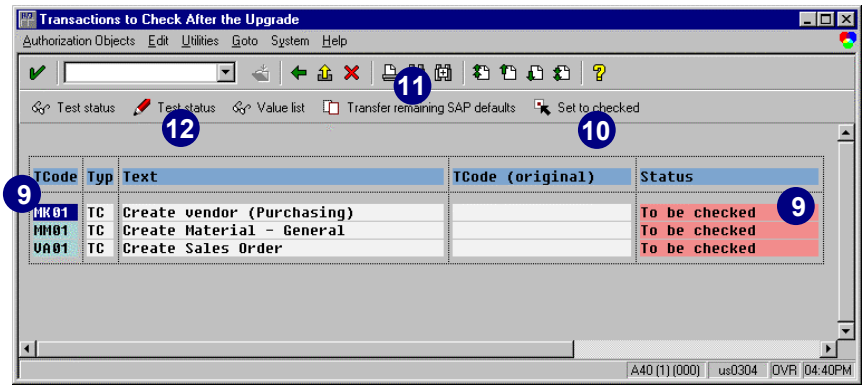


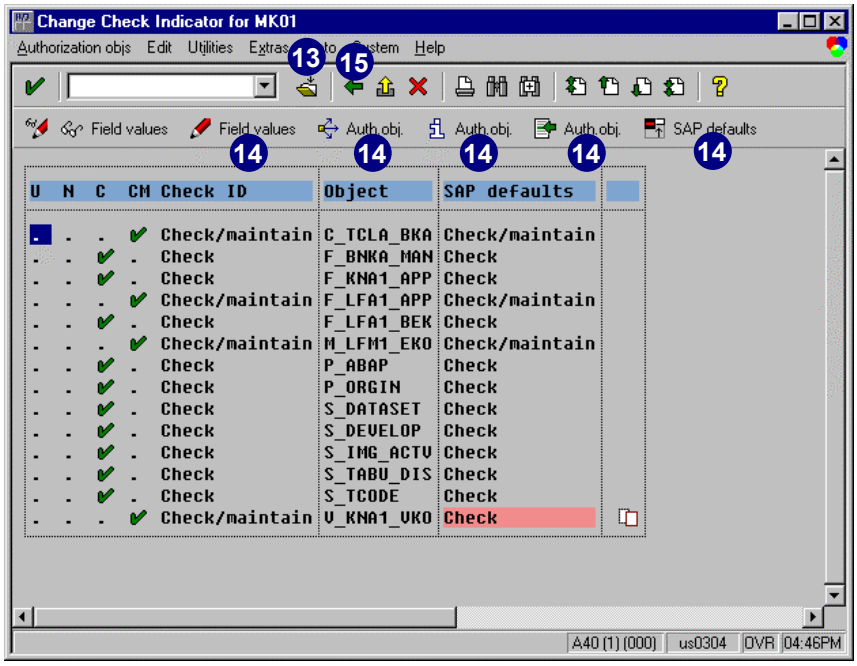
7. If you made changes, these changes will still be active after the upgrade. The output will be a list of affected transactions.
8. In the output list of transactions, you can see the *Status,* which shows whether a transaction has already been checked.

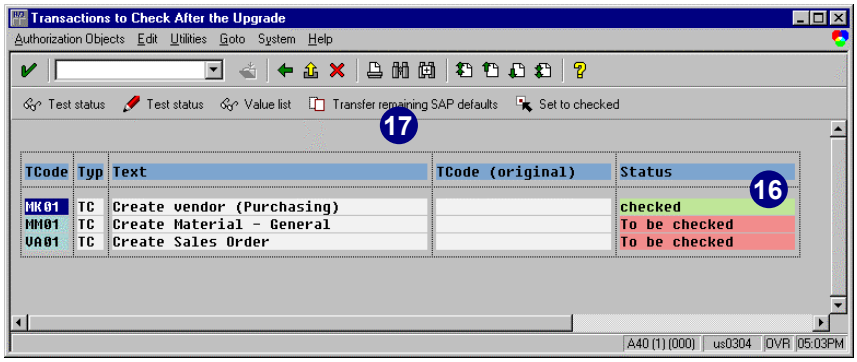


9. Select a transaction where the current status is *To be checked*.
10. Choose *Set to checked* to set the status to *checked* without changing any check indicator settings for this transaction.
11. Choose the *Transfer remaining SAP defaults* button to change the current active check ID setting to the SAP default value and the status to *checked*.
12. Choose *Change Test status* (*Test status* is wrong, the button should be labeled *Check ID*).
13. Choose *Save*.
    If you save without making any changes, the status is automatically set to *checked*, and the changes remain.
14. Choose any other menu option to make additional changes to this transaction and its settings for check indicators and field values.

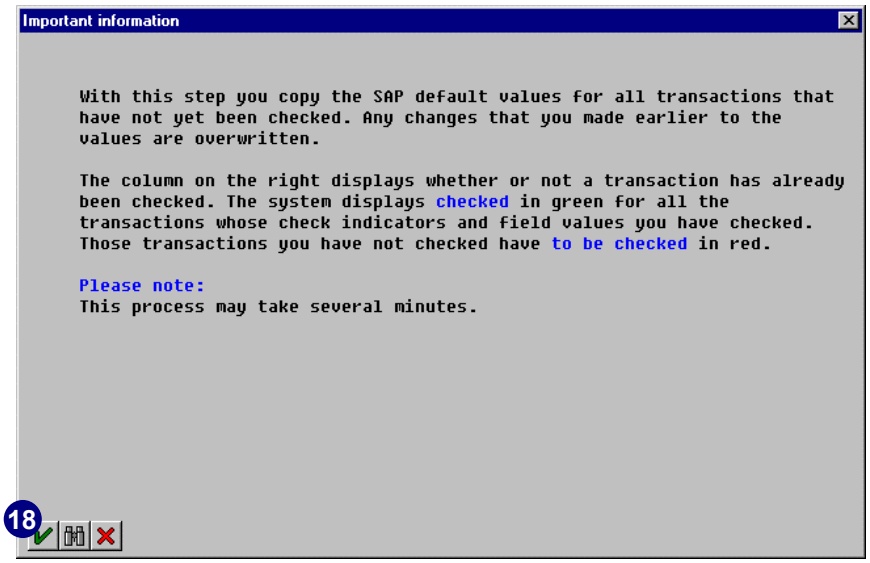
    Please read chapter 2, the sections *Change SAP Check Indicator Defaults and Field Values* and *Reducing the Scope of Authority Checks* to learn more about the functionality available.
15. Once finished, choose *Back*.
16. The status has changed to *checked*.
17. To use the SAP default values for all the transactions that you have not yet manually checked, choose the *Transfer remaining SAP defaults* button to copy the remaining SAP default values.



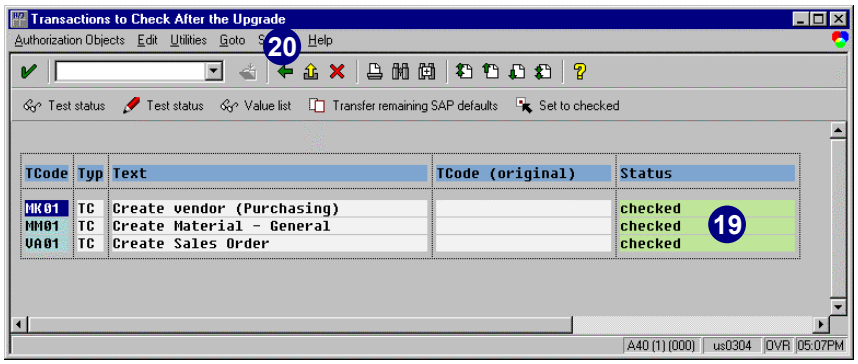




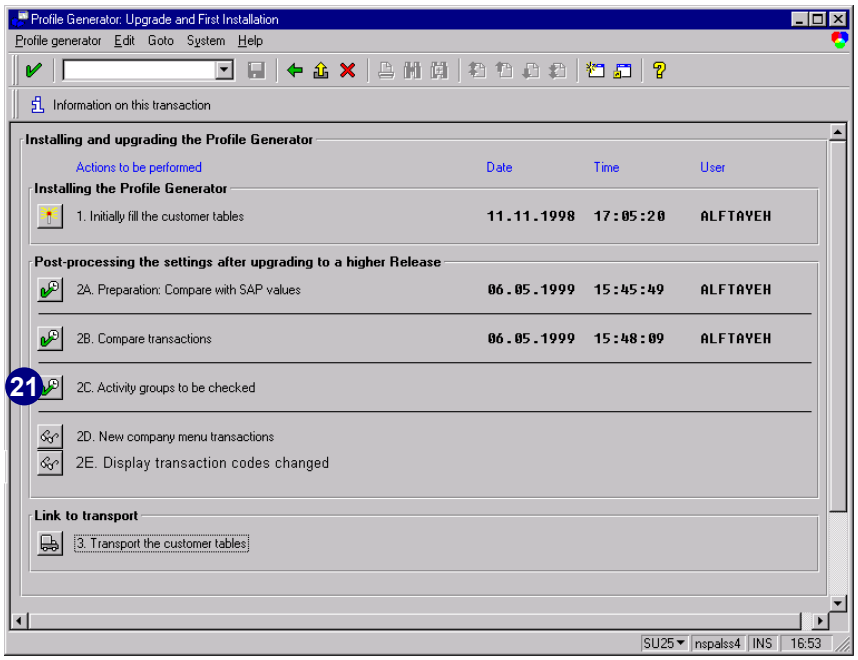
18. Choose *Continue*.



19. For all remaining transactions, the status has been set to *checked*.
20. Choose *Back*.

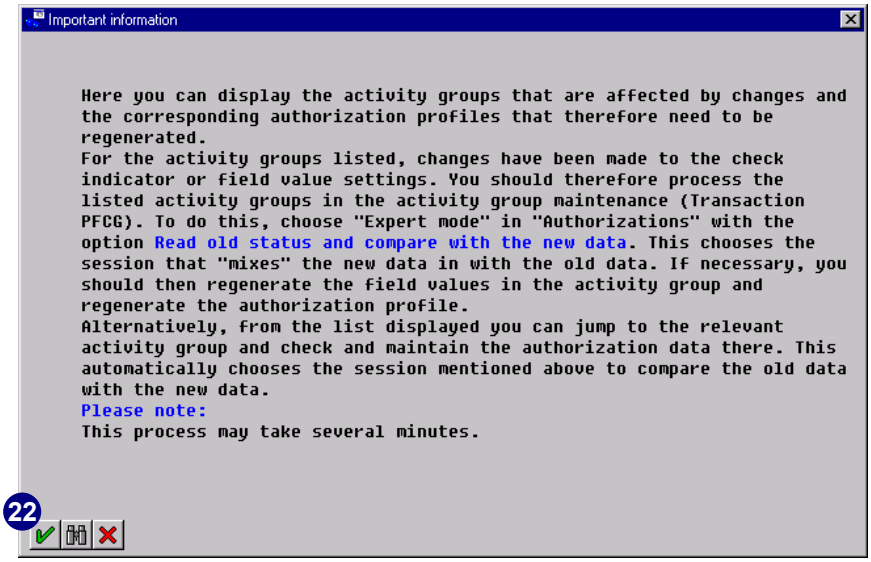


21. Choose *2C. Activity groups to be checked*.



22. Choose *Continue*.

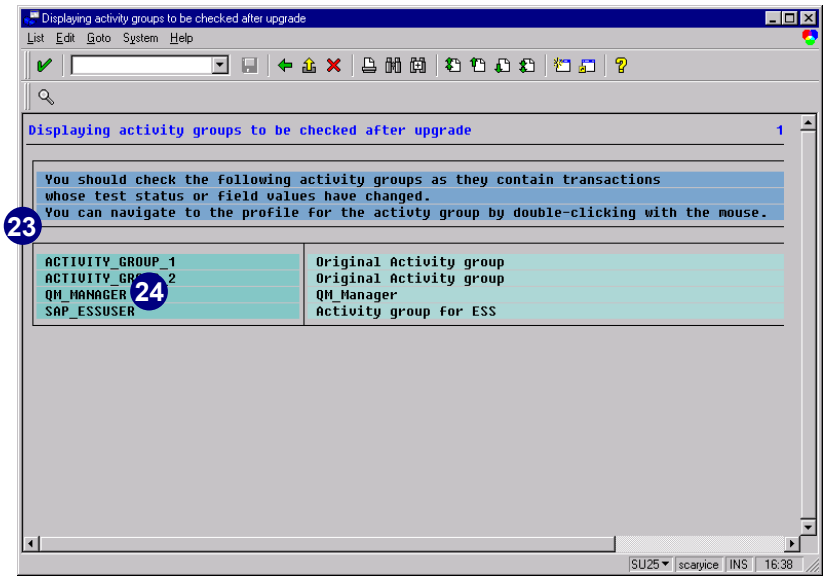
    The output is a list of activity groups that are affected by either changes you made or by changes from our improved default data.



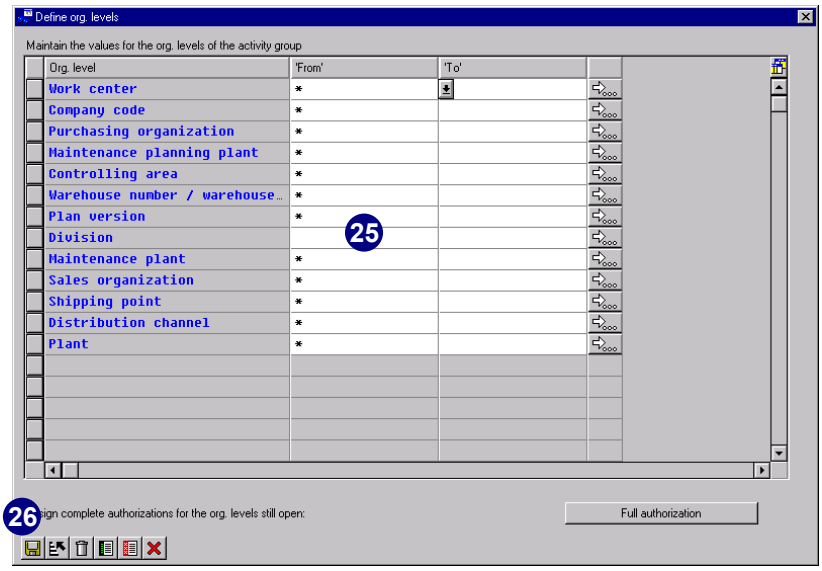
23. For the listed activity groups, changes have been made to check indicators or default transaction values. Therefore, the corresponding authorization profiles need to be adjusted.

    Make sure you select each entry in this list.

24. Double-click on the activity group you would like to adjust.



25. Maintain the correct organizational level
26. Choose *Transfer*.

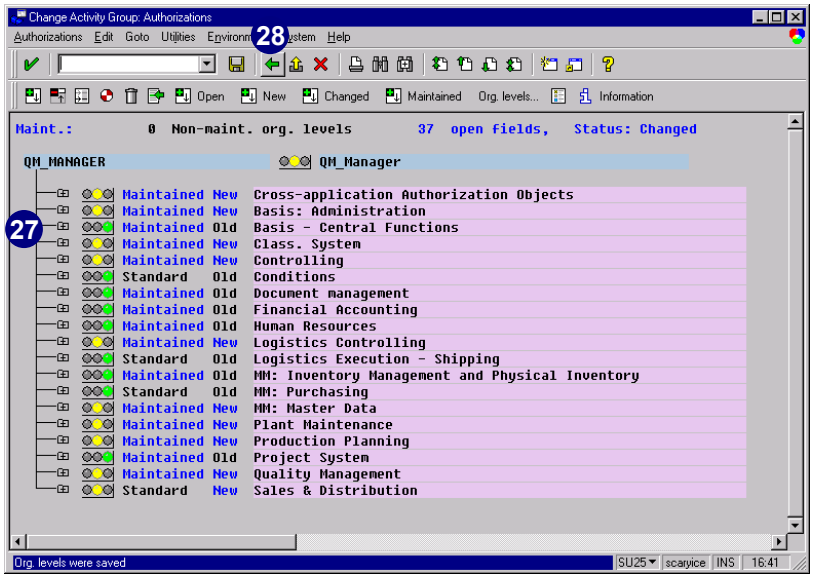


27. Postmaintain any open authorization fields, if required (yellow or red lights).

    Due to changes in the SAP defaults for check indicators and field values in Release 4.5x, the PG may create some new authorizations. You will see new authorizations created where you have already maintained authorizations. Just activate, or delete, the new authorizations. The system does include the new required authorizations without checking for existing ones for the same authorization object. This feature may sound unusual, but has more advantages than disadvantages and also improves PG performance.

    To postmaintain all open authorization fields, follow the instructions in chapter 5, the section *Regenerating the Authorization Profiles after Making Changes*.

28. After regenerating, choose *Back*. Continue with the next entry in the list of activity groups in the same procedure until you have adjusted all activity groups.



After completing steps *2A, 2B* and *2C*, you have performed the most important steps after your Release 4.5x upgrade.

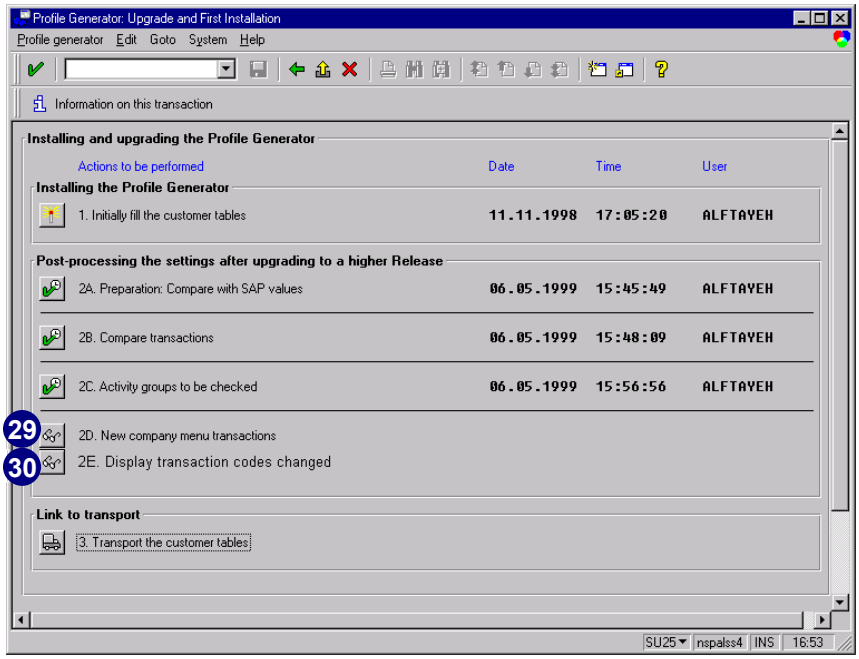
You still need to perform step *3. Transport the customer tables*, and transport the changes to your other R/3 systems. All systems must have the same settings for check indicators and field values.

29. Choose *2D. New company menu transactions*.

    This report lists all the transactions that have come into your company menu since the last release. This list should give you information about the new transactions.

30. Choose *2E. Display transaction codes changed*.

    This report lists all activity groups where transactions have been replaced by other transactions. The old and new transactions are also displayed. You can change the transaction code in the corresponding activity group by double-clicking on the entry in the list.

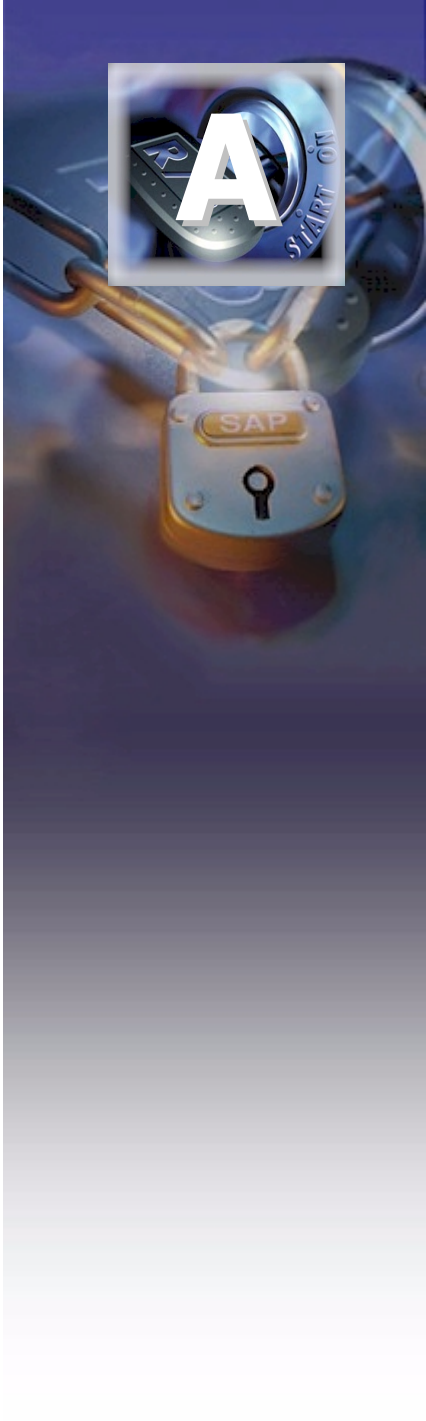


31. Due to new transactions in the menu tree, you must regenerate the SAP standard and company menus. To generate these menus:
    - Reset the generation.
    - Choose *Generation* → *Reset* in transaction *SSM1*.

      The languages for which the menus are to be generated can be reselected after you reset. Refer to chapter 2, the section *Generating the SAP Standard Menu and Company Menu* to regenerate the menus.

Menu options may appear under a new folder with the description *cannot be assigned* while you are maintaining the selection of business transactions for an activity group. If you see this description, please refer to Online Service System note *85565* for more detailed information.

You have completed the upgrade steps for authorization profiles created in releases before 4.5x.



Appendix A: Online Service System Notes

Contents

Overview

The following table describes the application areas (BC Basis Components) used to search the Online Service System for additional security administrator information:

Application Area	Description
BC-CCM	Computing Center Management System
BC-CCM-USR	Users and Authorizations
BC-CCM-USR-ADM	Users and Authorizations Maintenance
BC-CCM-USR-KRN	Users and Authorizations Kernel Functions
BC-CCM-USR-PFC	Profile Generator
BC-FES-SEM	Session Manager
BC-SRV-REP	Reporting
BC-BMT-OM	Organizational Management
BC-BMT-OM-OM	Organizational Plan

Each application area can also be searched using a keyword such as *profile generator, PFCG, activity group, pre-defined activity groups, authorization, profile, user, SU53, security* and so on.

Online Service System Notes

(As of April 1999)

Legend:

- RI = Release independent
- * = 4.5A and 4.5B
- OR = older release, but still valuable information

Subject	Release	Note	Title
ABAP	*	**69098**	Runtime error due to missing authorizations
Authorization Check	RI	**18529**	Which authorization objects are checked
Authorization	RI	**20643**	Naming conventions for authorizations
Authorization Check	RI	**20534**	Authorization check - a short introduction
Authorization Check , S_TCODE	*	**67766**	S_TCODE: Authorization check on start transaction
Authorization Concept	RI	**28175**	Questions regarding the authorization concept
Authorizations, Reporting Tree	RI	**7642**	Authorization protection of ABAP/4 programs
Authorizations, Trace	RI	**65054**	Trace function: multiple users
Authorizations, Trace	*	**66056**	Authorization trace with Transaction *ST01*
Documentation, ABAP	*	**60382**	New: ABAP/4 Workbench Docuset
Documentation, Basis Knowledgeware Products	OR	**61675**	Info for customer - Basis Knowledge Products
Hot Packages	OR	**33525**	Important Information about Hot Packages
Hot Packages	*	**37617**	ONLINE CORRECTION SUPPORT (OCS)
Hot Packages	*	**42763**	Hot Packages for systems without OSS access
Hot Packages	*	**53902**	
Hot Packages	*	**97612**	New Hot Packages for Profile Generator
Knowledgeware Products	OR	**52286**	Questions and answers on the R/3 Basis Knowledge Product CDs
Naming Conventions	*	**16466**	Customer name range for SAP objects

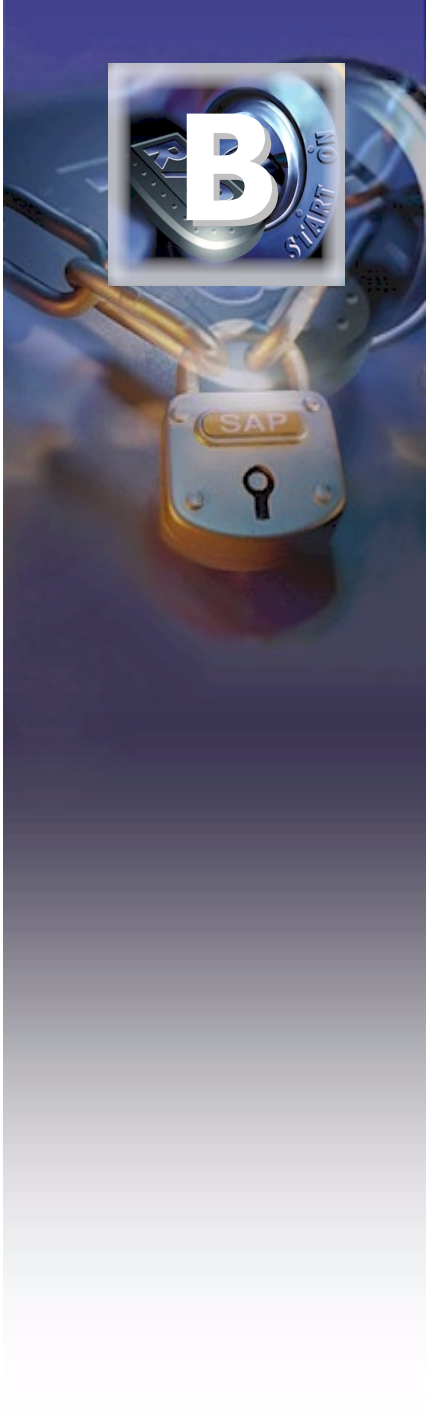
Subject	Release	Note	Title
Organizational Management	*	**31621**	PD and Workflow application do not run correctly
Organizational Management	*	**87540**	Transport planning dates between SAP Systems
OSS	RI	**26740**	OSS Registration Form (for North America)
OSS	RI	**28750**	Documentation on training info in the OSS
OSS	RI	**29501**	Search procedure for notes and messages in OSS
OSS	RI	**30068**	SAP America's Production Registration Form
OSS	*	**32789**	OSS – Quick Reference Sheet
OSS	RI	**33246**	SAPLOGON for OSS
OSS	OR	**35010**	Service connections: Composite note (overview)
OSS	RI	**36677**	Structure of application areas in OSS
OSS	RI	**45027**	User maintenance and creation in OSS for customer
OSS	OR	**50464**	FLCS Feedback for the Notes within the OSS System
OSS	RI	**64417**	OSS corporate group functionality: Collective note
OSS	RI	**75002**	Confirmation of OSS Registration
OSS and OSS1	RI	**17285**	Log on to OSS (Transaction OSS1)
OSS and OSS1	RI	**22235**	OSS1: What to do if R/3 will not run
OSS and OSS1	RI	**33135**	Guidelines for OSS1 (Version for SAPSERV3)
OSS and OSS1	RI	**33221**	Easy-to-use guide for Transaction OSS1
OSS and Printing	RI	**15641**	Print / Download in OSS
OSS and Printing	RI	**26746**	Downloading – Printing notes in OSS
Passwords in R/3	RI	**2467**	Answers on "Security"
Patch download from SAPSERVx	RI	**13719**	Advance transports to customers
Profile Generator	*	**117790**	Replacmnt trans. after upgrade in profile generator
Profile Generator	*	**76802**	Problems with table SMEN_DATES
Profile Generator	*	**79742**	Entire menu branch missing in S000 menu
Profile Generator	*	**80210**	Profile Generator: Collective note
Profile Generator	*	**81508**	PD table infotypes: entries not deleted
Profile Generator	*	**85233**	Profile Generator: profile not assigned

Subject	Release	Note	Title
Profile Generator	*	**85234**	Missing authorization when using the Profile Generator
Profile Generator	*	**85565**	Inexplicable menu options in the activity group
Profile Generator	*	**88216**	NO_BTREE or BRTEE in the display of *PFCG*
Profile Generator	*	**88314**	Problems when scrolling in org. level dialog box
Profile Generator	*	**88573**	Error message 5@011 profile cannot be generated
Profile Generator	*	**103497**	Error 5@022 in profile generation
Profile Generator	*	**89110**	Reference SAP_ALL is missing in profile generator
Profile Generator	*	**89116**	Transaction is missing in PG
Profile Generator	*	**90770**	*0 problem for the PG
Profile Generator	*	**91397**	Nodes in company menu cannot be activated
Profile Generator	*	**93769**	Documentation on the PG
Profile Generator	*	**96836**	Problem with profile number after transport
Profile Generator	4.5A	**97152**	Profile Generator: Authorization codes are missing
Profile Generator	*	**117790**	Replacmnt trans. After upgrade in profile generator
Profile Generator	*	**104992**	Error message "Profiles already exist"
Profile Generator	4.5A	**109212**	Error in the F4 help on the org.level dialog box
Profile Generator	4.5A	**125927**	Authorizations in PFCG are inactive for no reason
Profile Generator	4.5A	**129092**	Activity groups for Customizing projects
Profile Generator	4.5A	**138366**	Problem when printing authorizations
Profile Generator	RI	**144034**	Regeneration of activity groups-authorization loss
Profile Generator	RI	**113290**	Merg. Process with authorization data: Explanation
Profile Generator, Session Manager	*	**75626**	Problem with Session Manager/Report tree
Profile Generator, Transport PD objects (activity groups)	OR	**77607**	Transporting PD objects by client copy
Report RHAUTUP1	OR	**82145**	Activity group maint., user master data comparison
Report RSUSR406	*	**82390**	Generate profile SAP_ALL
SAP Software Change Registration	OR	**27532**	SAP Software Change Registration (SSCR)

Subject	Release	Note	Title
SAP_ALL	*	**82390**	Generate profile SAP_ALL
SAP_NEW	RI	**28186**	What does the profile SAP_NEW do?
SAPNet	RI	**69224**	Access to the SAPNet server with OSS User ID
SAProuter	*	**30289**	SAProuter
SAPSERVx	OR	**40024**	Transferring customer files to sapserv# with ftp
Security in R/3	*	**23611**	FAQs concerning R/3 security
Security in R/3	RI	**27928**	Consequences in transport during password change
Security in R/3	RI	**30724**	Data protection and security in R/3
Security in R/3	RI	**35493**	Secrecy and Data Security Obligations
Security in R/3	*	**66687**	Network security products Secude and Kerberos
Security in R/3, ABAP	RI	**13202**	Security aspects in ABAP/4 programming
Security in R/3, CPI-C	RI	**29276**	SAPCPIC: Where are passwords visible?
Security in R/3, Customer Exit	*	**37724**	Customer exits in SAP log on
Session Manager	*	**46252**	Session Manager Debugging
Session Manager	*	**47810**	Documentation on the Session Manager
Session Manager	*	**61013**	Session Manager Releases and Bug fixes
Session Manager	*	**71340**	Missing menu options in the Session Manager
Session Manager	*	**72758**	Auto Log on and Session Manager
Session Manager	OR	**74089**	Generation of Session Manager menus takes too long
Session Manager	*	**87829**	Problems when transporting session manager menus
Session Manager	4.5A	**97140**	Starting transaction from transaction SESS
Session Manager	4.5A	**130993**	Only S_TCODE check on transaction start
SU01	*	**94104**	User maintenance (*SU01*): Error in address management
SU01	4.5A	**110179**	User SAP* cannot be deleted with SU01
SU01	*	**138254**	SU01: check during passw.change
SU02	*	**92855**	Profile maint. (SU02): scroll bar does not function
SU02	*	**121002**	SU02: Incorrect auth. check when inserting profile
SU21	*	**94294**	Creating authorization objects (SU21): some errors
SU21	*	**111579**	SU21: Dump for key 'Authorization objs'

Subject	Release	Note	Title
SU24	4.5A	**135766**	Incorrect data in SU24
SU53	RI	**23342**	You are not authorized to ... > Analysis
SU53	OR	**78106**	*SU53*: Authorization value contains special chars
SU53	OR	**87926**	*SU53*: Object name overwrites object text
SUIM	*	**38075**	InfoSys/WU list authorization: Result incorrect
System Profile Parameters	RI	**31395**	System parameters: Defined where? Displayed how?
Transporting	RI	**11013**	Transporting profiles and authorizations
Transport	OR	**86544**	Transport profiles, author., in logon language
Transport, User Buffer	RI	**84209**	Authorizations not current after profile transport
Transporting, AS/400	*	**37987**	AS/400: Importing transports
User administration	*	**82390**	Generating profile SAP_ALL
User administration	*	**85676**	Customer objects: conversion of SADR addresses
User administration	*	**93802**	User maintenance in the batch input
User administration	*	**96607**	Changes in the address management in Release 4.0A
User administration	RI	**10187**	Users with large master rec. missing authorizations
User administration	4.5A	**111527**	Short dump for change documents profiles
User administration	*	**111579**	SU21: Dump for key 'Authorization objs'
User administration	4.5A	**129727**	SCUL, SCUA: Raise_exception in child system
User administration	*	**135040**	SU03: No scroll bar in authorization maintenance
User administration	*	**144970**	Cntrl usr admin:only one profle/act.gr.transferred
User administration	*	**144194**	Central user distribution: too many ALE processes
User administration	*	**143999**	Cen. User adm.: SU01 Last change not always dspled.
User administration	*	**138477**	Incorrect change documents in SUIM
User administration	*	**136647**	Use of wildcard '*' in authorizations
User administration	4.5A	**136596**	Delete key active although maintenance not allowed
User creation in Batch Input	RI	**80317**	User creation in batch input: Premature termination
User Information System (SUIM)	OR	**40689**	New reports for the user information system

Subject	Release	Note	Title
User Information System (SUIM)	OR	**85158**	Where-used list: Surnames missing in user list
User SAP*	RI	**4108**	How to assign an identifier to SAP*
User SAP*	RI	**4326**	How do I delete the user SAP*?
Workflow Management	*	**73318**	Q&A: Transport of workflow objects



Appendix B: Frequently Asked Questions

Contents

Overview

This appendix contains some of the most frequently asked questions about R/3 and the Profile Generator (PG). We hope the answers:

- Help you to better understand the system
- Facilitate your implementation
- Resolve basic system issues

Profile Generator Setup

How Does the AUTHORITY-CHECK Work with the Profile Generator?

When AUTHORITY-CHECK is called, the system checks whether the system parameter, *auth/no_check_in_some_cases* is set to *Y*. If the parameter is not set to *Y*, the normal AUTHORITY-CHECK is conducted. If the parameter is set to *Y*, it searches for an entry in table *USOBX_C* (refer to structure *USOBX_C*) with the current transaction code and authorization object. If nothing is found, the normal AUTHORITY-CHECK is conducted. If an entry is found (and *USOBX_C-OKFLAG* is set to *N*) no check is performed, regardless of the actual user profile. In all other cases, the regular authorization check is conducted and succeeds when the user profile contains an authorization with the corresponding expressions for the current object.

In a new installation the parameter is set to *Y*, since the PG is already activated. For further information, see chapter 2.

Do I Need to Shutdown and Restart the Instance After I Changed the System Profile Parameter?

Yes, you must restart the instance after adding the instance profile parameter. For further information on how the PG is set up and what settings need to be performed, see chapter 2, *Setting up the Profile Generator.*

Working with the PG and Profiles

Can I Include an Existing Profile in an Activity Group?

Yes, you can include an existing single profile into an activity group. Please refer to chapter 6, the section *Manually Postmaintaining Authorizations.*

Why Is Only One Profile Sometimes Generated?

Technically, only 150 authorizations can fit into one profile, so several profiles are created for large activity groups. Since the last two digits are required for the internal numerator, only 10 digits are available for the profile name.

Can I Manually Change Generated Profiles?

You can only change generated profiles with transaction *PFCG*, where you have all the same options as in *SU02*. To block generated profiles for maintenance, use *SUO2*.

Can I Include Manual Profiles in the Profile Generator?

In the PG, choosing *Edit* → *Insert auth.* → *from profile* includes all authorizations from a manually created profile in a generated profile. These authorizations remain in manual status and, if the activity group changes, the authorizations remain unchanged when you compare the profile. However, you can only insert authorizations from a single profile.

Can I Manually Enter Generated Profiles in the User Master Record?

Yes, but we do not recommend it for the following reasons:

- If the activity group is extremely large (or is increased by a later change), the PG generates more than one authorization profile and automatically updates the affected user masters, which have to be manually inserted.
- When assigning with the PG, you can include time dependencies and assign the profile for a limited time period. To do this, in the *User assignment* screen:
  1. Select *View* → *Overview* **before** you create the link
  2. Enter the user ID for which you want to create the link
  3. A *Create link* popup appears with a *Period*.
  4. Determine the period for which the *User* <-> *Activity group* link is valid.
  5. This link is stored in HR. For the profile to be withdrawn from the user at the correct time, schedule report *RHAUTUP1* as a background job.

Is it Possible to Change the Profile Name Later?

Yes, only the long text (descriptive text) to a profile can be changed with the PG, which does not affect the authorizations used in this profile. It is not possible to manually change the technical profile name of a generated profile with the PG.

Can I Copy an Activity Group, and Will this Procedure also Copy the Profile?

Yes, you can copy activity groups, but while copying, choose a different name for the new activity group. The activity group, the activities, and the profile data are then copied. Please see chapter 4, the section *Copying and Deriving Activity Groups* for detailed information.

If I Generate a Profile that May Use a Previously Built Authorization, Will the System Create a New One or Use the Existing One?

Every time you generate a new profile for an activity group, new authorizations are created. It takes longer to search for existing authorizations with the same values than to create new ones. Each authorization can only be used in one activity group.

How Do I Restrict Activities by Specific Time Periods?

Even if you do not use BC-Org, you can still choose to assign activity groups to users for a limited time. This action makes sense, for example, when your company enters a new fiscal year. Physical inventory activities should only be allowed for a limited period of time. For further information on setting time limits, please refer to chapter 8.

Which Transactions Are Used by the PG to Maintain a Specific Authorization?

On the *Change Activity Group: Authorizations* screen, choose *Utilities* → *Settings* → *For Overview of Authorization Object Use,* to import an icon into your profile tree. This icon, which looks like a mountain, displays the transactions for which the *Check/maintain* flag is set for the object.

Authorization Checks (SU24)

What Do the Different Check Flags Stand For?

CM (Check/Maintain)

- An authority check is carried out against this object.
- The PG creates an authorization for this object and field values are displayed for changing.
- Default values for this authorization can be maintained.

C (Check)

- An authority check is carried out against this object.
- The PG does not create an authorization for this object, so field values are not displayed.
- No default values can be maintained for this authorization.

N (No check)

- The authority check against this object is disabled.
- The PG does not create an authorization for this object, so field values are not displayed.
- No default values can be maintained for this authorization.

U (Unmaintained)

- No check indicator is set.
- An authority check is always carried out against this object.
- The PG does not create an authorization for this object, so field values are not displayed.
- No default values can be maintained for this authorization.

To learn more about transaction *SU24*, please see chapter 2, the section *Reducing the Scope of Authority Checks in R/3*.

Why Does the Profile Generator Maintain Authorizations for More Objects Than You Can See?

With transaction *SU24* you can browse the entries of tables *USOBX_C* and *USOBT_C*. The PG uses table *USOBX_C* to check for transactions in the corresponding activity groups where the authorization object's authorizations are to be maintained. The corresponding values are stored in table *USOBT_C*. But, the parameter transactions are an exception. These transactions work with a powerful core transaction, restricted by the initial screen of the core transaction that is filled and skipped in the parameter transaction.

The authorization checks are coded exclusively in the core transaction. However, the authorization field values can be specified more precisely in the parameter transaction than in the core transaction. The PG first maintains the authorizations in *USOBX_C* and *USOBT_C* under the parameter transaction, and then lists authorizations for all authorization objects in the core transaction as *to be maintained.* As a result, for the parameter transaction, more authorizations are maintained than can be seen in *SU24*.

For example, transaction *OC41* (which maintains exchange rates) uses the general table maintenance transaction *(SM30).* On the initial screen for *SM30,* enter the view name **`V_TCURR`** and choose *Maintain*. The PG reads *SU24* for *OC41* and maintains an authorization for the object *S_TABU_DIS* with the *Change* and *Display* values for the activity and the *FC32* value for the authorization group. The PG also reads *SU24* for the core transaction *SM30* and maintains an authorization for *S_TABU_CLI* with a *BLANK* value, because this object is not listed in *SU24* under *OC41*.

How Do I Reduce the Scope of Authority Checks in R/3?

Please see chapter 2, the section *Reducing the Scope of Authority Checks in R/3* in this guide.

How Can a Customer Include Individual Authorization Checks in a Transaction?

For individual authorization checks, there are the so-called field exits. These are enhancements that you can create for any data element, and where you can implement your checks. Field exits are always run if a field was selected on a screen for this data element. When you create the field exit, you can determine whether this check should be carried out:

- Always
- Only on certain screens
- Only in certain transactions

For more information on field exits, please look at the online documentation for transaction *CMOD*.

When Starting Transactions, What Should I Know About the New Authorization Check?

Each time a new transaction is called (*MM01*, for example), the system checks whether the user is authorized to start that transaction. (No check takes place for the ABAP command *CALL TRANSACTION*.) If you use the PG and its menus to form activity groups, an authorization for object *S_TCODE* is automatically defined for each activity group. It contains the exact transactions that you selected for the activity group.

If you want to allow transactions that you did not assign using the activity group menu, manually add an authorization for object *S_TCODE*, and enter the missing transactions. You can now avoid problems when you compare the authorization data.

S_TCODE is found in the object class *Nonapplication-specific Authorization objects*. The *S_TCD_ALL* authorization is delivered with the profile *SAP_NEW_40B*, which allows you to execute all transactions. By giving restricted authorizations for *S_TCODE*, the user administrator can restrict individual users or user groups to remain within the transactions

they require. The authorization checks defined by the developer with transaction *SE93* (transaction maintenance), or in the ABAP source code, continue to be performed.

These are the advantages of the new authorization check:

- A guarantee that each transaction performs at least one authorization check
- An easy way to determine which transactions a user can execute

Including Transactions or Reports

How Can I Include Customer-Specific Transactions?

1. Perform one of the following two options:
   - Use transaction *SSM1* and add your transaction to the company menu tree.
     In the same way, you can also include transactions for the PG from the *System* menu option. Transactions from this menu option are not displayed automatically in the company menu.
   - If you activated a menu enhancement (in the SAP menu tree S000) for your own transactions, first reset the SAP and company menu, then regenerate the SAP and company menu.
2. Maintain the default values for your transactions in *SU24*.

Please refer to chapter 2, the section *Generating the SAP Standard Menu and Company Menu* and the following sections in chapter 6: *Adding your Customer Transaction to the SAP Menu Tree* and *Adding any Missing Transactions to the Company Menu*.

How Can I Include Individual Authorization Checks in Transactions?

For individual authorization checks, there are the so-called field exits. These are enhancements that you can create for any data element, and where you can implement your checks. Field exits are always run if a field was selected on a screen for this data element. When you create the field exit, you can determine whether this check should always be carried out only on certain screens or in certain transactions. Further details on field exits can be found in the online documentation for transaction *CMOD*.

How Can I Include Reports in the Profile Generator? Are the IS Solutions Already Integrated?

IS solutions and reports will be integrated later so that authorization profiles can be automatically generated.

Missing Authorizations

What if an Authorization Is Still Missing for the Generated Profile, and the User Gets a "No authorization..." Message?

Create an Online Service System message to specify the transaction and the precise error message (preferably a copy of the output from transaction *SU53*) that you included in the activity group. To correct the error in your system, please refer to chapter 6, the section *Manually Postmaintaining Authorizations*.

User Administration

How Can You Set Up Remote User Administrators?

Since the PG selects the authorization objects, it is no longer necessary to decide who maintains authorizations for an object. The check against the object *S_USER_AUT* is carried out only if the administrator manually inserts an authorization. With authorization object *S_USER_AGR,* a check is possible at the activity group level to see who is allowed to select which transaction for this activity group. For a further classification into authorization and activation administrator, see *Administration When Using the Profile Generator* in the online documentation.

Session Manager

Where Can I Find More Documentation on the Session Manager?

Documentation for the GUI part of the Session Manager can be obtained by clicking on the *Help* icon in the Session Manager. To access the documentation on preparing to work with the Session Manager:

1. Go to the Enterprise IMG.
2. Choose *Basis* → *Front-end services* → *Session Manager*.
3. Double-click on *Session Manager* to access the required documentation.

Transporting

Is There a Way to Transport Activity Groups?

Yes, you can either use the standard transport connection in transaction *PFCG* or use mass-transport activity groups inside the PG.

Does the Transport of Activity Groups Between Two Clients, in the Same System, Work with Transaction *SCC1*?

Yes, after being imported to the target client, the transported activity groups are now active and do appear in transaction *PFCG*. This step was not possible in releases before 4.0B.

What if the Generated Profile Only Has Authorizations for Object S_TCODE?

The SAP default tables may not have been copied into the customer tables. If you get a *No organizational data available* message, run transaction *SU25*. Please see chapter 2 in this guide for more detailed information on transaction *SU25*.

Menu Generation

What Does the Checkbox “without company IMG filtering” (in the Company Menu Generation SSM1) Mean?

While generating the Enterprise IMG, choose *Tools* → *Business Engineering* → *Customizing* → *Basic functions* → *Generate Enterprise IMG* to select the business application components that your company implements. This impacts the SAP standard menu. To ensure that you begin with the standard SAP menu tree (as SAP delivers it), please select *without company IMG filtering*. For more detailed information, please refer to Online Service System note *71340*.

Tables

How Do I Display the Transaction Codes that Are Included in an Activity Group?

Run transaction **SE16** *(Tools → ABAP Workbench → Overview → Data Browser)*.

1. Enter **AGR_TCODES** in the *Table name* field.
2. Display the table contents (*Table → table contents*).
3. In the selection screen, enter the activity group name in the field *AGR_NAME*.
4. Choose *Execute* (or choose *Program → Execute)*.
5. You will receive a list with all transaction codes in that activity group name.

How Do I Display in Which Activity Group a Certain Transaction Code Is Being Used?

Run transaction **SE16** *(Tools → ABAP Workbench → Overview → Data Browser)*.

1. Enter **AGR_TCODES** in the *Table name* field.
2. Display the table contents (*Table → table contents*).
3. In the selection screen, enter the transaction code in the field *TCODE*.
4. Choose *Execute* (or choose *Program → Execute)*.
5. You will receive a list with all activity groups name where that transaction code is being used.

How Do I Display Which Activity Group Is Used by Which User?

Run transaction **SE16** *(Tools → ABAP Workbench → Overview → Data Browser)*.

1. Enter **AGR_USERS** in the *Table name* field.
2. Display the table contents (*Table → table contents*).
3. In the selection screen, enter the activity group name in the field *TAGR_NAME*.
4. Choose *Execute* (or choose *Program → Execute)*.
5. You will receive a list with the names of all users that are assigned to that activity group.

How Do I Display Which User Is Assigned to Which Activity Group?

Run transaction **SE16** *(Tools → ABAP Workbench → Overview → Data Browser)*.

1. Enter **AGR_USERS** in the *Table name* field.
2. Display the table contents (*Table* → *table contents*).
3. In the selection screen, enter the name of the user in the field *UNAME*.
4. Choose *Execute* (or choose *Program* → *Execute)*.
5. You will receive a list with the all activity groups this user is assigned to.

Does the Authorization Object Allow Activities Not Maintained in Table *TACTZ?*

Table *TACTZ* contains allowable activities for an authorization object. If you find a transaction looking for an authorization object with an activity that is not maintained or offered by PG, maintain the missing activity for the appropriate authorization object in table *TACTZ* with transaction *SM31*. The PG then offers this value.

What Is the Structure of Table USOBX_C?

Field name	Key	Description
NAME	X	Program/transaction/function module name
TYPE	X	Type of report
OBJECT	X	User master maintenance: authorization object
MODIFIER		Last changed by
MODDATE		Date of change
MODTIME		Time of change
OKFLAG		N = No authorization checks X = Authorization checks take place Y = Authorization checks take place; default values in USOBT_C U = Not maintained

The *NAME* and *TYPE* fields identify a transaction, and *OBJECT* identifies the authorization object. *MODIFIER*, *MODDATE*, *MODTIME* contain administrative information about the most recent changes. *OKFLAG* is important because when it contains the value *N*, no authorization check is performed for the transaction and authorization object.

Examples

Enter *NAME* = **VA01**, *TYPE* = **TR**, *OBJECT* = **C_STUE_BER**, *OKFLAG* = **N**. Every authorization check, AUTHORITY-CHECK OBJECT C_STUE_BER ID... will succeed, regardless of the user's authorization profile.

Enter *NAME* = **VA01**, *TYPE* = **TR**, *OBJECT* = **C_DRAW_TCD**, *OKFLAG* = **X** or another value <> **N**. An authorization check, AUTHORITY-CHECK OBJECT C_DRAW_TCD ID... will succeed only when the user's authorization profile contains the combination of fields or field contents, under ID.

Infotypes

How Do I Display Data Stored in an Infotype?

Run transaction **SE16** (*Tools* → *ABAP/4 Workbench* → *Overview* → *Data Browser*).

1. Enter the infotype number in the *Table name* field.
2. Display the table contents (*Table* → *table contents*).
3. In the selection screen, enter the necessary data.
4. Choose *Execute* (*Program* → *Execute*).
5. Print the list.

Appendix C: Important System Profile Parameters

Contents

Incorrect Logons, Default Clients, and Default Start Menu

Use the following system profile parameters to set incorrect logon limits and the default client:

- **Login/fails_to_session_end**

  This parameter defines the number of times a user can enter an incorrect password before the system terminates the logon attempt. The default is three characters, but this value can be set to any number between 1–99.

- **Login/fails_to_user_lock**

  This parameter defines the number of times a user can enter an incorrect password before the system locks the user from making additional logon attempts. If the system locks, an entry is written to the system log, and the lock is released at midnight. The default is 12 times, but this value can be set to any value between 1–99.

- **Login/failed_user_auto_unlock**

  This parameter unlocks users who got locked out by logging on incorrectly. If the parameter is set to *1* (the default), due to a previous incorrect logon attempt, the system does not consider users locked. The locks remain if the parameter value is *0*.

- **Login/system_client**

  This parameter specifies the default client. This client is automatically filled in on the system logon screen. Users can enter a different client.

- **Login/ext_security**

  Since Release 3.0E, external security tools such as Kerberos or Secude have managed R/3 System access. If this parameter is set, an additional identification can be specified for each user (in user maintenance) where users log on to their security system. To activate, set the value to *X*.

- **Start_menu**

  This parameter specifies the default start menu for all users and can be overwritten with the user-specific start menu (transaction *SU50*). The default is *S000*, and this value can be set to any other area menu code.

Setting Password Length and Expiration

Use the following system profile parameters to specify the minimum length of a password and the frequency with which users must change passwords.

- **Login/min_password_lng**

  This parameter defines the minimum password length. The default is three characters, but this value can be set from three to eight characters.

- **Login/password_expiration_time**

  This parameter defines the number of days after which a password must be changed. The parameter allows users to keep their passwords without time limit and leaves the value set to the default, 0.

To make the parameters globally effective in an R/3 System, set them in the default profile, *DEFAULT.PFL*. To make them instance-specific, you must set them in the profiles of each application server in your R/3 System.

Specifying Impermissible Passwords

To forbid use of a certain password, enter it in table *USR40*. You can maintain this table with transaction *SM30*. In *USR40*, you may also generically specify prohibited passwords.

There are two wild-card characters:

- A question mark (?) means a single character.
- An asterisk (*) means a sequence of any combination characters of any length.

Examples:

- *123** in table *USR40* prohibits any password that begins with the sequence 123.
- **123** prohibits any password that contains the sequence 123.
- *AB?* prohibits passwords that begin with AB and have an additional character, such as ABA, ABB, and ABC.

Securing SAP* Against Misuse

Login/no_automatic_user_sap*

If the parameter is set to *1*, then *SAP** has no special default properties. Resetting the parameter to *0* allows logins with **`SAP*`**, password **`PASS`**, and unrestricted system access privileges. Even if you set the parameter, ensure that there is a user master record for *SAP**. If a user master record for *SAP** exists, it behaves like a normal user, is subject to authorization checks, and its password can be changed.

Tracing Authorizations

Auth/check_value_write_on

By entering transaction **`SU53`** in the *Command* field, you can analyze an authorization-denied error that has just occurred in your session. This function is active only if you have set the system profile parameter to a value greater than *0*. By default, the function is inactive, and the parameter value is *0*.

Profile Generator and Transaction SU24

Auth/no_check_in_some_cases

By using transaction **SU24**, you can activate or deactivate authorization checks for transactions. This function is active only if you set the system profile parameter to *Y*. By default, the function is inactive, and the parameter value is *N*. To activate the parameter, set the value to *Y*. If you want to work with the PG, the parameter must be set.

User Buffer

Auth/auth_number_in_userbuffer

To have a good performance in the system, the names of all the authorizations included in a user master for a user are buffered in a table. In the standard, this buffer can deal with up to 1,000 authorizations. If a user has more than 1,000 authorizations the value can be set to *2000*. The default value is *800*, but this default value can be set to between 1–2000. If for any reason you have to reset the user buffer, see Online Service System note *84209* and *75908* for detailed information.

No Check on Object S_TCODE

Auth/no_check_on_tcode

From Release 3.0E, the system checks on object *S_TCODE*. In specific instances, you can turn this check off, but this step results in a big security risk for your system. By default, the function is inactive, and the parameter value is *N*. To switch the check off set the value to *Y*.

No Check on Certain ABAP Objects

Auth/system_access_check_off

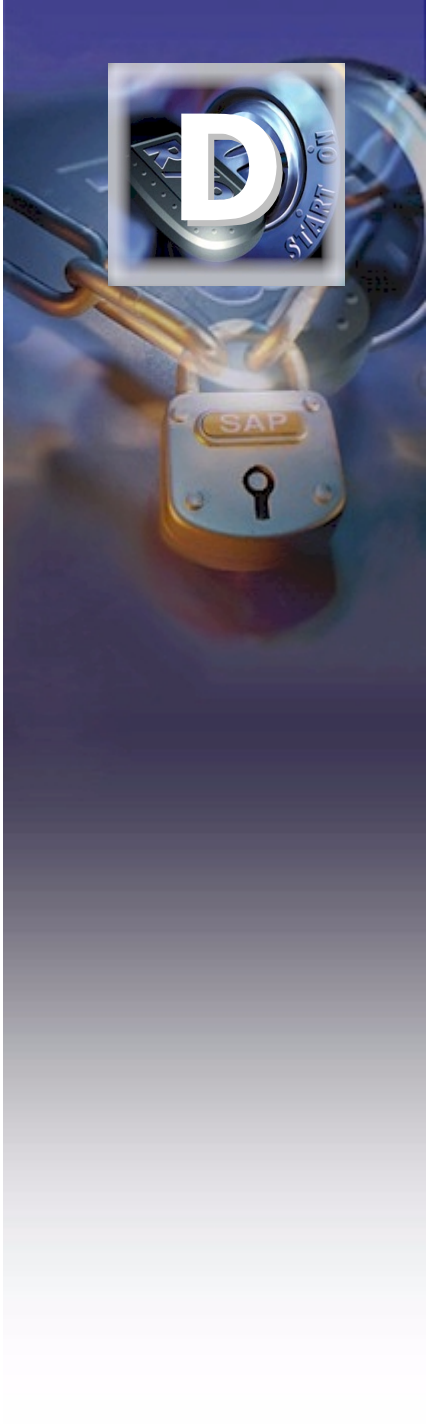
Use this parameter to turn off the automatic authorization check for particular ABAP language elements (file operations, CPIC calls, and calls to kernel functions). This parameter ensures the downward compatibility of the R/3 kernel. By default, the function is inactive (value = *0* and check remains active). To turn the check off, set the value to *1*.

RFC Authority Check

Auth/rfc_authority_check

You can use this parameter to determine whether object *S_RFC* is checked during RFC calls.

- Value = *0*, no check against *S_RFC*
- Value = *1*, check active but no check for *SRFC-FUGR*
- Value = *2*, check active and check against *SRFC-FUGR*



Appendix D: Frequently Used Transactions

Contents

Overview

The following tables show some useful transactions for working with authorizations. Although many transactions are not described in detail in this guidebook, we thought it is worth mentioning them. Bear in mind that some transactions are for more "advanced" functions than those targeted in the scope of this guidebook and therefore improper use could damage the system. Those transaction codes are indicated by an "X" in the column "Dangerous."

Transaction Code Switches

/n<trans code>	Exit current transaction and start the new transaction.
/o<transcode>	Open a new session (window) and start a new transaction.

Authorizations/User Administration Function

Transaction Code	Menupath	Description	Dangerous
PFCG	Tools→ Administration, User Maintenance→ Activity Groups	Maintain Activity Groups (Profile Generator)	
SU24	Tools→ Business Engineer→ Customizing; select Enterprise IMG→ Basis Components→ System Administration→ Users and Authorizations→ Maintain Authorizations and Profiles Using Profile Generator→ Work on SAP Check Indicators and Field Values→ select Change test status	Maintain check indicators for transaction codes	
SU25	Tools→ Business Engineer→ Customizing; select Enterprise IMG→ Basis Components→ System Administration→ Users and Authorizations→ Maintain Authorizations and Profiles Using Profile Generator→ Work on SAP Check Indicators and Field Values→ select Copy SAP test statuses and field values	Installing and upgrading the Profile Generator	

Transaction Code	Menupath	Description	Dangerous
SESS		Session Manager	
SU01D	Tools→ Administration, User Maintenance→ Display Users	Display Users	
SU01	Tools→ Administration, User Maintenance→ Users	Maintain Activity Groups (Profile Generator)	
SU02	Tools→ Administration, User Maintenance→ Profiles	Maintain Authorization Profiles	X
SU03	Tools→ Administration, User Maintenance→ Users	Maintain Authorizations	X
SU10	Tools →Administration, User Maintenance →Environment → Mass changes →User profile	Mass Changes to User Master Records	X
PPOC	Human resources→ Organizational management→ Simple maintenance →Basic org. plan →Create	Create Organizational plan	
PPOM	Human resources→ Organizational management→ Simple maintenance →Basic org. plan → Change	Maintain Organizational Plan	
SUIM	Tools→ Administration, User Maintenance→ Repository Infosys.	Infosystem Authorizations	
SUPC		Activity Groups: Execute User Master Record Adjustment	
PFUD	Tools→ Administration, User Maintenance→ Activity Groups→ Goto→ Mass Compare	User Master Data Reconciliation	

Miscellaneous Transactions

Transaction Code	Menu Path	Description	Dangerous
SSM1	Through IMG	SAP menu and company menu generation	
SPRO	Tools→ Business Engineer→ Customizing	Implementation Guide (IMG)	
SA38	System→ Services→ Reporting	Execute Reports	
SE38	Tools→ ABAP Workbench→ ABAP Editor	ABAP Editor	X
SE16	Tools→ ABAP Workbench→ Overview→ Data Browser	Data Browser	
SCC1	Tools→ Administration→ Client admin.→ Special functions→ Copy transport request	Transporting between clients	X
SCCL	Tools→ Administration→ Client admin.→ Client copy→ Local Copy	Client import – postprocessing	X
SCC8	Tools→ Administration→ Client admin.→ Client transport→ Client export	Client export	X
ST01	Tools→ Administration→ Monitor→ Traces→ System Trace	System Trace	
SU53	System→ Utilities→ Displ. Auth. Check	Display Check Values	
RZ10	Tools →CCMS, configuration → Profile Maintenance	Maintenance of profile parameters	
SE10		Customizing Organizer	
OSS1		OSS login	

Glossary

Term	Definition
ABAP	ABAP is an interpretative, platform-independent, fourth-generation language tailored to develop business applications. The language supports structured programming and contains elements necessary to call external relational databases through open SQL calls or database-specific native SQL calls. The developer is not required to know the underlying infrastructure.
ABAP Development Workbench	The ABAP Development Workbench provides a complete client/server runtime environment and extensive management and tuning tools. The Workbench is SAP's integrated toolset to develop enterprise-wide client/server applications. This tool-set is particularly suited to R/3 customers who want to enhance standard R/3 business applications with customized, add-on functionality. The major components of the ABAP Development Workbench include: ▸ ABAP Programming Language ▸ ABAP Dictionary ▸ ABAP Editor ▸ ABAP Function Library ▸ Data Modeler ▸ R/3 Repository ▸ Test Tools, Screen Painter ▸ Menu Painter, Workbench Organizer/Transport System ▸ R/3 Repository Information System The workbench is also available to companies who are not R/3 users, but want the benefits of SAP's proven development environment for their software projects.
ABAP Dictionary	The ABAP Dictionary, a component of the Development Workbench, is a central information base for application and system data. The Dictionary describes this data from a logical point of view and stores information about how the data is reproduced in the underlying relational database. The ABAP Dictionary is active and fully integrated with the other Development Workbench tools. Any changes to the Dictionary are automatically and immediately updated throughout the system.

Term	Definition
ABAP Editor	The ABAP Editor, a component of the Development Workbench, provides the following functions to support the application developer: ▸ Syntax check with automatic correction of errors ▸ Insertion of coding patterns for frequently used instructions ▸ Navigation into other workbench tools ▸ Generation of where-used lists for all data objects ▸ Split-screen editor with program comparison
Activation administrator	An activation administrator activates authorization profiles and authorizations, making them effective in the system. These administrators can only change or delete the profiles and authorizations specified in their authorization profile.
Active plan version	This is the plan version that the R/3 System recognizes as valid and currently in operation. The information in the active plan version is used to perform all day-to-day processing and cross-application maintenance. You must designate one plan version active if: ▸ You are a SAP Business Workflow user ▸ Integration is active between PD and other R/3 business applications, such as the PG Your selected plan should reflect the actual state of operations at your firm. Any other plan versions your company maintains can be used to experiment with different organizational scenarios.
Activity group	An activity group is a collection of individual activities that are routinely performed together or are affiliated in some way. For example, the translation tasks activity group could include all tasks, reports, and transactions associated with translation. You set up activity groups by linking single activities under an activity group name. A single activity may be included in more than one activity group.
Application server	A computer where the application logic and application control services of the R/3 System run.
Authorization	An authorization is the authority to perform a particular action in the R/3 System. Each authorization refers to one authorization object and defines one or more possible values for each authorization field listed for that authorization object. A user's authorizations are combined in a profile that is entered in the user's master record.
Authorization administrator	The user responsible for maintaining authorizations and authorization profiles is the authorization administrator. For security reasons, this user should not be authorized to activate authorizations and profiles or to maintain user master records. Otherwise, one user would single-handedly define, activate, and assign system access authorizations.

Term	Definition
Authorization check	This check decides whether a user is authorized to execute a particular function. Processes, functions, and data accesses in the R/3 System can only be performed when user authorizations have been checked in the respective system and application programs.
Authorization concept	General access to a standard database for different applications requires reliable mechanisms designed to ensure the confidentiality of personal information. A multilevel, graded authorization concept has been set up to regulate data access. Only those people with active user master records can access the system. The authorization concept covers the structure and functionality of authorization assignment and checking in the R/3 System. Authorizations protect the system from unauthorized access.
Authorization field	One element of an authorization object is the authorization field. In authorization objects, these fields represent values for individual system elements, which undergo authorization checking to verify a user's authorization.
Authorization group	An authorization group is the combined fields of the authorization objects *S_DEVELOP* (program development and program execution) and *S_PROGRAM* (program maintenance). The authorization group field contains the name of a program group that allows users to perform the following operations: ▸ Execute programs ▸ Schedule jobs for background processing ▸ Maintain programs ▸ Maintain variants When creating a program, you can specify an authorization group as one of the program attributes. This step allows you to group programs for authorization checking.
Authorization object	Another element of the authorization concept is the authorization object that allows you to define complex authorizations. An authorization object groups up to 10 authorization fields in an "AND" relationship to check whether a user is allowed to perform a certain action. To pass an authorization test for an object, the user must satisfy the authorization check for each field in that object.
Authorization profile	The authorization profile is another element of the authorization concept that gives users access to the system. The profiles contain authorizations identified by the authorization object and the authorization name. If a profile is specified in a user master record, the user has all the authorizations defined in that profile.
Authorization trace	This is a transaction that records all the required authorization objects in a processing step.
Background process	The background process is the noninteractive execution of programs, which in the R/3 System, are handled like online operations. Background processes often use the same programs that control the dialogs.

Term	Definition
Business process	Business processes group tasks made across cost centers in your company. This process enables you to structure your company's processes by function. Examples include: ▸ Developing a product ▸ Drawing up a quotation ▸ Purchasing a material ▸ Processing an order
Business Workflow (SAP)	This support, provided for by transaction processing in the R/3 System, takes into account the business environments' needs.
Check indicator	A check indicator is set to determine whether authorization objects are unmaintained, not checked, checked, or checked/maintained.
Client/server architecture, 3-tier	Owing to the software-oriented client/server architecture of the R/3 System, logic and data of the three implemented levels—database, application, and presentation services—can be distributed among dedicated servers. The individual services can be flexible, either as clients or servers, depending on the tasks to be performed in each case.
Customizing & Configuration	In SAP terminology, customizing is the implementation of configurations within the flexibility of the R/3 System. It is the basis for every R/3 project, whether it is an introduction, subsequent project stage, or process change. The configuration includes: ▸ R/3 Procedure Model, a procedural guide for structuring a SAP implementation ▸ R/3 Reference Model in the Business Navigator, a graphical description of business processes ▸ Implementation Guide (IMG), menu-led parameter settings ▸ Project management through upload and download facilities and to and from Microsoft Project ▸ A model company (IDES), a fully integrated and preconfigured system used for training and testing The customizing tools also belong to the Business Engineering Workbench and are provided at no extra charge with the R/3 System. Add-on customizing is discussed in the *ABAP Development Workbench* section.
Database server	This is the computer where a database is installed. Specially optimized hardware may be used for running databases.
Desktop	A PC that is used as a workstation is considered to be desktop. Ideally, the desktop has access to all systems and functions needed for a user to manage authorized tasks.

Term	Definition
Dynpro	Short for dynamic program, a dynpro consists of a screen and associated processing logic, such as validation procedures. Each dynpro controls exactly one dialog step.
Generate	This function saves and activates an object. Before activating the object, the system automatically performs a consistency check.
GSS-API	The GSS-API is the standardized Security API with a standard communication model to abstract from the individual products and their characteristics. The Common Authentication Technologies (CAT) work group of the Internet Engineering Task Force (IETF) defines the standardization proposals. The functional specification of GSS-API Version 2, the version supported by R/3, is currently an Internet draft.
Human resources planning	Personnel planning and development deals with anticipating future personnel needs. Planners should consider short-, medium-, and long-term goals when considering company policy and the costs involved. Good human resources planning ensures that the company has the appropriate number of employees with the required skills in the correct position.
IMG activity	An Implementation guide (IMG) activity is an explanation of a system-setting activity. Activities in the IMG are linked directly to the corresponding customizing transactions, used to create the appropriate system setting. You can use IMG activities to record the notes that document your system settings. You can also base the recording or status of project management information on IMG activities.
Implementation	This process involves switching from an existing management system and business practice and having R/3 run part of, or the entire, business.
Implementation Guide	Also referred to as the IMG, the guide is a tool for configuring the R/3 System to meet customer requirements. For each business application, the implementation guide: ▸ Explains all the steps in the implementation process ▸ Tells you the SAP standard (factory) settings ▸ Describes system configuration work (activities) and interactively opens the activities The IMG are structured as hypertext. The hierarchical structure reflects the structure of the R/3 business application components and lists all the documentation related to implementing R/3. The IMG contains active functions with which you can: ▸ Open customizing transactions ▸ Write project documentation ▸ Maintain status information ▸ Support your project documentation work and the management of your R/3 System implementation.

Term	Definition
Implementation project	This project relates to the implementation of a specific group of R/3 functions and processes with a common go-live date.
Implementation strategy	An implementation strategy is an approach to R/3 implementation. The strategy is based on long-term perspectives and includes all steps across the whole enterprise planned in connection with implementing the R/3 System. Establishing this strategy is an essential part of project preparation and impacts the sequence of implementation projects.
Infotype	Infotypes allow you to describe, or define the different attributes that objects have. Within personnel development (PD) there are many different infotypes, each one describing a specific set of attributes. Some infotypes apply only to certain types of objects, while others can be defined for any type of object.
Instance profile	The instance profile contains application server-specific configuration parameters, which complete the set values of the default profile.
Job	A job is a general classification of work duties, such as secretary and manager. Many employees may have the same job classification. That is, there can be 20 secretaries and eight managers. Jobs should not be confused with positions (see below).
Menu	Menus are control elements, offering the user a range of options which, when chosen, prompts the system to execute an action. One action might be the opening of a subordinate *possible entries* menu. The layout of the menu bar or the *possible entries* menu, has been defined for each R/3 System level. Menu options are selected either with a single mouse click or by positioning the cursor and by pressing *Enter*.
Menu bar	A menu bar is the menu on a screen or window. The bar is located between the title and standard toolbars. When you choose a menu option from the menu bar, you open the corresponding *possible entries* menu. You can maintain up to six *possible entries* menus in a menu bar. The system automatically includes the *System* and *Help* menus.
Name range	The name range is a key area of a table. It effectively reserves part of the key area only for customers or for SAP.
Network security	Network security is a network connection configured to protect SAP and its customers from problems, such as unauthorized access inherent to WAN network connections.
Organizational level	Organizational levels are hierarchical levels where certain data in a material master record is created. Examples of organizational levels are client, plant, and storage location.

Term	Definition
Online Service System	The Online Service System provides a direct communication link to SAP, allowing customers to quickly and efficiently obtain problem-solving information for the R/3 System.
Password	A password is a user code that comprises the following elements that users need to logon to the system: ▸ String of figures ▸ Letters ▸ Special characters that the user must enter ▸ A user ID
Plan version	A plan version is a designated area where you deposit, or store, sets of information. Whenever you enter any information in PD, you must specify the plan version where the information should be kept. A single plan version could include information from any of the PD modules, such as Organization and Planning, Seminar and Convention, or Shift Planning. You can maintain more than one plan version. This allows you to use different plan versions to represent different scenarios for your firm. However, you must designate one plan version as the active plan if you are a SAP Business Workflow user and if integration is active between PD and other R/3 business applications.
Position	Positions are the individual employee placements or assignments in a company (for example, secretary of marketing or a sales manager). By creating positions and creating relationships between the positions, you identify the authority structure or chain of command at your firm. Positions should not be confused with jobs (see above).
Presentation server	A computer, usually a PC or Macintosh, used for presentation in the R/3 System is called a presentation server.
Process flow view	The process flow view is one of the two navigation paths in the Business Navigator, the other being the component view. The process flow view of the R/3 Reference Model provides process-oriented access to the scenarios and processes in the Model. It is arranged as a structure with the following levels: ▸ Enterprise areas ▸ Scenario processes ▸ Processes
Process selection matrix	The process selection matrix is a model type in the R/3 Reference Model. The matrix describes the assignment of processes to scenarios, which are the columns in a process selection matrix. Processes belonging to a scenario are listed and assigned under that scenario (column head). Scenario and process icons provide access to corresponding EPCs.

Term	Definition
Profile	A profile is a collection of authorizations for particular user groups, entered in the user master record. The same profile can be assigned to any number of users. There are two types of authorization profiles: ▸ Simple, a collection of authorizations for a particular task ▸ Composite, a collection of several simple profiles
Profile comparison	When an activity group is modified using transaction *PFCG,* its associated authorization profile is not automatically updated. The user must carry out a profile comparison to ensure that the authorizations contained in the authorization profile correspond with the new contents of the activity group.
Profile Generator	The Profile Generator (PG) supports the authorization administrator setting up the authorization concept at the customer site. According to a set of application components chosen by the administrator, the PG automatically creates an authorization profile. The administrator can then easily customize and modify the authorizations in the profile by using special maintenance transactions offered by the PG.
Program attribute	A property of a program is called a program attribute. The attributes of an ABAP program define its basic characteristics, so that the system can process it correctly. The program attributes include the following elements: ▸ Program title ▸ Program type ▸ Program status ▸ Authorization group ▸ Development class
Push button	Push buttons, or buttons, are graphical control elements that you click once to execute the functions linked to them. In the R/3 System, you can also start functions with the keyboard. To do this, place the cursor on the button and press either the *Enter* key or *Enter* button. Push buttons may contain text or graphic symbols.
Radio button	The radio button is another graphical control element that allows the user to select an item from a list of fields. If the user is allowed to select several fields at once, checkboxes are used.
Release Changes and Upgrades	You can generate specific IMG for release upgrades or changeovers. These guides contain a specific list of IMG activities, including all changed or new functions in the new R/3 release. This facilitates the implementation of release projects. All release notes can also be immediately accessed from this location.

Term	Definition
Report	A report selects data from a database and displays it in a structured form for analysis. You may print the report results or display them online. The system also provides the option of saving the selected report data, to review without having to re-create it.
Responsibility	Responsibilities differentiate authority profiles generated from activity groups. Responsibilities are linked to authority profiles and to activity groups. An activity group is an object where you collect a number of system activities. An authority profile is generated using PG, which designates the user's authorities in the system.
SAP Business Workflow	SAP Business Workflow 3.0® comprises technologies and tools to automatically control and execute cross-application processes, which primarily involves coordinating the: ▸ Persons involved ▸ Work steps required ▸ Data (business objects) that need to be processed Our primary goals with the workflow are to reduce throughput times, to reduce the costs involved in managing business processes, and to increase transparency and quality.
SAP standard menu	From the SAP standard menu, you can access the full range of SAP functions.
SAPgui	SAPgui is the graphical user interface of the R/3 System.
SAProuter	SAProuter is a software module that acts as part of a firewall system. SAProuter simplifies the configuration of network security and the routing of traffic to and from R/3. The SAProuter establishes an indirect connection between the R/3 network and an outer network. There is restricted access to the application layer between client software and the R/3 application server.
Screen	A screen is, essentially, the primary window of a session.
Secure Network Communications (SNC)	Within the framework of the Secure Network Communications project, SAP is implementing the GSS-API in R/3, enabling R/3 to be integrated into company-wide network security systems, such as Kerberos or SecuDE. As the GSS-API is the standard interface in the security area, SAP operates with all GSS-API compliant security systems.
Select	This function allows you to select an object for further processing by placing the cursor on the object and clicking on the object.
Session	A session is a window where the user processes a certain task. When you log on to the R/3 System, it automatically opens the first session, but you can simultaneously open up to nine sessions. The number of the current session appears in the status bar.

Term	Definition
Session Manager	The Session Manager is SAP's new GUI for working with the R/3 System. It offers an updated user interface and the ability to customize menus. A user can choose between three different views of R/3: ▸ The complete SAP menu ▸ The enterprise-specific menu ▸ The user-specific menu Additionally, the Session Manager allows you to simultaneously log on to more than one R/3 System.
SSCR	SAP Software Change Registration (SSCR) is a procedure that registers all modifications to R/3 Repository objects and provides an overview of modified R/3 Repository objects. SAP matchcodes and tuning measures, for example, creating database indices and buffers, are not registered by SSCR.
System parameter	A system parameter is the basic system configuration required to ensure smooth functioning of the software.
Table	Data can be arranged in table form. A table consists of columns (data values of the same type) and rows (data records). Fields identify a record.
Transaction	A transaction is a series of related steps required to perform a certain task.
Transaction code	A sequence of four characters represents a SAP transaction. To call a transaction in the R/3 System, you can follow an IMG path or enter the transaction code in the command field. For example, *SM31* is the code for the table maintenance transaction.
User maintenance	User maintenance transactions allow the system administrator to create and maintain user master records. This process includes generating and assigning authorizations and their profiles.
User master record	This record contains important master data for an R/3 System user. Only users with a user master record can logon to the system. A user's authorizations are defined in the user master record.
User menu (Session Manager)	The user menu is a Session Manager facility. The menu provides access to a restricted selection of task-specific functions derived from the company menu, and is based on a user's regular activities.
Validity period	Validity periods define the life span of an object or infotype record. When creating objects and infotype records, specify a validity period by providing a start and an end date.
Work process	The application services of the R/3 System perform special work processes, such as for dialog processing, updating of the database as dictated by change documents, background processing, spooling, and lock management. Work processes can be assigned to dedicated application servers.

Term	Definition
Workbench Organizer / Transport system	The Workbench Organizer is a central management tool for large-scale project management that supports individual developers and large project teams. The Organizer also does the following: 1. Organizes related project components into orders 2. Locks the components during development 3. Stores a version of each project between transports The transport system supports the transfer of development objects between distributed systems by creating an extensive log recording of when and why each transport was executed and who executed it.
Workflow task	A workflow task is a multistep task defined by the customer, which references a workflow definition. Workflow tasks (organizational management object type WF) are client dependent, have a validity period, and are plan-version specific.
Workload monitor	The workload monitor displays the distribution of the workload across servers and transactions.

Index

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W