

# Users and Roles (BC-CCM-USR)



**Release 4.6C**



## Copyright

© Copyright 2001 SAP AG. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.

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

Microsoft<sup>®</sup>, WINDOWS<sup>®</sup>, NT<sup>®</sup>, EXCEL<sup>®</sup>, Word<sup>®</sup>, PowerPoint<sup>®</sup> and SQL Server<sup>®</sup> are registered trademarks of Microsoft Corporation.

IBM<sup>®</sup>, DB2<sup>®</sup>, OS/2<sup>®</sup>, DB2/6000<sup>®</sup>, Parallel Sysplex<sup>®</sup>, MVS/ESA<sup>®</sup>, RS/6000<sup>®</sup>, AIX<sup>®</sup>, S/390<sup>®</sup>, AS/400<sup>®</sup>, OS/390<sup>®</sup>, and OS/400<sup>®</sup> are registered trademarks of IBM Corporation.

ORACLE<sup>®</sup> is a registered trademark of ORACLE Corporation.

INFORMIX<sup>®</sup>-OnLine for SAP and Informix<sup>®</sup> Dynamic Server<sup>™</sup> are registered trademarks of Informix Software Incorporated.

UNIX<sup>®</sup>, X/Open<sup>®</sup>, OSF/1<sup>®</sup>, and Motif<sup>®</sup> are registered trademarks of the Open Group.






HTML, DHTML, XML, XHTML are trademarks or registered trademarks of W3C<sup>®</sup>, World Wide Web Consortium, Massachusetts Institute of Technology.

JAVA<sup>®</sup> is a registered trademark of Sun Microsystems, Inc.

JAVASCRIPT<sup>®</sup> is a registered trademark of Sun Microsystems, Inc., used under license for technology invented and implemented by Netscape.

SAP, SAP Logo, R/2, RIVA, R/3, ABAP, SAP ArchiveLink, SAP Business Workflow, WebFlow, SAP EarlyWatch, BAPI, SAPPHIRE, Management Cockpit, mySAP.com Logo and mySAP.com are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world. All other products mentioned are trademarks or registered trademarks of their respective companies.

## Icons

Icon	Meaning
	Caution
	Example
	Note
	Recommendation
	Syntax

## Contents

<b>Users and Roles (BC-CCM-USR)</b> .....	<b>6</b>
Changes for Release 4.6.....	6
Creating and Maintaining User Master Records.....	10
Maintaining Logon Data .....	12
Assign Roles.....	15
Assigning Profiles.....	15
Assign User Groups.....	16
Personalization.....	17
User Maintenance Functions.....	17
Mass Changes.....	20
Logon and Password Security in the SAP System .....	21
Setting Password Controls.....	23
Limiting Logon Attempts and Setting up Clients.....	24
Logging Off Inactive Users.....	24
Maintaining User Defaults and Options.....	25
Comparing User Master Records.....	27
The Effect of Changes on User Master Records.....	28
Create and Maintain Internet Users.....	28
Assign Standard Roles.....	30
Role Maintenance .....	36
Change and Assign Roles.....	37
<b>Create Roles</b> .....	<b>38</b>
Editing Predefined Authorizations .....	44
SAP Authorization Concept Modules .....	47
Authorization Check Scenario.....	52
Symbols and Status Text in Authorization Maintenance.....	53
Copying Authorizations From Templates.....	55
Generating Authorization Profiles .....	56
Regenerate the Authorization Profile Following Changes .....	57
Mass Generation of Profiles .....	59
Assign Users .....	60
Personalization .....	62
<b>Create Composite Roles</b> .....	<b>62</b>
<b>Derive Roles</b> .....	<b>63</b>
<b>Compare Roles</b> .....	<b>64</b>
<b>Transport/Distribute Roles</b> .....	<b>66</b>
Upload/Download Roles .....	67
<b>Role Maintenance: Example</b> .....	<b>67</b>
<b>Role Maintenance: Tips and Tricks</b> .....	<b>73</b>
<b>Using the Infosystem</b> .....	<b>74</b>
<b>Reducing the Scope of Authorization Checks</b> .....	<b>75</b>
<b>Preparatory Steps</b> .....	<b>76</b>

<b>Globally Deactivating Authorization Checks</b> .....	<b>77</b>
<b>Reducing Authorization Checks in Transactions</b> .....	<b>77</b>
<b>Editing Templates for General Authorizations</b> .....	<b>79</b>
<b>Comparing Check Indicators/Field Values After Upgrade</b> .....	<b>80</b>
<b>Transporting Authorization Components</b> .....	<b>80</b>
<b>Analyzing Authorization Checks</b> .....	<b>83</b>
<b>Analyzing Authorizations using the System Trace</b> .....	<b>83</b>
<b>Authorization Checks in Your Own Developments</b> .....	<b>84</b>
<b>Creating Authorization Fields</b> .....	<b>85</b>
<b>Assigning an Authorization Object to an Object Class</b> .....	<b>85</b>
<b>Creating/Maintaining Authorizations/Profiles Manually</b> .....	<b>86</b>
<b>Line-oriented Authorizations</b> .....	<b>86</b>
<b>Administration Tasks</b> .....	<b>87</b>
<b>Maintaining Authorization Profiles</b> .....	<b>87</b>
Simple and Composite Profiles .....	88
Defining Profiles and Authorizations .....	88
Alternative Authorizations .....	89
Choosing Authorization Objects .....	89
Maintaining Composite Profiles .....	90
Activate profiles .....	90
Naming Convention for Predefined Profiles .....	90
<b>Maintaining Authorizations</b> .....	<b>91</b>
Creating and Maintaining Authorizations .....	91
Entering Values .....	91
Activating Authorizations .....	93
Naming Convention for SAP Authorizations .....	93
<b>Central User Administration</b> .....	<b>94</b>
<b>Setting Up Central User Administration</b> .....	<b>94</b>
Setting-up CUA for Systems with different Releases .....	98
<b>Setup field distribution parameters</b> .....	<b>100</b>
<b>Migration of Existing Users into the Central System</b> .....	<b>102</b>
<b>Central User Distribution</b> .....	<b>103</b>
<b>Distribution Logs</b> .....	<b>104</b>
<b>Global User Manager</b> .....	<b>105</b>
<b>Preparatory Steps</b> .....	<b>109</b>
<b>Global User Manager authorizations</b> .....	<b>111</b>
<b>Global User Manager Functions</b> .....	<b>111</b>
<b>First Installation Procedure</b> .....	<b>113</b>
<b>Organizing User and Authorization Maintenance</b> .....	<b>115</b>
Managing users and roles .....	116
Distributed Administration.....	116
Setting up Administrators.....	117
<b>Protecting Special Users</b> .....	<b>118</b>
Securing User SAP* Against Misuse.....	119
Protecting User DDIC Against Unauthorized Access.....	120
<b>Security in System Groups</b> .....	<b>121</b>
<b>Upgrade Procedure</b> .....	<b>123</b>

## Users and Roles (BC-CCM-USR)

### Purpose

Users must be setup and roles assigned to user master records before you can use the SAP System.

A user can only log on to the system if he or she has a user master record with a password. A user menu and authorizations are also assigned to the user master record via one or more roles.

Roles are collections of activities which allow a user to use one or more business scenarios of an organization. The transactions, reports and web-based applications in the roles are accessed via user menus. User menus should only contain the typical functions in the daily work of a particular user.

The integrity of business data is also ensured by the assignment of roles. Authorization profiles are generated which restrict the activities of users in the SAP System, depending on the activities in the roles.

### Integration

The mySAP.com Workplace offers users a role-based portal to perform his or her tasks via a web browser. This is documented in SAPNet under the alias *Workplace*. The following notes refer to the R/3 user administration and role maintenance.

Data is also protected in the SAP System by the following mechanisms as well as the assignment of authorizations described in the following sections:

- Secure Network Communication (SNC)
- Secure data formats (Secure Store and Forward (SSF))
- Internet security
- System passwords
- Database access
- Transport system
- Individual directory structures for the SAP System and so on

See the *R/3 Security Guide*. It is in SAPNet under <http://sapnet.sap.com/securityguide>.

## Changes for Release 4.6

The following areas were extended:

- Role Maintenance
  - Flexible user menus
  - Composite roles
  - Distribution of roles
  - Read roles from other systems

- Link a role to Knowledge Warehouse documentation
- Comparison of roles
- User administration
  - Central User Administration
    - Global User Manager
    - Simplified ALE system environment setup for central user administration
  - User groups
  - Mass changes in user administration
  - Alias names for users
  - Reference user



The term *Activity group* has been replaced by *Role* in Release 4.6C.

## Role Maintenance

The current Release contains more than 1200 single roles from all application areas. You can use the roles as they are delivered by SAP or you can copy and change them and assign them to users.

The delivered roles include:

- Basis: Authorization data administrator
- Basis: Authorization profile administrator
- Basis: User administrator
- Basis: System administrator
- Basis: Batch administrator
- Basis: Database administrator
- Basis: Customizing project member
- Basis: ABAP developer
- Basis: Uncritical basis authorizations for all users

See [Assign standard roles \[Page 30\]](#).

## Flexible user menus

In role maintenance (transaction PFCG), the administrator can construct the user menu for a role by adding transactions, reports, and Internet/intranet links to the menu. The structure and terminology for the functions contained can be specified as needed.

You can specify transactions to add to the user menus or choose transactions from the SAP menu. The company menu is no longer available as of Release 4.6A.

Along with the user menus, you can display a complete view of all functions delivered by SAP using the SAP menu. This complete view is only displayed if no user menus have been defined.

See [Create roles \[Page 38\]](#).

---

## Changes for Release 4.6

### Composite roles

It is often necessary to define a work center using more than just a role and the menu structure, authorization data and user assignment information it contains. To simplify maintenance and improve the reusability of the information, a work center can also be modularized into several roles and then combined into one composite role.

Users assigned to a composite role are automatically assigned to the roles included in the composite activity group.

You can edit the complete menu structure that is the sum of the individual roles included in the composite role.

See [Composite roles \[Page 62\]](#).

### Distribution of Roles in Target System

You can distribute roles into target systems from Release 4.6C provided that the target system also has Release 4.6C.

See [Create roles \[Page 38\]](#).

### Read roles from other systems

You can copy component system roles to the work center server by RFC. You can also read roles from earlier releases (down to Release 3.1H) into the work center, if you have the appropriate plug-in.

### Link a role to Knowledge Warehouse documentation

You can link a role to a document in the Knowledge Warehouse with *Utilities* → *Info object* → Assign in the role maintenance Change roles screen.

### Comparison of roles

You can compare and adjust role menus across systems from Release 4.6C with the transaction ROLE\_CMP.

See [Compare roles \[Page 64\]](#).

### New authorization functionality: Mass generation of derived roles

You can derive roles from existing roles in the role maintenance. The role menu is copied into the derived roles. You can perform a mass generation of the derived roles in the authorization maintenance of the original role to copy the authorization data as well.

The organization level data is only copied the first time the authorization data is adjusted for the derived role. If organization level data is maintained in the derived role, it is not overwritten by subsequent adjustments.

See [Derive roles \[Page 63\]](#).

## User administration

### Central User Administration

An SAP system group consists of several R/3 Systems with several clients. The same users are frequently created and assigned to roles in each client. The central user administration performs these tasks in a central system and distributes the data to the systems in the system group.



## Global User Manager

From Release 4.6A the system administrator can get an overview of the users, existing user groups, the systems in the system group and the roles, in the Global User Manager, based on the central user administration. The system administrator can make changes in the overview using drag and drop. These changes take effect after being distributed to the dependent systems.

Previously, user data had to be maintained in every client in every system. With the introduction of central user administration, this can all be maintained in a central system. User groups can be used to reduce the administration overhead required for maintaining user data, as authorization data then only has to be maintained once for each user group.

See [Global User Manager \[Page 105\]](#).

## Simplified ALE system environment setup

From Release 4.6C, simple system landscapes can be setup with transaction SCUA.

See [Setting up Central User Administration \[Page 94\]](#).

## Cross-system role assignment in workplace

If the Workplace server is the origin for the central user administration, the single roles and their profiles are automatically assigned to the component system user when you assign a composite role to a user. The composite role menu is called on the Workplace Server. Authorization checks are made in the component systems.

## User groups

Previously, user groups were used to distribute user administration among several administrators. As of Release 4.6A, the *User group* category can be used to improve the distribution of users thus increasing the speed of user administration.

See [User groups \[Page 16\]](#).

## Mass changes in user administration

Most changes which can be made for one user in the user management can also be made for a set of users.

Logon data, constants, parameters, roles and profiles can be changed for a set of users.

You select users in the user administration Infosystem. Users can be selected, for example, according to address data or authorization data.

See [Mass changes \[Page 20\]](#).

## Alias names for users

You can assign an alias to a user when you create it. This gives you 40 characters for user names which can be longer and more meaningful. The user can be identified by either the (12-character) user name or the (40-character) alias. The alias also identifies a dialog user in the internet.

See [Create and maintain internet user \[Page 28\]](#).

---

## Creating and Maintaining User Master Records

### Reference user

A reference user can be assigned to each user when assigning roles. Reference users are an authorization enhancement. They are used to give internet users identical authorizations.

See [Create and maintain internet user \[Page 28\]](#).

## Creating and Maintaining User Master Records

### Use

The existence of a user master record is a prerequisite for logging on to the SAP System. The user master record determines which role is assigned to the user, i.e. which activities are in the user menu and which authorizations the user has.

### Integration

User master records are client-specific. You therefore need to maintain individual user master records for each client in your SAP System. If you use the Central User Administration, you should create and maintain the users in the central system. See [Central User Administration \[Page 94\]](#).

### Prerequisites

You need authorizations to create or maintain user master records:

- Authorization to create and/or maintain user master records and to assign a user group (object S\_USER\_GRP).
- Authorization for the authorization profiles you want to assign to users (object S\_USER\_PRO).
- Authorization to create and maintain authorizations (object S\_USER\_AUTH).
- Authorization to protect roles. You can use this authorization object to determine which roles may be processed and which activities (*Create, Display, Change* and so on) are available for the role(s) (object S\_USER\_AGR).
- Authorization for transactions that you may assign to the role and for which you can assign authorization at the start of the transaction in the Profile Generator (object S\_USER\_TCD).
- Authorization to restrict the values which a system administrator can insert or change in a role in the Profile generator (S\_USER\_VAL)

See [Organizing User and Authorization Maintenance \[Page 115\]](#).

### Features

Functions for maintaining user master records are in the menu path: *Tools* → *Administration* → *User Maintenance* → *User*.

The system administrator can use the [User maintenance functions \[Page 17\]](#).

The system administrator or the user can [Maintain user values and options \[Page 25\]](#).



See:

[Compare user master records \[Page 27\]](#)

[The Effect of User Master Record changes \[Page 28\]](#)

## Activities

To create and maintain user master records:

1. Choose *Tools* → *Administration* → *User maintenance* → *Users*. You go to the *User maintenance: Initial screen*.
2. Enter an existing user name and choose  or enter a new user name and choose .

You can assign an alias to a user when you create it. This gives you 40 characters for user names which can be longer and more meaningful. The user can be identified by either the (12-character) user name or the (40-character) alias.



To create a user with aliases, enter them in the *Logon data* tab.

The alias is also used for internet transactions. When users logon in the internet via the [Internet Transaction Server \[Ext.\]](#), they use the source system user name. The alias and password must be entered for identification in internet transactions (e.g. for ordering articles). If the user has forgotten his or her alias, he or she can create a new account. A new user and alias are created in the SAP System. The 12-character user name is generated using a specified algorithm.

The *Alias* field in the initial user maintenance screen is mainly for finding internet users whose internal technical user name is not known.

3. Enter user personnel data in the *Address* tab. The *Last name* field must be filled.

There is a set of tabs for user data categories: *Address*, *Logon data*, *Constants*, *Parameters*, *Roles*, *Profiles*, *Groups* and *Personalization*.



If you are using the SNC interface or central user administration, the system displays the additional corresponding tab.

The *Constants* and *Parameters* tabs contain optional fields.

Users can change this data and their address information by choosing *System* → *User profile* → *Own data* (see [Maintaining User Defaults and Options \[Page 25\]](#)).

The tabs *Address*, *Logon data*, *Roles* and *Profiles* contain fields that you must fill in.

The application toolbar contains the following pushbuttons:

<i>Measurement data</i>	You can enter measurement data. See the SAP <i>System Measurement Guide - Individual Installation</i> brochure. This describes the measurement program enabling you to determine the total number of R/3 users and HR master records that have been set up.
-------------------------	---

---

**Maintaining Logon Data**

<i>References</i>	<p>You can assign business object types to a user in a table. An object type is a description of data (objects) used in the system, created at definition time in the <a href="#">Business Object Builder [Ext.]</a>. Object types include:</p> <ul style="list-style-type: none"><li>• Documents (invoices, purchase requisition, applications, etc.)</li><li>• Master data (customer, material, vendor, etc.)</li><li>• Transaction data (order, quotation, etc.)</li></ul> <p>An object is any kind of set of information which can be addressed uniquely with an identifying key.</p> <p>The possible entries help for the <i>Object type</i> field lists all object types.</p>
-------------------	---

See also:

[Maintaining Logon Data \[Page 12\]](#)

[Assigning roles \[Page 15\]](#)

[Assigning Profiles \[Page 15\]](#)

[Assigning user groups \[Page 16\]](#)

[Personalization \[Page 17\]](#)

## Maintaining Logon Data

In the *Logon data* tab you must enter an initial password for the new user in the *Initial password* field. All other entries on this screen are optional.

Further information is available by choosing F1.

You can maintain the following fields:

Maintaining Logon Data

<p>Initial password</p>	<p>You are required to enter the password twice to eliminate the possibility of typing errors.</p> <p>Passwords:</p> <ul style="list-style-type: none"> <li>- are not case-sensitive (the R/3 System does not differentiate between upper- and lowercase letters)</li> <li>- must be at least three characters long. have a maximum length of eight characters</li> <li>- may contain any characters which can be input from the keyboard. This includes digits, spaces and punctuation marks</li> <li>- cannot begin with a question mark or exclamation mark</li> <li>- may not contain spaces within the minimum length. This is normally the first three characters</li> <li>- may not begin with three identical characters</li> <li>- may not be PASS or SAP*</li> <li>- may not be used if its use has been forbidden</li> <li>- may not start with a sequence of three characters which appears in the user name</li> </ul> <p>When the user logs on for the first time, he or she must enter a new password. When a user changes his or her password, the new password must be different to each of that user's last five passwords.</p> <p>See <a href="#">Logon and password protection in the SAP System [Page 21]</a>.</p>
<p>User group</p>	<p>Enter the name of the user group to which this user is to belong.</p> <p>If you want to distribute the user maintenance tasks amongst several user administrators, you must assign the user to a group. Only the administrator with authorization for that group may then change the master record.</p> <p>A user master record which is not assigned to a group can be changed by any user administrator.</p>

## Maintaining Logon Data

user type	<p>The system proposes <i>Dialog</i> for normal dialog users. The following user types exist:</p> <p><b>Dialog user:</b> individual, interational system access</p> <ul style="list-style-type: none"> <li>• obsolete/initial password check</li> <li>• passwords can be changed</li> <li>• repeat dialog logon check</li> </ul> <p>use: individual (internet) user</p> <p><b>Service user:</b> anonymous, interational user, repeated system access</p> <ul style="list-style-type: none"> <li>• no obsolete/initial password check</li> <li>• only the user administrator can change passwords</li> <li>• multiple logon allowed</li> </ul> <p>use: anonymous system access (e.g. ITS scenarios: product catalog display)</p> <p><b>System user:</b> system-dependent and system-internal procedures, not interaction-capable</p> <ul style="list-style-type: none"> <li>• no obsolete/initial password check</li> <li>• only the user administrator can change passwords</li> <li>• multiple logon allowed</li> </ul> <p>use: background processing, ALE, Workflow, TMS, etc.</p> <p><b>Reference user:</b> authorization enhancement</p> <ul style="list-style-type: none"> <li>• logon not possible</li> <li>• authorization enhancement tool</li> </ul> <p>use: internet users with identical authorizations</p> <p>You can specify a reference user for additional authorizations for each user in the <i>Roles</i> tab.</p> <p>The application controls the assignment of reference users. The reference user name can be assigned in variables. Variables begin with "\$". Variables are assigned to reference users in the transaction SU_REFUSERVARIABLE.</p>
Valid from... Valid to...	These optional fields allow you to specify a start and end date for the user master record. Leave them blank if you do not want to set a limit.

## Assign Roles

Account Number	<p>For each user or user group, assign an account name or number of your choice. The user appears in the RZ accounting system (ACCOUNTING EXIT) under this number.</p> <p>A recommended account number would be the user's cost center or company code, for example.</p> <p>You should always enter an account name or number in the SAP accounting system. The user will otherwise be assigned to a general category without account number.</p>
----------------	---

## Assign Roles

In the *Roles* tab the possible entries help displays a list of the existing roles from which you can select one. You can assign a role to as many users as you like.

You can create a link with the user master record for a specified validity period by clicking on the relevant field in the *Valid from* or *Valid to* column and then using the calendar to choose a new date.

You can delete a line by selecting it and then choosing *Delete*.

Note that you can use the separator to move the column separators so that you can read texts that are not completely visible.

## Assigning Profiles

You assign authorization profiles to a user in the *Profiles* tab.

You can assign a large number of authorization profiles to a user (about 150).

Profiles give users authorizations.

You should maintain your profiles in the role maintenance transaction PFCG unless you have to edit profiles that were created manually.

You can manually maintain profiles by choosing *Tools* ® *Administration* ® *Manual maintenance* ® *Edit profiles manually* (see [Creating and Maintaining Authorizations and Profiles Manually \[Page 86\]](#)). You can also enter composite profiles (a combination of several profiles) in the user master records when manually maintaining profiles.

If you choose automatic maintenance, the Profile Generator generates an authorization profile on the basis of an role.

You can go to role maintenance and profile generation from the user maintenance with *Environment* → *Maintain roles*. See [Role maintenance \[Page 36\]](#).

You assign roles to a user in the *Roles* tab. This simultaneously assigns the associated authorization profiles to the user. See [Assigning roles \[Page 15\]](#) and [Comparing profiles with roles in the user master record](#).

## Assign User Groups



Never insert profiles generated in the role maintenance directly into the user master record. The profiles are automatically transferred to your user master record after a user comparison in the Profile Generator.

The SAP System contains predefined profiles:

- SAP\_ALL: assign the profile SAP\_ALL to users who are to have all R/3 authorizations including superuser authorization.
- SAP\_NEW: assign this profile to users who are to have access to all not yet protected components.

The SAP\_NEW profile grants unrestricted access to all existing functions for which additional authorization checks have been introduced. Users can therefore continue to work uninterrupted with functions which are subject to new authorization checks. This ensures upward compatibility.

For this reason you should assign SAP\_NEW to all user master records. You can then decide which users are to have which authorizations and delete the SAP\_NEW profile.



If you have skipped releases or upgrades, when you execute this operation you need to take into account all authorizations which have come into the system in the meantime. SAP\_NEW is a composite profile which contains a simple profile S\_NEW\_<Release> with new authorizations for functional Releases.

- You must add the new authorizations to manually generated profiles
- Following a Release or upgrade you need to regenerate all authorization profiles which have been generated using the Profile Generator. Choose *Environment* → *Installation/Upgrade* in the role maintenance (transaction SU25).

## Assign User Groups

User groups have been used to distribute user maintenance between administrators, but users can now be assigned to one or more user groups. The category *User group* can now be the basis for better assignment of user data and speed up central user administration.

You can go to the user group maintenance from the user maintenance via *Environment* → *User groups*. You can display, create, change and delete user groups.

When you create or change a user, you can assign it to one or more groups in the last tab *Groups*.

See [Global User Manager \[Page 105\]](#) for further information about using user groups.



## Personalization

### Use


You can set certain system person or role defaults in this tab. Tasks in a role can have person or role default values.

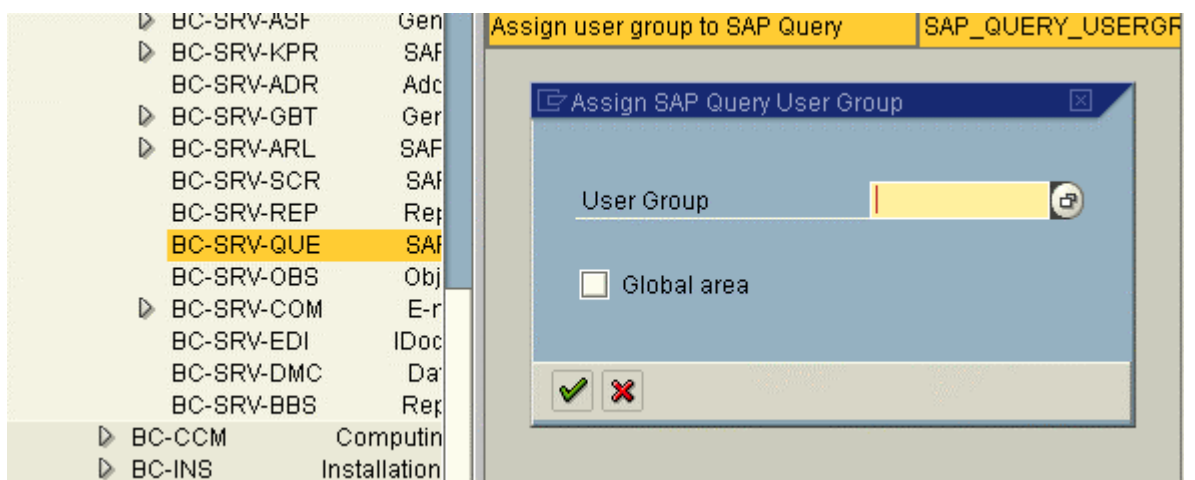
### Integration

You can call the *Personalization* tab in the role or user maintenance.

### Activities

To assign personalization data to the user or role:



1. Choose the *Personalization* tab.
2. Choose  to display the application components on the left-hand side of the screen.
3. Choose a component whose personalization data is to be maintained. The personalization objects for the component are output on the right-hand side.






4. Double-click on a personalization object. A default value entry dialog box appears.

## User Maintenance Functions

User maintenance (*Tools* → *Administration* → *User maintenance* → *Users*) includes the following functions:

Function:	Description:
 - Create	Enter a user name and choose <i>Create</i> . See <a href="#">Create and maintain user master records [Page 10]</a> .
 - Change	Enter an existing user name and choose <i>Change</i> . See <a href="#">Create and maintain user master records [Page 10]</a> .

## User Maintenance Functions

 - <i>Display</i>	Enter a user name and choose <i>Display</i> . The maintenance description contains information about the contents of the tab displayed.
 - <i>Copy</i>	Choose <i>Copy</i> . Enter the name of a reference user and the new user name. You can specify whether you want to copy only some of the user data or all of it. On the following screen you can edit the new user master record as required.  You can also rename user master records if you simply want to replace one record with an identical one of a different name.
 - <i>Lock/Unlock</i>	Enter an existing user name and choose <i>Lock/Unlock</i> to grant or deny a user access to a system. Locking or unlocking a user master record takes effect the next time a user attempts to log on. Users who are logged on at the time that changes are made are not affected.  The system automatically locks users if twelve successive unsuccessful attempts are made to log on. The lock is recorded in the system log, along with the terminal ID of the machine where the logon attempt took place.  You can set the number of permissible unsuccessful logon attempts in a system profile parameter. See <a href="#">Limiting Logon Attempts and Predefining Clients [Page 24]</a> for further details.  This automatic lock is released by the system at midnight. You can also remove the lock manually before this time. Locks that you specifically set yourself apply indefinitely until you release them.
Change password	Enter the user name and choose <i>Change password</i> .  This new password must fulfill the standard conditions regarding permissible passwords. See <a href="#">Maintain logon data [Page 12]</a> or choose F1.  The new password is effective immediately. If users forget their password, they can use the new one as soon as it has been set.  Users may change their passwords no more than once a day. System administrators, on the other hand, may change user passwords as often as necessary.
<i>Edit</i> → <i>Address</i>	Choose a component (telephone number, fax number, and so on) and make changes as needed.
<i>Environment</i> → <i>Mass changes</i>	Most changes which can be made for one user in the user management can also be made for a set of users. See <a href="#">Mass changes [Page 20]</a> .

User Maintenance Functions

<p><i>Environment</i> → <i>Archive and read</i></p>	<p><b>Displaying Change Documents</b></p> <p>Choose <i>Info</i> → <i>Infosystem</i> and <i>Change documents</i> in the overview displayed to call a list of changes to user master records, authorization profiles and authorizations. The system logs the following changes:</p> <ul style="list-style-type: none"> <li>• Direct authorization changes for a user (that is, changes to the profile list in the user master record). <ul style="list-style-type: none"> <li>Indirect changes are changes to profiles and authorizations contained in the user master record. These changes cannot be seen in the display. You can, however, see them in the change documents for profiles and authorizations.</li> </ul> </li> <li>• Changes to user passwords, user type, user group, validity period and account number</li> </ul> <p>For each change made, the log shows the deleted value in the <i>Deleted entries</i> line. The changed or new value is displayed in the <i>Added entries</i> line.</p> <p><b>Archiving Change Documents</b></p> <p>User master records and authorizations are stored in the USR* tables. You can reduce the amount of space that these take up in the database by using the archiving function. Change documents are stored in USH* tables. The archiving function deletes change documents that are no longer required from the USR* tables.</p> <p>You can archive the following change documents relating to user master records and authorizations from the USH* tables:</p> <ul style="list-style-type: none"> <li>• Changes to authorizations (archiving object US_AUTH)</li> <li>• Changes to authorization profiles (archiving object US_PROF)</li> <li>• Changes to the authorizations assigned to a user (archiving object US_USER)</li> <li>• Changes to a user's password or to defaults stored in the user master record (archiving object US_PASS)</li> </ul> <p>The functions for maintaining users and authorizations provide access to the archiving system. In the user maintenance initial screen, choose <i>Environment</i> ® <i>Archive and read</i>. In profile and authorization maintenance, choose <i>Utilities</i> → <i>Archive and read</i>. You then have two options, either <i>Archive auth. docs</i> or <i>Read auth. docs</i>. These options refer to whether you want to archive or read change documents pertaining to users, profiles or authorizations.</p> <p>See <a href="#">Archiving user and authorization changes [Ext.]</a>.</p>
<p><i>Environment</i> → <i>User groups</i></p>	<p>Users can be assigned to one or more user groups. See <a href="#">User groups [Page 16]</a>.</p>

**Mass Changes**

<i>Environment</i> → <i>Organizational assignment.</i>	Location of user in HR-ORG.
<i>Environment</i> → <i>Maintain company address</i>	You can maintain the company address using an additional transaction and assign it in user maintenance using the appropriate pushbuttons.

## Mass Changes

Most changes which can be made for one user in the user management can also be made for a set of users.

Logon data, constants, parameters, roles and profiles can be changed for a set of users.





You can make changes to a set of users with *Environment* → *Mass changes* (transaction SU10) in the user maintenance.

If you use the Central User Administration, i.e. you make the mass changes from the central system, profiles and roles are displayed system-dependently. See [Distributing users \[Page 103\]](#).




The mass user data change functions apply to the users displayed in the initial screen unless you make a selection.



You must choose *Change* in the *Address*, *Logon data* and *Constants* tabs for each change. This ensures that your change, e.g. deleting the contents of a field, is made for all fields.

Select users	You select users in the user administration Infosystem. 1. Select either by <i>Address</i> or by <i>Authorization data</i> . 2. Select some or all users and choose <i>Copy</i> .
Create users	1. Enter names in the <i>User</i> column. 2. Choose  . Maintain the user data as in the user maintenance (SU01). See <a href="#">Create and maintain user master records [Ext.]</a> .  You cannot assign individual passwords because you create several users at the same time. They are generated automatically and displayed in the mass changes log.
Change users	1. Choose  . 2. Change the user data. You can decide whether parameters, roles, profiles and groups are added to or removed from the user master records.
Delete users	Choose  .

**Logon and Password Security in the SAP System**

Lock/unlock users	Choose  or  .   The users are only locked or unlocked if it is allowed in the current system. If the system is in the Central User Administration, only the central system may be able to lock and unlock. See <a href="#">Defining Fields to be Transferred [Page 100]</a> .
-------------------	---

**Mass changes log**

After each mass change you are asked in a dialog box whether you want a log. The log shows who made which changes in which system at what time.

The log contains several message levels which you can expand with a pushbutton. If a message has a long text, you can display it with a pushbutton next to the message.

You can make certain settings for the log display under *Settings* and the *Color legend* explains the colors used in the display.

You can print the log or save it in a PC file.

**Logon and Password Security in the SAP System**

This section provides a general overview of logon and password security in the SAP System.

**The Initial Password**

When you create a user, you are required to enter a password for the user. The password must meet all of the internal requirements set by the SAP System as well as any Customizing changes that you have made. For more information, see [Setting Password Controls \[Page 23\]](#).

When a new user logs on for the first time, he or she must specify a new password before proceeding.

**Password Requirements**

The following table shows password requirements and whether they are fixed by the system or whether you can customize them.

Password Requirement	Type
Minimum length: 3 characters	Can be defined by the customer. Minimum length can be increased
Expiration	Can be defined by the customer. Number of days after which a password must be changed can be set. Rule: password must not be changed
Password may not be set to a value that is contained in a "lock-out list"	Can be defined by the customer. Rule: only the passwords PASS and SAP* are excluded from the application.
First character may not be ! or ?	Fixed in SAP System

**Logon and Password Security in the SAP System**

First three characters may not appear in the same sequence in the user ID	Fixed in SAP System
First three characters may not be identical	Fixed in SAP System
Space character not allowed within first three characters	Fixed in SAP System
Password may not be PASS or SAP*	Fixed in SAP System
Any character which may be typed on the keyboard is allowed in a password. Password is not case-sensitive. No distinction is made between upper and lowercase letters	Fixed in SAP System
A user can change his or her password no more than once a day. Restriction does not apply to user administrators	Fixed in SAP System
Password may not be changed to any of a user's last five passwords	Fixed in SAP System

For help in setting the customizable password requirements, see [Define password rules](#)

## Logging On

To access the R/3 System and its data, a user must log on to the system. A user must enter both user ID and password; it is not possible to have an empty password.

Before the user is admitted to the system, the system checks whether either of two conditions applies:

- The user has been locked.  
If this is the case, the user is not permitted to log on. As user administrator, you can lock a user to prevent logons. You can find further details in [Locking and Unlocking User Master Records \[Ext.\]](#).
- The user's current password is not longer valid. If so, the user must enter a new password before proceeding.  
You can specify how long passwords remain valid in the system profile. By default, there is no limit on the validity of passwords.

A user cannot change a password more than once a day. The system requires both the user's current password and two matching entries of the new password.

If the user ID and password are correct, then the system displays the date and time of the user's last logon. With the date and time, the user can check that no suspicious logon activity has occurred, such as a logon in the middle of the night. The logon date and time cannot be changed in a standard production R/3 System. The system does not record the logoff date and time.

## Logon Errors

If a user has not entered a valid user ID, the system allows the logon attempt to continue until the user enters a valid user ID. User IDs, and passwords as well, are not case-sensitive. A user can enter his or her user ID in lowercase, uppercase, or a combination of both.

## Setting Password Controls

If a user enters an incorrect password, then the system allows the user two retries before terminating the logon attempt. Should the user continue to enter an incorrect password in subsequent logon attempts, then the system automatically locks the user against further logon attempts. The default maximum number of consecutive incorrect password entries is set to 12. For more information, see [Setting Password Controls \[Page 23\]](#).

A user that was locked because of too many incorrect passwords is automatically unlocked at midnight of the day the lock was set. A user administrator can unlock the user at any time.

## Setting Password Controls

You can set controls on user passwords in two ways:

- With system profile parameters, you can specify a minimum length for passwords. You can also specify how frequently users must choose new passwords.
- With a reserved-password table, you can specify passwords that users may not choose. Generic specifications are possible.

### Setting Password Length and Validity

Use the following system profile parameters to specify the minimum length of a password and the frequency with which users must change their password.

- *login/min\_password\_lng*: minimum password length.  
Default value: Three characters. You can set it to any value between 3 and 8.
- *login/password\_expiration\_time*: number of days after which a password expires  
To allow users to keep their passwords without limit, leave the value set to the default 0.

### Specifying Impermissible Passwords

You can prevent users from choosing passwords that you do not want to allow. To prohibit the use of a password, enter it in table USR40. You can maintain table USR40 with Transaction SM30.

In USR40, you can specify impermissible passwords generically if you want. There are two wildcard characters:

- ? stands for a single character
- \* stands for a sequence of any combination characters of any length.



**123\*** in table USR40 prohibits any password that begins with the sequence "123."

**\*123\*** prohibits any password that contains the sequence "123."

**AB?** prohibits all passwords that begin with "AB" and have one additional character: "ABA", "ABB", "ABC" and so on.

---

**Limiting Logon Attempts and Setting up Clients**

## Limiting Logon Attempts and Setting up Clients

You can use the following system profile parameters to limit the permitted number of failed logon attempts and to set the default client.

- *login/fails\_to\_session\_end*: This parameter specifies the number of times that a user can enter an incorrect password before the system ends the logon attempt.  
Default value 3. You can set it to any value between 1 and 99 inclusive.
- *login/fails\_to\_user\_lock*: This parameter specifies the number of times that a user can enter an incorrect password before the system locks the user against further logon attempts.  
Default value 12. You can set it to any value between 1 and 99 inclusive.
- *login/system\_client*: Specifies the default client. This client is automatically entered in the system logon screen. Users can type in a different client.

Maintain the system profile parameters under *Tools* → *CCMS* → *Configuration* → *Profile maintenance*.

To make the parameters globally effective in an SAP System, set them in the default system profile DEFAULT.PFL. However, to make them instance-specific, you must set them in the profiles of each application server in your SAP System.

## Logging Off Inactive Users

You can set up your SAP System to automatically log off inactive users after a specified period of time. This improves system security by assuring that SAP sessions at unattended terminals do not stay active indefinitely.

By default, automatic logoff is not activated in the SAP System. Users remain logged on no matter how long they may be inactive. You activate automatic logoff by setting the system profile parameter *rdisp/gui\_auto\_logout* to the number of seconds of inactivity you want to permit. Enter as a value for this parameter the number of seconds of inactivity that must elapse before a user is automatically logged off.

Once you have activated this function, inactive users are logged off once the idle-time limit has been exceeded. The system does not save data before logging off the user. Unsaved data will be lost. The system also does not display a logoff confirmation prompt.

## Procedure

To activate automatic logoff, proceed as follows:

1. Call the system profile maintenance functions with *Administration* → *CCMS* → *Configuration* → *Profile maintenance* (transaction RZ10).
2. Define or maintain parameter *rdisp/gui\_auto\_logout*. Enter as a value for this parameter the number of seconds of inactivity that must elapse before a user is automatically logged off.



---

## Maintaining User Defaults and Options

To activate automatic logoff throughout the system, set the parameter in the default profile (DEFAULT.PFL) . However, if you want to activate automatic logoff only for a specific SAP application, set the parameter in the profile for that particular instance.



Remember that many users are not "active" for extended periods of time. Such users may include:

- Programmers or other users of SAP editors, who regularly work for long periods of time only using the frontend software.
- Users who only occasionally enter data but who should not be logged off.  
Example: Production employees who only enter data in the SAP System when, for example, materials are delivered.

You should either set a high value for parameter *rdisp/gui\_auto\_logout*, or deactivate automatic logoff on the servers on which such users are active. This protects these users from loss of data or the inconvenience of having to log on again.

You can activate automatic logoff selectively by server by setting the parameter only in the profiles for the relevant instance. You can also define logon groups and thereby specify which users should not be automatically logged off. For more information about logon groups, see the R/3 Library *Computing Center Management System*.

To deactivate automatic logoff, delete the parameter from your profile(s) or set it to the value 0.

## Maintaining User Defaults and Options

Both system administrators and individual users can maintain user data.

The system administrator can maintain all data (see [Creating and Maintaining User Master Records \[Page 10\]](#)).

Users can maintain the following user data: *Constants*, *Addresses* and *Parameters*.

The following sections summarize the user options which you can define.

### Maintaining Own User Data

Users can maintain their own data by choosing *System @ User profile @ Own data*.

Choose F1 to display field help. F4 displays the input values that are available.

#### Defaults

You can set the following defaults:

- Start menu

You can specify the name of an area menu from the possible entries help in this field. The SAP Menu then only contains the components of this area menu.

---

## Maintaining User Defaults and Options



A user needs the credit management transactions for his or her daily work. If the start menu in his or her user data is FRMN, the SAP Menu only contains the credit management transactions.



The systemwide initial menu can be specified in the transaction SSM2.

- Logon language  
The default system language at logon. The user can however choose another language on the logon screen
- Printer
- Spool control
- Personal time zone (different from the company time zone in *Address*, crucial with RFC)
- Date format
- The format for decimals
- CATT check indicators

Information about these default values is available if you choose F1 .

## User Address

The user address data fields are self-explanatory.

Only the system administrator can maintain company addresses.

A time zone is assigned to each company address. User-specific time zones can overlap company time zones (see *Defaults* above).

## Parameters

User parameters supply defaults to R/3 fields. If a field is indicated, the system automatically fills in the default value. Depending on the field definition, the entry can also be replaced with a value entered by the user.

The two input fields on the parameter maintenance screen are described briefly below. Further information is available by choosing F1.

- *Parameter*: Enter the parameter ID for which you want to define a default value. You can display all of the parameter IDs defined in the system by choosing F4.
- *Value*: Enter the default value for the parameter.

## Comparing User Master Records

You can set a time limit on the assignment of roles to user master records. As a result some data will become invalid on a particular day, whilst other data becomes valid.



You cannot set time limits for authorization profiles and their entry in user master records.

To ensure that only authorization profiles which are valid are contained in the user master record each day, you must execute a daily profile comparison.

So that changes in the user master record are effective, you should execute the comparison before the user logs on.

There are two ways to execute the comparison.

1. As a background job before the start of each day.

If report **PFCG\_TIME\_DEPENDENCY** is run every night, the authorization profiles in the user master will be current each morning (assuming that the job has run correctly). The best procedure is to schedule this as a periodic background job.



Report **PFCG\_TIME\_DEPENDENCY** must also have run after each import of roles from other systems.

2. Using Transaction PFUD, *Compare User Master*

As an administrator, it is recommended that you use this transaction regularly to check that no errors have occurred in the background job. Any such errors can then be corrected manually.

To ensure that the authorization profiles in the user master records are always current, you should always execute a complete comparison of all roles (by choosing *Complete comparison*).

Following the comparison the system displays a log which includes any errors that occurred (background processing log for background report).

You have the following options in Transaction PFUD:

- *Schedule or check job for the full comparison*

Here you can start report **PFCG\_TIME\_DEPENDENCY** by specifying the time when the job is to start. The overview displays the status of jobs that have already been scheduled.

- *Manual profile selection*

Before comparing the user master record, you can select the profiles that are to be compared. The system displays an overview of the user master records to which profiles have been added, or from which profiles have been removed, during the comparison. If you deselect the relevant checkbox, you can exclude the profiles that should not be included in the user master record comparison. You start the comparison by choosing *User master comp.*

---

## The Effect of Changes on User Master Records

To compare the user master records belonging to selected users, first position the cursor on a user name and then choose *Select user*. You execute the comparison by choosing *User master comp*.



The status display for the user master comparison is only set to green once the comparison is executed.

- *Complete comparison*

With a complete comparison, all invalid authorization profiles are removed from the user master record and all new authorization profiles are inserted in the user master record.

The options *Add new profiles*, *Delete expired authorization profiles* and *Output error messages* are related to the actions described above.

You can also specify whether or not HR Organizational Management should be included in the comparison (*Reconcile with HR Organizational Management*).

## The Effect of Changes on User Master Records

Changes to user master records take effect when the user next logs on. If a user is logged on at the time when the system administrator implements the changes, these will only take effect when the user logs on to their next session.

You can also change a user's authorizations by changing and then reactivating profiles and authorizations within the user master record. Changes to reactivated authorizations have immediate effect. Changes to profiles, on the other hand, only take effect at the user's next logon.

## Create and Maintain Internet Users

### Use


Some internet application components (IAC) require an individual SAP user name and password, most do not. However even these IACs may require identification. A user can e.g. navigate anonymously in a product catalog; but must identify him or herself as a customer to place an order.

There are two procedures for creating an internet user, depending on which internet application component is used.

The following section describes how a normal SAP System dialog user can be active in the internet and the features which the SAP System user administration provides in this respect. It

then describes how you create and maintain internet users for the IACs which require an additional accounts for the internet.

### Create an (internet) user in user maintenance (SU01)

4. Choose *Tools* → *Administration* → *User maintenance* → *Users*. You go to the *User maintenance: Initial screen*.
5. Enter the user name and then choose .

You can assign an alias to a user when you create it. The user can be identified by either the (12-character) user name or the (40-character) alias.

When users logon in the internet via the ITS service, they use the source system user name. You can navigate in the internet with this user. If e.g. articles were ordered, the user must enter his or her alias and password for identification. The alias is used for identification in internet applications.

If the user has forgotten his or her alias, he or she can create a new account. A new user and alias are created in the SAP System. A 12-character user name is generated using a specified algorithm.

The *Alias* field in the initial user maintenance screen is mainly for finding internet users whose internal technical user name is not known.



To assign an alias to a user, enter it in the *Logon data* tab.

See [Create and maintain user master records \[Page 10\]](#) for the further procedure to create a user.

6. Assign a reference user to the user you want to use as internet user. Reference users extend authorizations and are used to give internet users identical authorizations. You can create one or more reference users, depending on the authorizations your staff are to have.



Reference users are assigned to a user master record in the *Roles* tab.

The authorizations of a reference user can be assigned to the user in the internet transaction program when the user is identified in the internet. The reference user can be assigned in a variable. The variable name should begin with "\$". Variables are assigned to reference users in the transaction SU\_REFUSER\_VARIABLE. Different variables can be assigned to a particular reference user for a group of users.



If no reference user is found for a variable in the transaction SU\_REFUSER\_VARIABLE, the variable is used as the user name.

### Create an Internet User with the *Maintain Internet User Function (SU05)*.

This transaction creates users and manages user data (e.g. passwords) in a table. Internet users are identified by:

- user name and
- user type

## Assign Standard Roles





The user type depends on the IACs which the user wants to run.

Internet user information is a client-specific user master record enhancement. When the internet user identifies him or herself to IACs later, these values are checked against the information in the table BAPIUSW01. Access is refused to unauthorized users.

1. Choose *Tools* → *Administration* → *User maintenance* → *Internet users*.

You go to the *Maintain internet users* screen.

2. Enter the user name and type. Choose one of the following functions:

 - <i>Create</i>	The system returns the initial password for the internet user. Note the password if you want to pass it on to the user. Otherwise choose <i>Change password</i> to give the user a new password.  Assign the created name and password to users.
 - <i>Change</i>	Enter a new user name or change the validity period.
 - <i>Delete</i>	Internet user is deleted after confirmation.
 - <i>Lock/Unlock</i>	A user is also locked after twelve failed attempts to logon.
<i>Change password</i>	Enter the new password twice.
<i>Initialize</i>	A new password is generated.

## Assign Standard Roles

### Use

The SAP standard contains more than 1200 predefined single roles from all application areas.

If you assign a predefined role to a user, he or she is automatically given the user menu required for his or her daily work and the authorizations required for it, when he or she logs on to the SAP System.

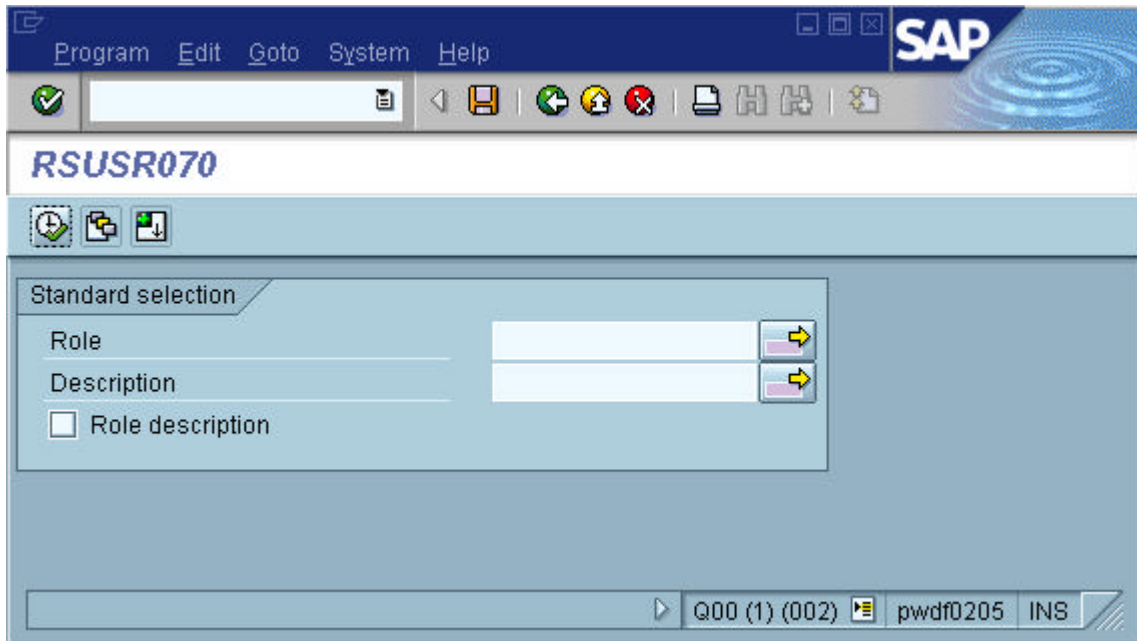
He or she can also define his or her personal Favorites from the functions assigned to him or her. The user calls transactions, programs or internet/intranet applications from the Favorites or the job structure tree.

Before you start to create your own roles for your staff, check whether the roles delivered by SAP can be used for the job descriptions in your company.

### Prerequisites

Get an overview of the roles delivered by SAP. The program RSUSR070 outputs descriptions of the existing example jobs. To run the program, choose *Tools* → *Administration* → *User maintenance* → *Infosystem* → *Roles* → *Roles by complex selection criteria* → *by role name*, or the transaction S\_BCE\_68001418.

## Assign Standard Roles



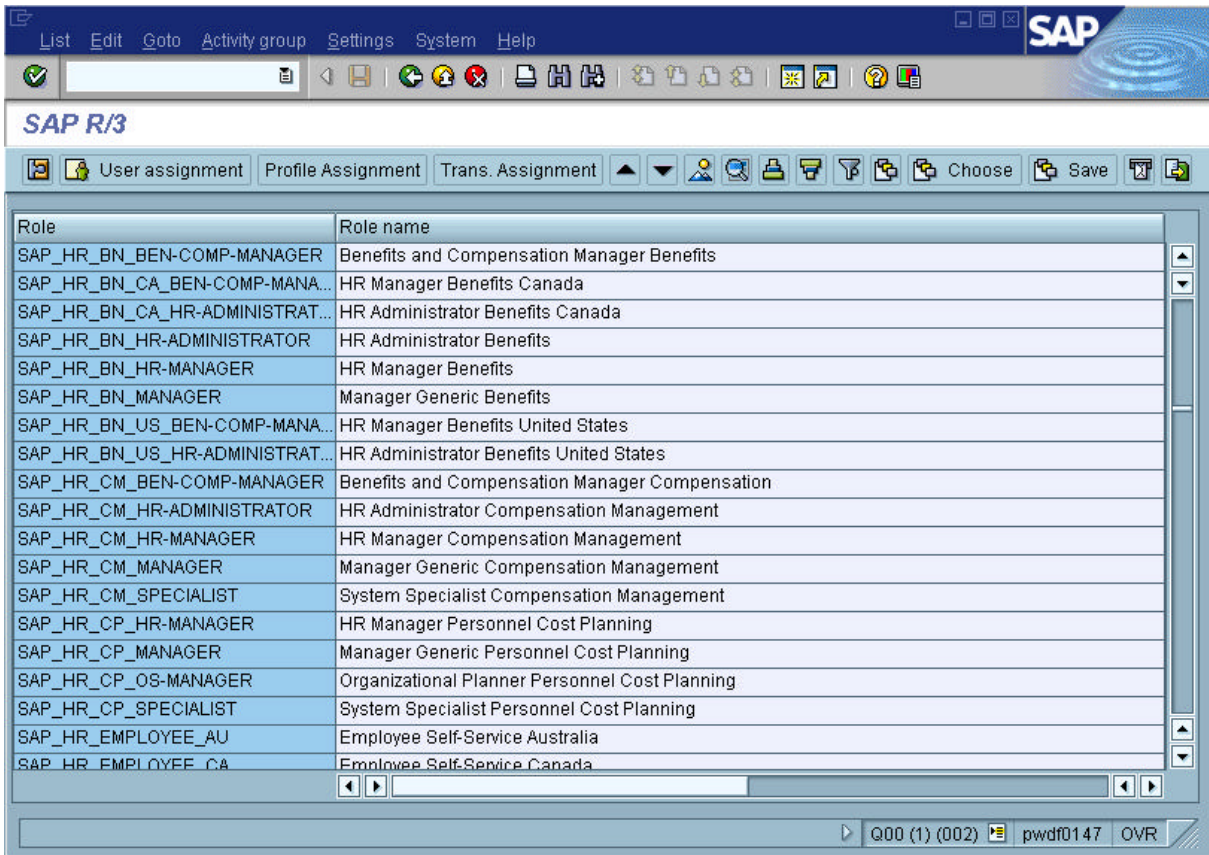
If you choose *Role description*, the description text of the predefined role is displayed as well as its name.

The list displayed lists the roles delivered in the SAP Standard.



Predefined roles are delivered as templates with the prefix 'SAP\_'.

Assign Standard Roles



Procedure

To assign user roles unchanged:

the SAP System *SAP Easy Access* initial transaction contains additional functions for administrators. You need authorization for the following authorization objects to be able to use these functions:

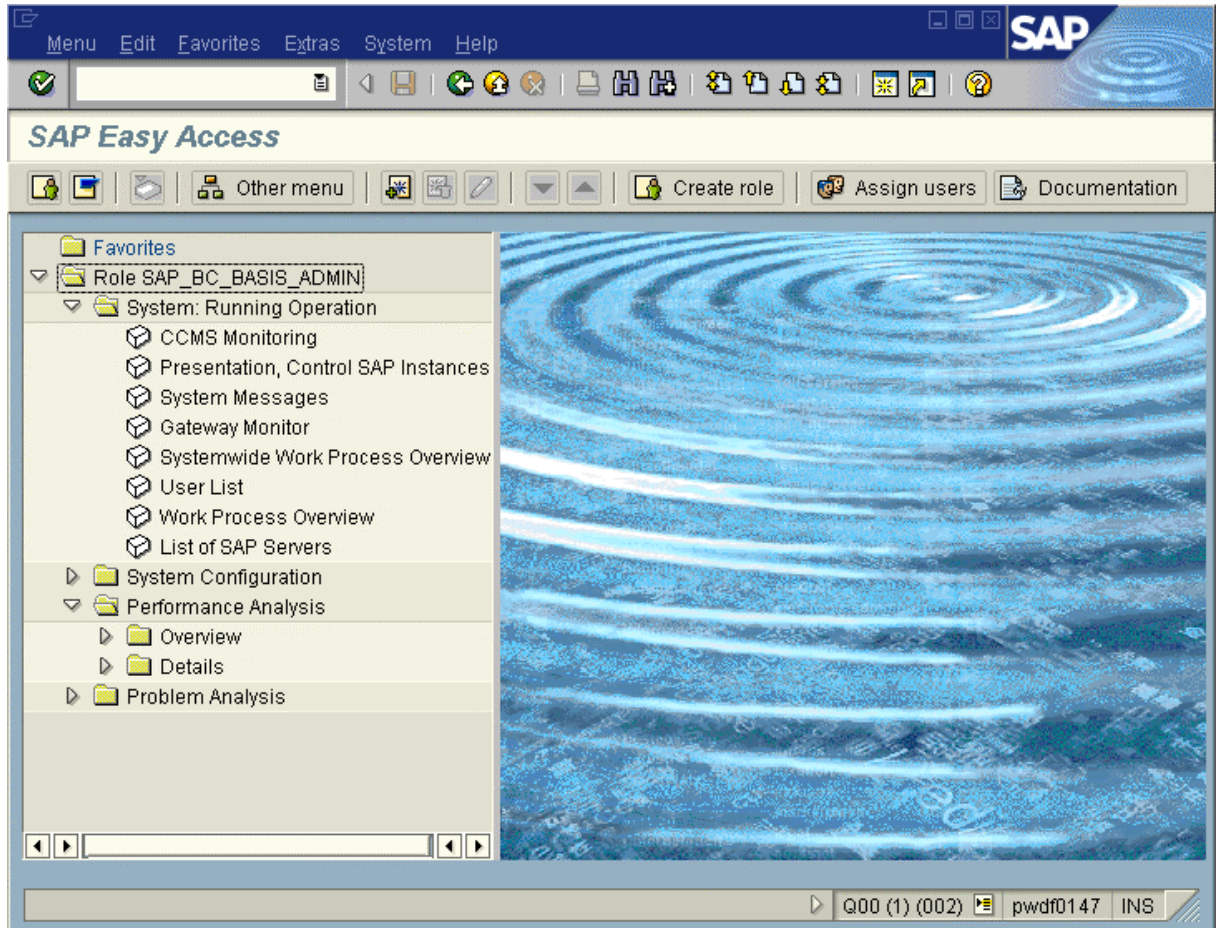
Authorization object:	Value:
S_USER_TCODE	PFCG
S_USER_PRO	*
S_USER_AUT	*
S_USER_GRP	*

You also need the following authorizations if the authorization profiles of the delivered roles are also to be generated automatically:

Authorization object:	Value:
S_USER_AGR	*
S_USER_TCD	*
S_USER_VAL	*



1. Choose *Other menu* in the initial transaction *SAP Easy Access*.



The delivered roles are output.

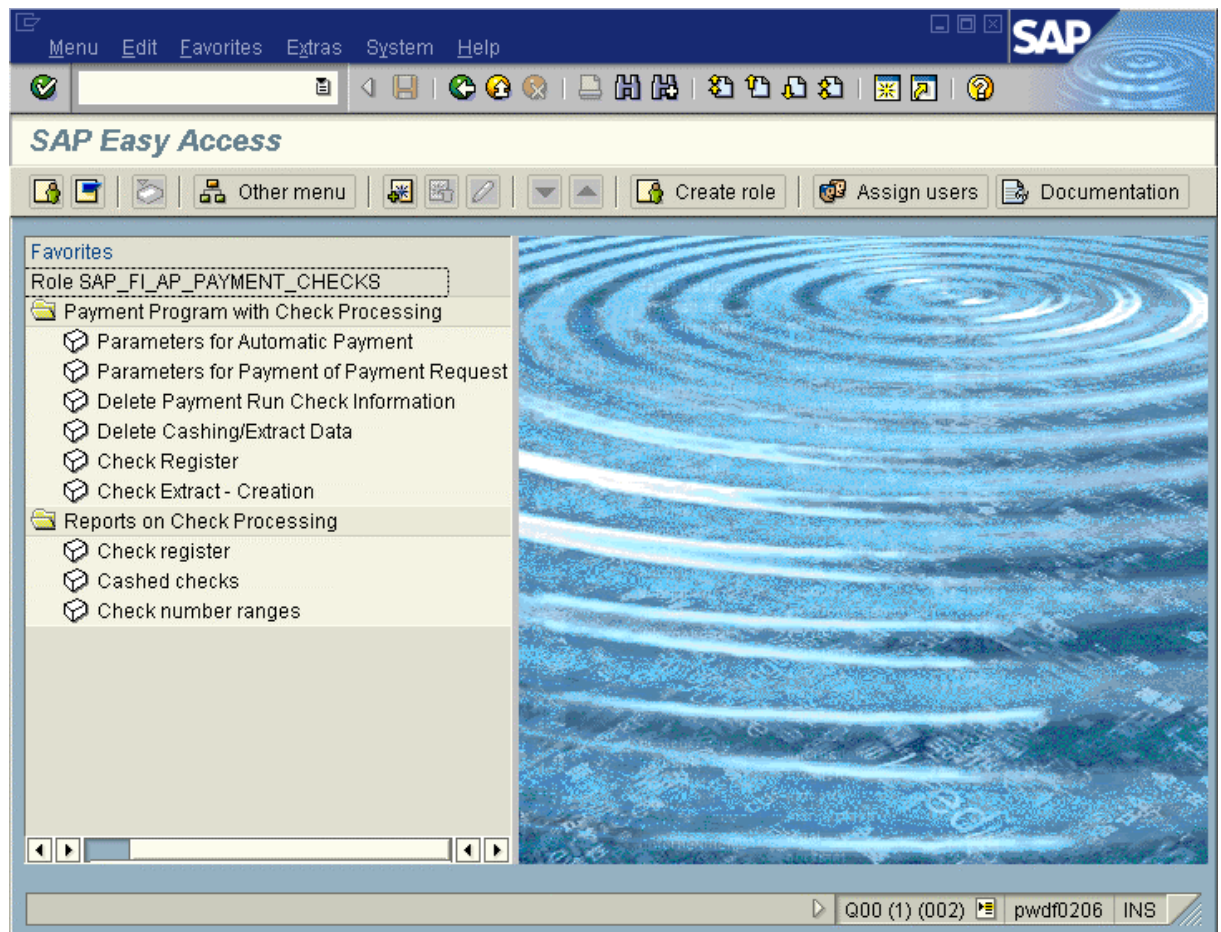
2. Choose a role/composite role by double-click.

## Assign Standard Roles

Role	Role name
SAP_FI_BL_BANK_MASTERDAT_DI...	FI: Bank master data display
SAP_FI_BL_BANK_MASTER_DATA	FI: Bank Master Data Maintenance
SAP_FI_BL_BANK_STATEMENT	FI: Processing bank statements
SAP_FI_BL_BILL_OF_EX_PRESENT	FI: Bill of exchange presentation
SAP_FI_BL_BILL_OF_EX_REPORTS	FI: Reports for Bill Holdings
SAP_FI_BL_CASHED_CHECKS	Cashed checks
SAP_FI_BL_INTRADAY_STATEMENT	FI: Import Intraday Bank Statement Information (USA)
SAP_FI_BL_LOCKBOX	FI: Processing Lockbox Data
SAP_FI_BL_ONLINE_PAYMENT	FI: Carrying out Online Payments
SAP_FI_BL_PAYMENT_TRANSACTI...	FI: Handling of Payments
SAP_FI_BL_PAYME_ADVICE_REPO...	FI: Reports on Payment Advices
SAP_FI_BL_POR_PROCEDURE	FI: Incoming payments using POR procedure (Switzerland)
SAP_FI_BL_RETURNED_BILL_OF_...	FI: Returned bills of exchange
SAP_FI_EMPLOYEE	Employee Self Service (FI)
SAP_FI_FM_BELEG	Change/display document
SAP_FI_FM_BUDGETEXECUTION	Maintain Budget Changes
SAP_FI_FM_BUDGETINFO	Report Selection Budgeting

3. You can view the user menu of the selected role/composite role. This does not create an assignment to your user.

## Assign Standard Roles



4. Choose *Assign user* to assign the currently displayed role directly to one or more users.
5. Enter the name of the user which you want to assign. *User selection* displays a multiple selection list of the current users in the system.

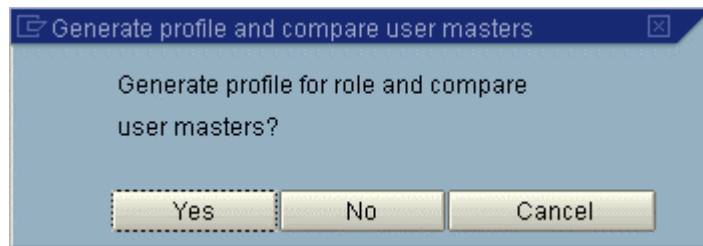


The users must already exist in the system before you can assign them. See [Create and maintain user master records \[Page 10\]](#).

6. Choose *Copy user*.
7. Confirm that the role profile is to be generated and the user master adjusted. The authorization profile is generated and put in the user master of the selected user in addition to the user menu of the selected role(s).

If you do not confirm the prompt, only the user menu is assigned to the selected users. The authorization profile is not generated and entered in the user master.

## Role Maintenance



The authorization data of all delivered roles are maintained. All customer-dependent fields, such as company code and plant, but also authorization groups and some other authorization fields, have the value '\*'. In many authorization fields, '\*' means the entire possible range of values. This allows usable authorization profiles to be pre-generated.

## Result

The users to whom you have assigned the role can logon to the system. The user menu appears with the functions which the user needs for his or her work and for which he or she has the necessary authorizations.

## Role Maintenance

### Purpose

You must maintain roles when the roles in the standard delivery need to be adjusted or you need to create new roles.

### Implementation

The SAP Standard contains a large number of roles. Check whether you can use a user role delivered in the standard before you define roles yourself.

Choose *Tools* → *Administration* → *User maintenance* → *Infosystem* → *Roles* → *Roles by complex selection criteria* in the SAP menu in the SAP Easy Access initial menu for an overview of the delivered roles.

You can also display a list of the delivered roles in the possible entries help for the *Role* field in the role maintenance (*Tools* → *Administration* → *User maintenance* → *Roles*).

You can copy and modify existing roles.

If you do not find a suitable role, write a job description before you maintain the role. See [Initial installation procedure \[Page 113\]](#).

All maintenance tasks can be executed centrally by a single "superuser". Alternatively, you can distribute these tasks amongst more than one user to ensure greater system security. Further details are contained in the section [Organizing User and Authorization Maintenance \[Page 115\]](#).

## Features

The system administrator chooses transactions, menu paths (in the SAP menu) or area menus, in the role maintenance (transaction PFCG). The selected functions correspond to the activities of a user or a group of users.

The tree which a system administrator creates here for a user group corresponds to the user menu which appears when the user to whom this role is assigned logs on to the SAP System.

The Profile generator automatically provides the required authorizations for the selected functions. Some of them have default values. Traffic lights show you which values need to be maintained.

Generate an authorization profile and assign the role to the users. The user menu appears when a user logs on to the SAP System.

In the role maintenance you can:

[Change and assign roles \[Page 37\]](#)

[Create roles \[Page 38\]](#)

[Create composite roles \[Page 62\]](#)

[Derive roles \[Page 63\]](#)

[Compare roles \[Page 64\]](#)

[Transport/assign roles \[Page 66\]](#)

**See also:**

[Assign standard roles \[Page 30\]](#)

## Change and Assign Roles

### Use

The roles in the standard delivery correspond to the working environment of certain users. They must be adjusted as required.

### Procedure

To copy, adjust and assign roles to one or more users:

1. Choose the pushbutton *Create role* or the transaction PFCG in the initial transaction SAP Easy Access.
2. Enter a name in the *Role* field or choose one from the possible entry help.



Predefined roles are delivered as templates with the prefix 'SAP\_'.

3. Copy the workplace example with *Copy role* and choose a name in customer namespace.
4. Choose *Change* (the new name is in the *Role* field).

## Create Roles

5. Choose the *Menu* tab to change the user menu. You can reduce, extend or restructure it. See [Create roles \[Page 38\]](#).
6. Choose the *Change authorization data* pushbutton in the *Authorizations* tab.
7. Maintain the authorization field values as required. To adjust the authorizations for the menu changes, choose the *Profile generation expert mode* pushbutton in the *Authorizations* tab and then *Read old version and adjust to new data*. The following overview shows you which authorizations you must maintain. See [Adjust default authorizations \[Page 44\]](#).
8. Generate the role profile.
9. Assign users in the *User* tab and compare users if necessary.



The users must already exist in the system before you can assign them. See [Create and maintain user master records \[Page 10\]](#).

## Result

The users to whom you have assigned the role can logon to the system. The user menu with the transactions, programs and internet links which the user needs for his or her work, and for which he or she has been assigned the necessary authorizations, appears.

## Create Roles

### Use

User-specific menus can be displayed for users after they have logged on to the SAP System by using either pre-defined roles or roles you created.

The role also contains the authorizations users need to access the transactions, reports, web-based applications and so on, contained in the menu.

You can assign a role to an unlimited number of users.

### Prerequisites

Check the suitability of the roles delivered by SAP before you create your own roles. You can use the user role examples just as they are delivered with the SAP System. If you want to modify them, all you need to do is copy the SAP template.

See [Assign standard roles \[Page 30\]](#) and [Change and assign roles \[Page 37\]](#).

### Procedure

The creation of a single role is described below. To create a composite role, see [Create composite role \[Page 62\]](#).

To create a single role:

## Create Roles

2. Choose the pushbutton *Create role* or the transaction PFCG in the initial transaction SAP Easy Access. You go to the role maintenance.
2. Specify a name for the role.

The roles delivered by SAP have the prefix 'SAP\_'. Do not use the SAP namespace for your user roles.

SAP does not distinguish between the names of simple and composite roles. You should adopt your own naming convention to distinguish between simple and composite roles.
3. Choose *Basic maintenance* (in the *Profile, Other objects* menu).
4. Choose *Create*.
5. Enter a meaningful role description text. You can describe the activities in the role in detail.



You may use an existing role as a reference. See [Derive roles \[Page 63\]](#).

6. Assign transactions, programs and/or web addresses to the role in the *Menu* tab. The user menu which you create here is called automatically when the user to whom this role is assigned logs on to the SAP System. You can create the authorizations for the transactions in the role menu structure in the *authorizations* tab.



If you want to call the transactions in a role in another system, enter the RFC destination of the other system in the *Target system* field.

You should only use RFC destinations which were created using the Trusted System concept ([Trusted System: Relationships between R/3 Systems \[Ext.\]](#)) to guarantee that the same user is used in the target system. This is only necessary if you want to navigate via the Easy Access Menu in the SAPgui.

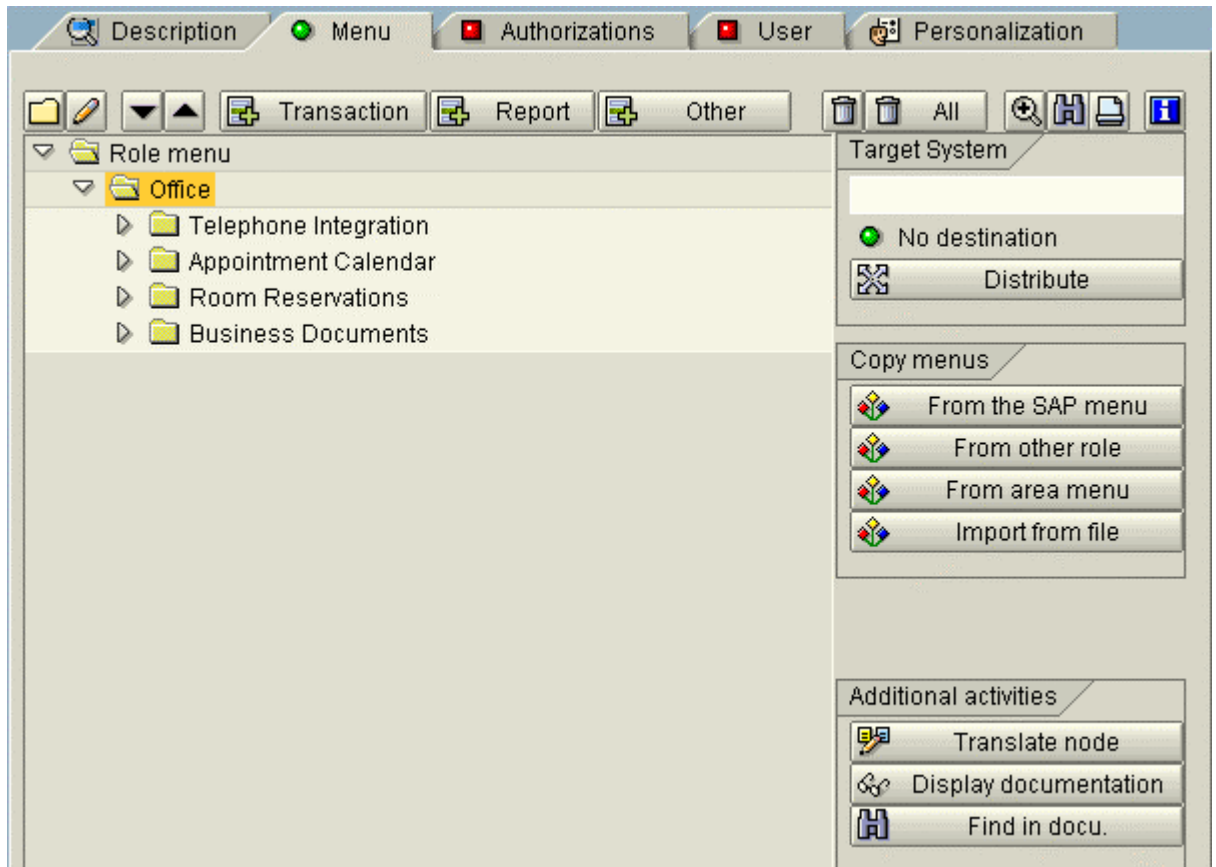
If you use the Workplace Web Browser, you can use any destination containing a logical system with the same name.

## Create Roles

If the *Target system* field is empty, the transactions are called in the system in which the user is logged on.

You can also specify a variable which refers to an RFC destination. Variables are assigned to the RFC destinations in the transaction SM30\_SSM\_RFC.

To distribute the role into a particular target system, specify the target system (its Release must be 4.6C) and choose *Distribute*. This function is most useful when you use the Workplace.



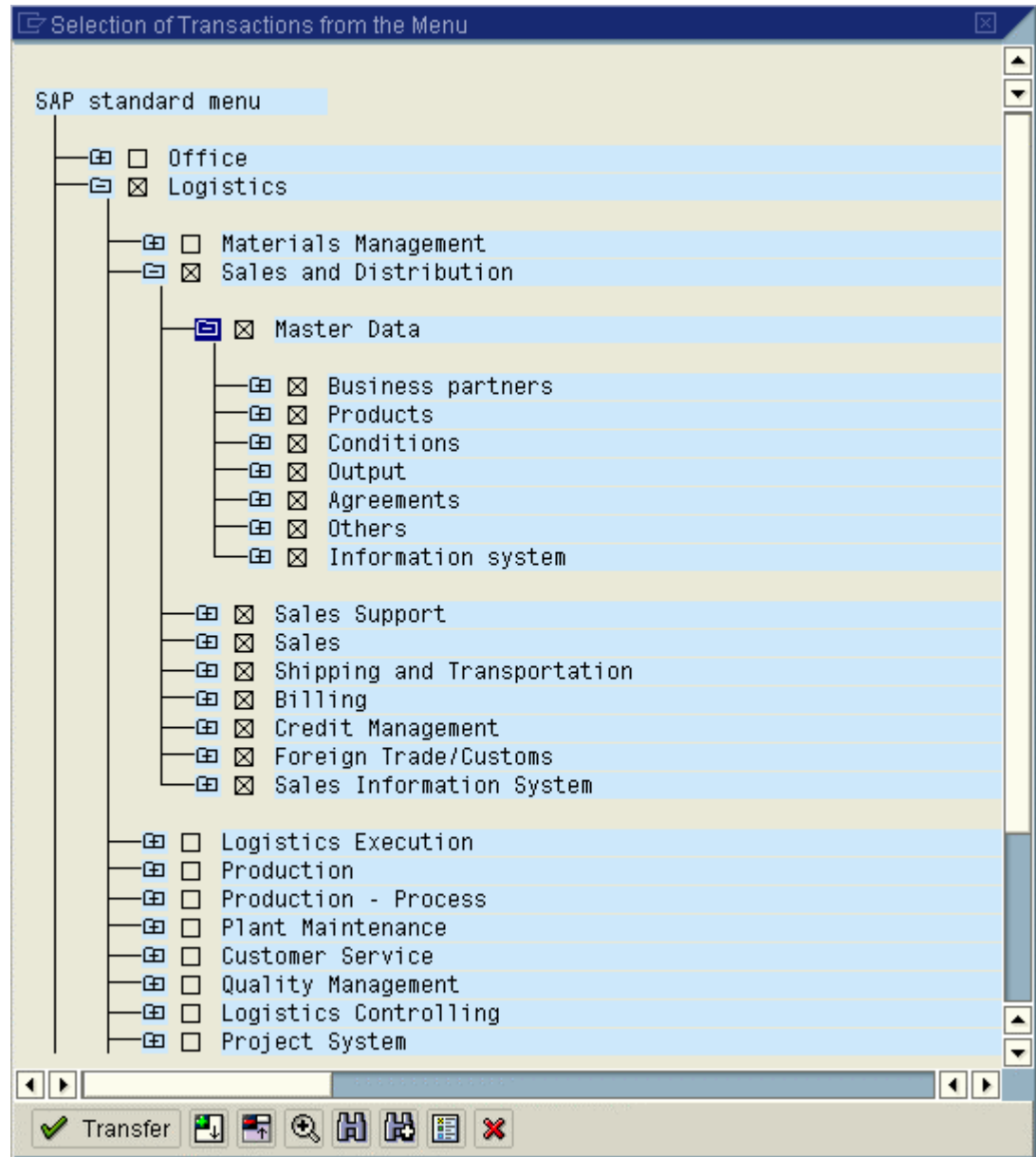
You can create the user menu:

- *from the SAP menu*



## Create Roles

You can copy complete menu branches from the SAP menu by clicking on the cross in front of it in the user menu. Expand the menu branch if you want to put lower-level nodes or individual transactions/programs in the user menu.



- *from a role*  
 this function copies a defined role menu structure in the same system into the current role. You can also copy the menu structure of a role delivered by SAP. Click on the menu branches and copy them.
- *from an area menu*  
 You can copy area menus (SAP Standard and your own) into a role menu. Choose an area menu from the list of menus and copy the transactions you want.

**Create Roles**

- *Import from file*

See [Upload/Download roles \[Page 67\]](#).

- *Transaction*

You can put a transaction code in the user menu directly.

- *Program*

This function puts programs, transaction variants or queries in the user menu. They need not be given a transaction code.

**ABAP Report**

Choose a report and a variant. You can skip the selection screen.

The screenshot shows the 'Transaction Code for Reports' dialog box. It has a title bar with a close button. The main area is divided into several sections:

- Report type:** A group of radio buttons with the following options:
  - ABAP report
  - SAP Query
  - Transaction with variant
  - BW Report
- ReportWriter options:** A group of radio buttons with the following options:
  - ReportWriter
  - Drilldown
  - Rep.portfolio
- ABAP report section:** A light-colored panel containing:
  - A 'Report' text label followed by a yellow input field with a magnifying glass icon.
  - A 'Variant' text label followed by a white input field.
  - A checkbox labeled 'Skip selection screen'.
- GUI-Fähigkeit section:** A light-colored panel containing three checkboxes:
  - SAP GUI für Windows
  - SAP GUI für Java
  - SAP GUI für HTML
- Generate automatically:** A checked checkbox.
- Transaction code:** A text label followed by a white input field.
- Adopt report description:** A checked checkbox.
- Description:** A text label followed by a white input field.

At the bottom of the dialog, there are two buttons: a green checkmark button and a red 'X' button.

You can generate a transaction code automatically and copy the report description by setting checkboxes.

#### *SAP Query*

Enter a user group and query name. If the query has a variant, you can specify it. You can also specify a global query. See [Query work areas \[Ext.\]](#).

#### *Transactions with variants*

The system administrator can create transaction variants in the SAP System [Personalization \[Ext.\]](#). Transaction variants adjust complex SAP System transactions to customer business processes, by e.g. hiding superfluous information and adding other information such as pushbuttons, text or graphics. You can put a transaction variant call in a user menu by entering the transaction code and variant which you created in the transaction SHD0.

#### *BW report*

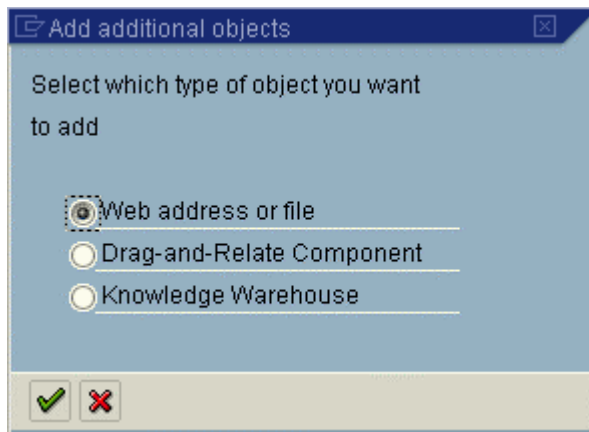
Include a Business Information Warehouse report. Enter the report ID.

#### *ReportWriter, Search, Report*

These function put other application-specific report types in the user menu.

- *Others*

Enter other objects:



#### *Web address or file*

Enter internet/intranet links with a descriptive text and the web address. You can enter a file name if the browser can call an application.

#### *Drag and relate component*










Enter the component name.

#### *Knowledge Warehouse link*

Use the *Document* field possible entries help. Choose the information object type. You go to a selection screen in which you can search for the object in the Knowledge Warehouse.

There are other pushbuttons for editing the user menu. Choose a menu entry with the cursor before you call one of the following functions.

## Editing Predefined Authorizations

Function:	Meaning
 <i>Create folder</i>	Group transactions, programs, etc. in a folder
 <i>Change node text</i>	Change a menu entry text
 <i>Move down</i>	Move a menu entry down one place
 <i>Move up</i>	Move a menu entry up one place
 <i>Delete nodes</i>	Delete a menu entry Any subnodes are also deleted.
 Delete all nodes	Delete the complete role menu
 <i>Translate node</i>	Translate a menu entry
 <i>Documentation</i>	Display the documentation of transactions, programs, etc.
 <i>Find doc.</i>	Find programs

You can restructure the menu by Drag & Drop.



The *Menu* tab status is red if no menu nodes are assigned. If at least one menu node is assigned, the status is green.



You can assign Implementation Guide (IMG) projects or project views to a role under *Utilities* → *Customizing auth.* Do this to generate IMG activity authorization and assign users. The authorization to perform all activities in the assigned IMG projects/project views is generated in profile generation. You make the assignments in a dialog box. Choose *Information* to display more information on using this option.

7. Save your entries.

## Result

You have created a role.

The next section [Edit predefined authorizations \[Page 44\]](#) describes how to display and edit predefined authorizations.

**See also:**

[Using composite roles \[Page 62\]](#)

## Editing Predefined Authorizations

Suppose you have created a role based on a selection of menu functions.

You can generate authorizations for this role automatically. Most of the fields for these authorizations are filled with SAP–assigned default values. However, you can add missing values, change default values and also add additional authorizations from SAP templates or profiles.

## Generating Authorizations

To create authorizations for a role, choose *Authorizations* in the role maintenance.

The *Authorizations* tab displays creation and change information as well as information on the authorization profile (including the profile name, profile text and status).

The screenshot shows the SAP 'Authorizations' tab with the following data:

Created by		Last changed on/by	
User	NIEDERMAIER	User	VOGTH
Date	20.12.1999	Date	14.02.2000
Time	13:51:51	Time	11:40:25

Information about authorization profile	
Profile name	T_BA800067
Profile text	Profile for role SAP_BC_ENDUSER
Status	Authorization profile is generated

Maintain authorization data and generate profiles	
	Change authorization data
	Expert mode for profile generation

There are open as well as default authorizations for the transactions you assign to the role. You can change this authorization data by choosing *Change authorization data* in *Authorizations*. Finally, you can use the Profile Generator to create an authorization profile based on this data. The authorization profile generated in this way is added to the authorization profiles of the users in the role after the user master records are compared.

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

The *Authorizations* tab index displays whether or not the corresponding authorization profile is current. The profile is not current if the display is red or yellow. The profile status text displayed on the tab explains the status of the profile in more detail. This helps you determine why the profile is not current.

Choose *Change authorization data* and then proceed as follows:

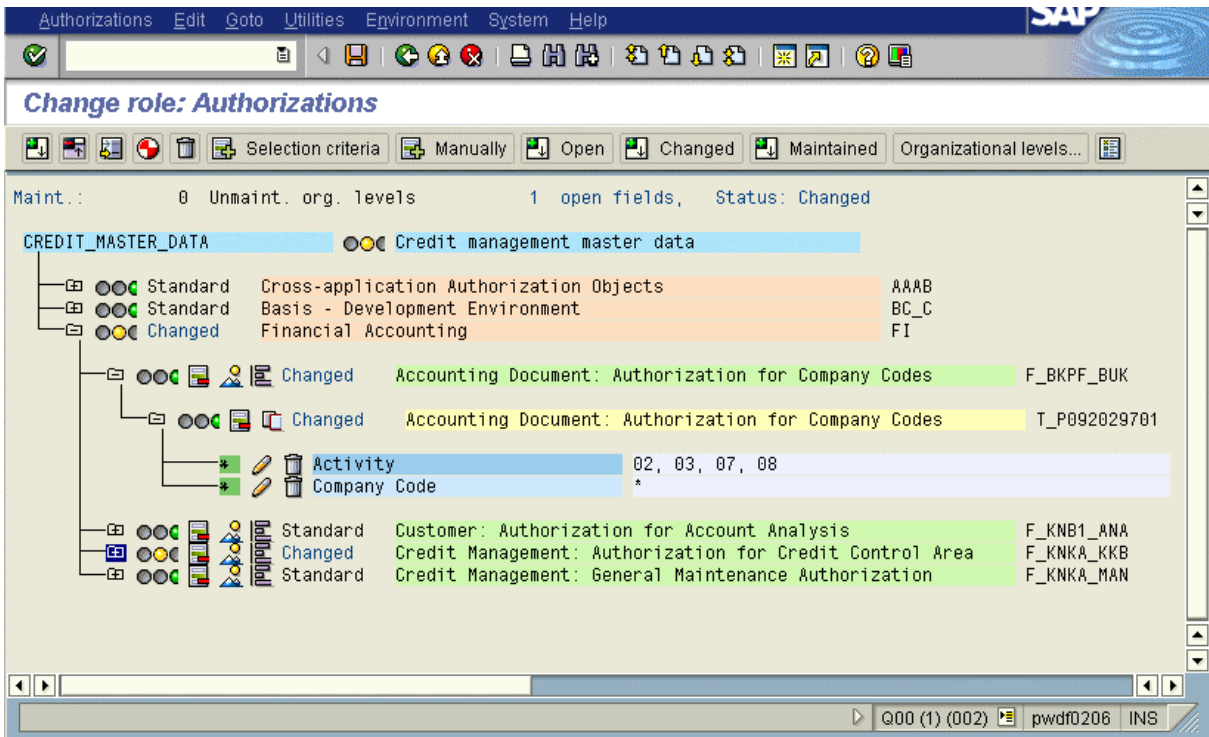
1. You can maintain organizational levels by choosing *Org. levels*.

Organization levels can be plants, company codes and business areas, for example. For each field that displays an organizational level, you determine the global values for these roles.



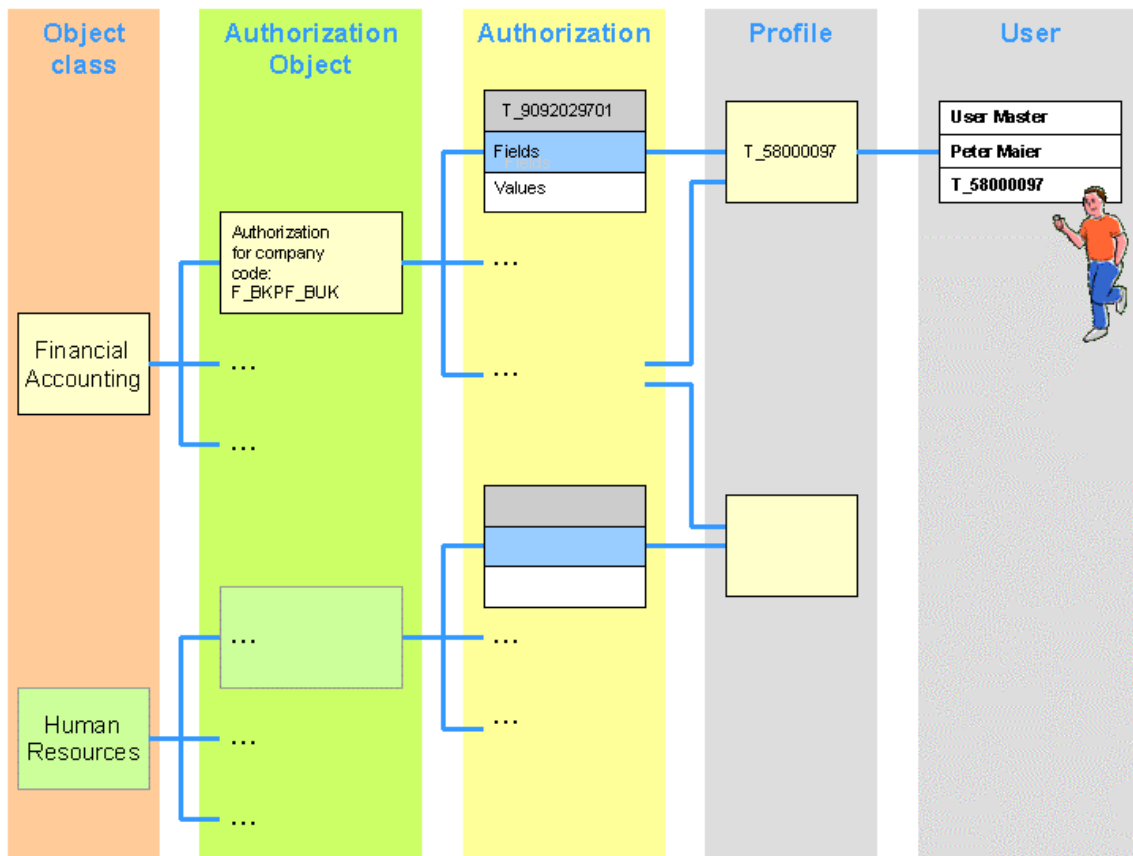
## SAP Authorization Concept Modules

The SAP authorization concept modules are color-coded in the hierarchy display.



The basic SAP authorization concept terms are displayed below, before you specify the authorization field values. The colors of the SAP authorization concept modules are the standard colors in the following hierarchy display.

SAP Authorization Concept Modules

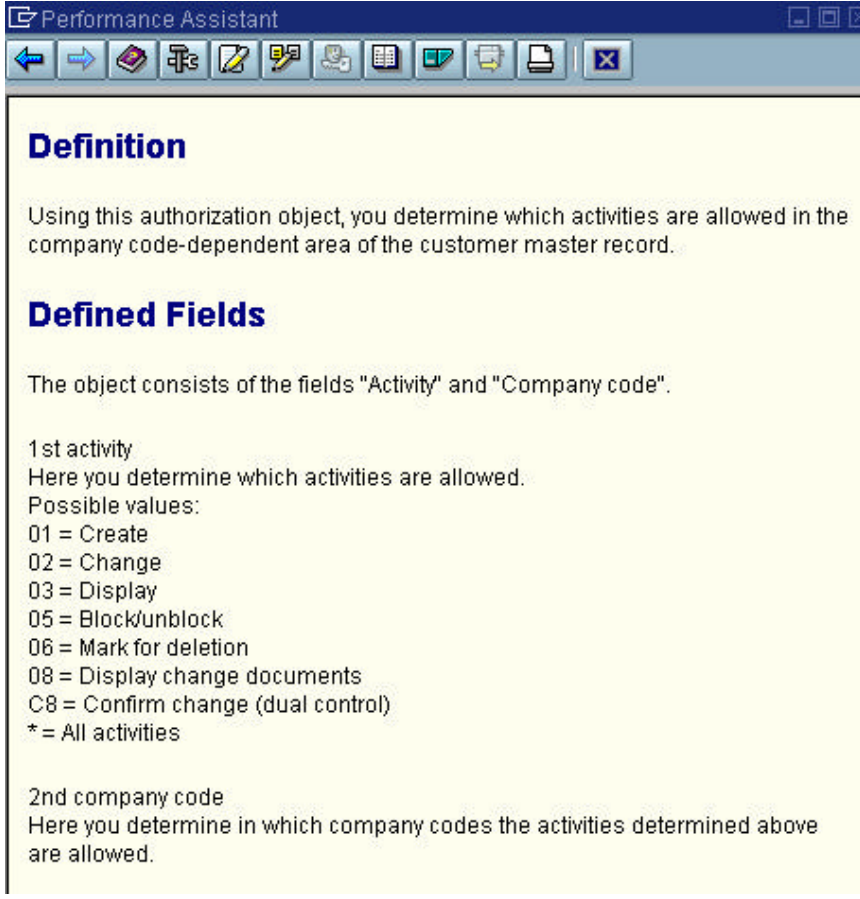


Explanation of terms:

<p>Object class</p>	<p>Object classes have an orange background in the hierarchy display.</p> <p>Authorization objects are divided into classes for comprehensibility. An object class corresponds e.g. to an application (Financial accounting, etc.)</p> <p>The SAP authorization concept object classes are under <i>Tools</i> → <i>Administration</i> → <i>User maintenance</i> → <i>Authorizations</i>.</p>
---------------------	--



SAP Authorization Concept Modules

<p>Authorization objects</p>	<p>Authorization objects have a green background in the hierarchy display.</p> <p>You may need several authorizations to perform an operation in the SAP System. The resulting contexts can be complex. The SAP authorization concept, based on authorization objects, has been realized to provide an understandable and simple procedure. Several system elements which are to be protected form an authorization object.</p> <p>An authorization object allows complex tests of an Authorization for multiple conditions. Authorizations allow users to execute actions within the system. An authorization object groups up to ten fields that related by AND.</p> <p>For an authorization check to be successful, all field values of the authorization object must be maintained in the user master.</p> <p>You get the authorization object documentation by double-click on an authorization object. The documentation describes how you maintain the authorization values.</p>  <p>The screenshot shows a window titled 'Performance Assistant' with a toolbar containing icons for navigation and editing. The main content area has a yellow background and contains the following text:</p> <p><b>Definition</b></p> <p>Using this authorization object, you determine which activities are allowed in the company code-dependent area of the customer master record.</p> <p><b>Defined Fields</b></p> <p>The object consists of the fields "Activity" and "Company code".</p> <p>1st activity Here you determine which activities are allowed. Possible values: 01 = Create 02 = Change 03 = Display 05 = Block/unblock 06 = Mark for deletion 08 = Display change documents C8 = Confirm change (dual control) * = All activities</p> <p>2nd company code Here you determine in which company codes the activities determined above are allowed.</p>
------------------------------	---

## SAP Authorization Concept Modules

## Authorizations

Authorizations have a yellow background in the hierarchy display. Authorization fields are light blue and their values are white.

An authorization enables you to perform a particular activity in the SAP System, based on a set of authorization object field values.

The programmer of a function decides whether, where and how authorizations are to be checked. The program determines whether the user is authorized to perform an activity by comparing the specified authorization object field values in the program with the authorization values in the user master record.



T\_9092029701 is an authorization for the authorization object F\_KNA1\_BUK with the following values:

\*           for company code and  
01,02    activity

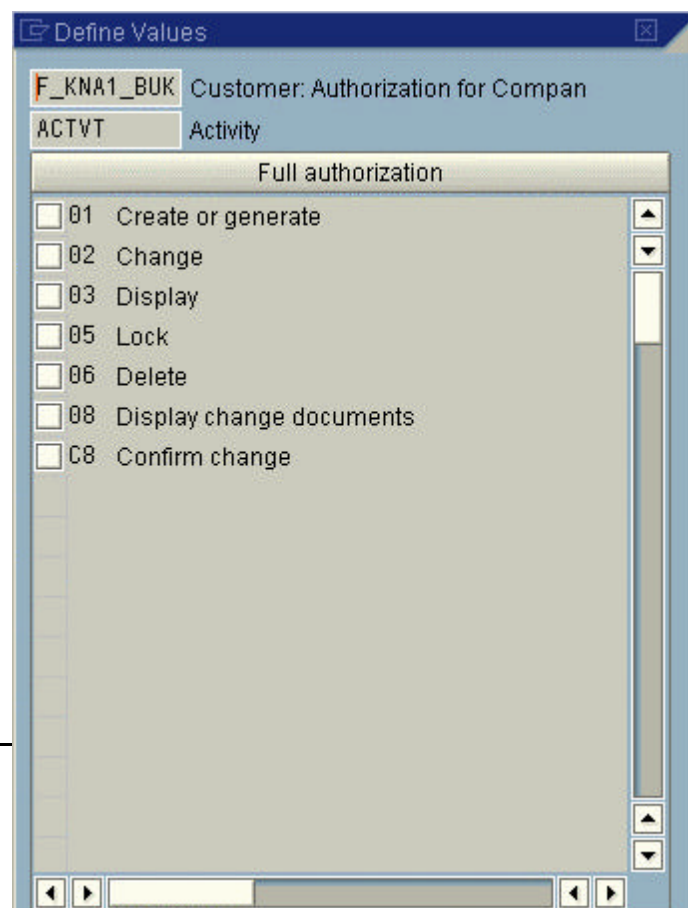
**Use of an authorization:** Specifies permissible authorization object field values.

**Contents:** One or more values for each field.

Authorizations allow you to specify any number of values or value ranges for a field. You can also allow all values, or allow an empty field as a permissible value.

**Changes:** All users with this authorization in their authorization profile are affected.

You can maintain authorizations manually with reference to the authorization object documentation or by double-click on a value field in the following dialog box:



SAP Authorization Concept Modules

<p>Profile</p>	<p>User authorizations are not usually assigned directly to user master records, but grouped together in authorization profiles.</p> <p>Authorizations can be collected in authorization profiles to reduce the maintenance effort which would be required to enter individual authorizations in the user master record. Access authorization changes affect all users with the profile in their master record.</p> <p>You can create profiles manually, but you should use the Profile generator.</p> <p><b>Use:</b> Specifies authorizations in user master records</p> <p><b>Contents:</b> Specific access rights, identified by an object name and a corresponding authorization name.</p> <p>Changes only take effect when the user next logs on. Users who are logged on when the change takes place are not affected in their current session.</p> <p>In the example, T_58000097 is an authorization profile containing company code authorizations.</p>
<p>User Master Record</p>	<p>These enable the user to log onto the SAP System and allow access to the functions and objects in it within the limits of the specified authorization profiles.</p> <p>Changes only take effect when the user next logs on. Users who are logged on when the change takes place are not affected in their current session.</p> <p>In the example a user whose user master record contains the profile T_58000097 can perform the activities in the profile authorizations.</p>

When a transaction is called, a system program makes various checks to ensure that the user has the appropriate authorization.

Is the transaction code valid? (table TSTC check).

Is the transaction locked by the system administrator? (table TSTC check).

Is the user authorized to call the transaction?

The authorization object S\_TCODE (call transaction) contains the field TCD (transaction code). The user must have an authorization with a value for the selected transaction code.

Does the transaction code have an authorization object? If so, a check is made that the user has authorization for this authorization object.

If one of this checks fails, the transaction is not called and the system sends a message.

If the transaction is called, it calls an ABAP program which makes further authorization checks with the AUTHORITY-CHECK command. The programmer specifies an authorization object and the required values for each authorization field.

AUTHORITY-CHECK checks whether a user has appropriate authorization. To do this, it searches in the specified authorization profile in the user master record to see whether the user has authorization for the authorization object specified in the command.

If the authorization is found and it contains the correct values, the check is successful.

## Authorization Check Scenario

[Authorization check scenario \[Page 52\]](#) contains an example of the use of the `AUTHORITY-CHECK` command.

## Authorization Check Scenario

A programmer wants to make an authorization check before bookings for business customers can be changed.

To do this, the programmer should [create an authorization fields \[Page 85\]](#) (`ACTVT` and `CUSTTYPE`) and assign for each field defined the value to be checked (`02`, `B`). Authorization fields are created under *Tools* → *ABAP Workbench* → *Development* → *Other tools* → *Authorization objects* → *Fields* (transaction `SU20`).

Programmers should also [create an authorization object \[Ext.\]](#) (here `s_TRVL_BKS`) and [assign the authorization object to an object class \[Page 85\]](#).

Authorization fields are created under *Tools* → *ABAP Workbench* → *Development* → *Other tools* → *Authorization objects* → *Objects* (transaction `SU21`). Authorization objects can also be created in the Object Navigator (transaction `SE80`).

You program the authorization check using the ABAP statement `AUTHORITY-CHECK`.

```
AUTHORITY-CHECK OBJECT 'S_TRVL_BKS'
                  ID 'ACTVT'    FIELD '02'
                  ID 'CUSTTYPE' FIELD 'B'.
IF SY-SUBRC <> 0.
  MESSAGE E...
ENDIF.
```

The `AUTHORITY-CHECK` checks whether a user has the appropriate authorization to execute a particular activity.

When this happens, the system checks the authorization profiles in the user's master record for the appropriate authorization object (`s_TRVL_BKS`). If the authorization is found and it contains the correct values, the check is successful.

The system administrator has defined the following authorizations for the authorization object `s_TRVL_BKS`:

- `s_TRVL_CUS1` with the following values:
  - \* for customer type (`CUSTTYPE` field) and
  - 02** for activity (field: `ACTVT`).

Users with this authorization may change bookings for all customers.
- `s_TRVL_CUS2` with the following values:
  - B** for customer type (`CUSTTYPE`) and
  - 03** for activity (`ACTVT`).

Users with this authorization may display all business customer bookings.

When assigning profiles, the system administrator gave different authorizations to different users.

**Symbols and Status Text in Authorization Maintenance**

User Miller has been assigned a profile containing both of these authorizations (S\_TRVL\_CUS1 and S\_TRVL\_CUS2). Miller can therefore change bookings for business customers.

User Meyers on the other hand, is only authorized to display the records (S\_TRVL\_CUS2) and therefore cannot change bookings.

**Symbols and Status Text in Authorization Maintenance**

You can edit the display elements using icons in the hierarchy level and in the toolbar.

The current status of the organizational units and authorizations is shown in the status (header) line and at the various levels of the tree structure with red, yellow and green traffic lights.

	Authorization fields are maintained
	Authorization fields not completely maintained
	<p>Organizational levels are not maintained. Choose <i>Org. levels</i> to maintain the organizational levels.</p> <p>Specify a global value for this role for each field representing an organizational level. If, for example, the organizational level <i>PLANTS</i> appears in several authorizations, you only need to maintain the plant values once on the <i>Organizational levels</i> screen.</p> <p>You can display a list of all existing organizational levels using Transaction SUPO.</p>



You should also check the values of the authorization fields marked with a green traffic light.

Choose *Open*, *Modified* or *Maintained* to display open, changed or modified authorizations, respectively.



The status line shows the status of the authorization profile: *Unchanged*, *Saved*, *Changed* or *Generated*.

Authorization field value maintenance functions:

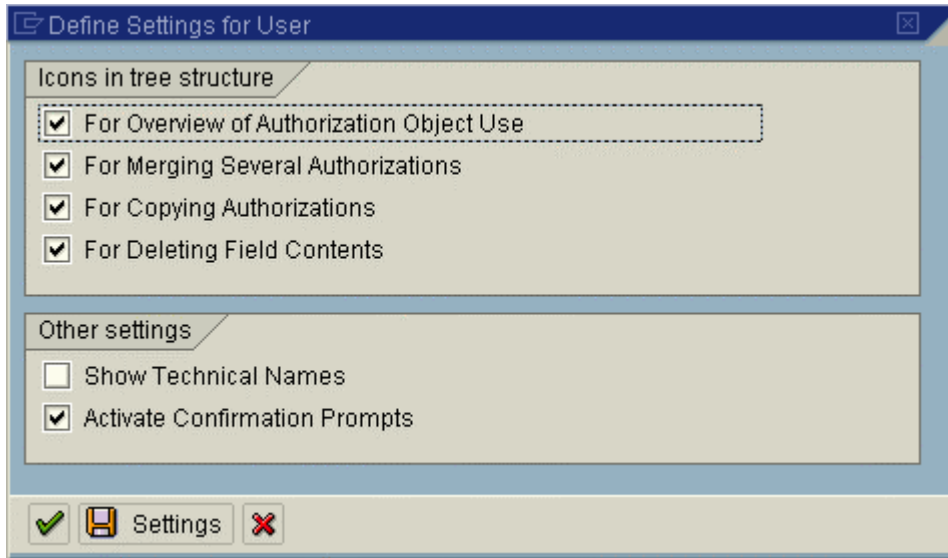
	<p>Click on the maintenance symbol to maintain an authorization field value. You can also double-click on an authorization field value or click on an empty field.</p> <p>Maintain the values in the dialog box.</p>
*	<p>You can setup general authorization by clicking on the asterisk in front of an authorization field name, or choosing a pushbutton in the input window.</p>





The following icons are also displayed where appropriate:

**Symbols and Status Text in Authorization Maintenance**

	Deactivate an authorization or authorization object. Inactive authorizations are ignored when profiles are generated.
	Reactivate inactive authorizations.

You can display other symbols with *Utilities* → *Settings*:




	Display transactions which use this object.
	Summary of authorizations. You can summarize identical authorization field contents of an authorization object by choosing <i>Utilities</i> → <i>Summarize auths.</i>
	Copy authorizations.
	Delete field contents.

You can also show the technical names of the authorization objects and activate security checks, under *Settings*.

The authorization status text displays their maintenance status. The status of a field, authorization, object, object class or the role is indicated as follows:




Standard	All field values in the subordinate levels of the hierarchy are unchanged from the SAP defaults.
Maintained	In the subordinate levels of the hierarchy there is at least one field that was delivered empty by SAP and which you have later filled with a value.

**Copying Authorizations From Templates**

Changed:	You have changed the SAP default value of at least one field in the subordinate levels of the hierarchy. The status also changes to <i>Changed</i> if you change an organizational level which was previously set globally (unless you make the change in the <i>Maintain organizational levels</i> dialog box.
Manual:	You have entered at least one authorization, template or profile in the hierarchy below with the  <b>Manually</b> function
Old:	The comparison found that all field values in the subordinate levels of the hierarchy are still current and that no new authorizations have been added.
New	The comparison found that at least one new authorization has been added to the subordinate levels of the hierarchy. If you now choose <i>New</i> , all new authorizations in the subordinate levels are expanded.

**Adding Authorizations**

The standard toolbar contains two pushbuttons to insert authorizations:

 Selection criteria	Enter single authorizations. Select via object classes. Click on the symbol  to copy authorizations. Choose the pushbutton <i>Insert selected</i> .
 Manually	Manual entry of authorization objects. Enter the technical names of the authorization objects which are to be put in the role. You can use possible entries help.

When you enter authorizations with *Edit* → *Enter authorization*, you can also:

- Add full authorization (add all authorizations for an authorization object)
- Add authorizations from a profile
- [Copying Authorizations From SAP Templates \[Page 55\]](#)

## Copying Authorizations From Templates

### Use

You can copy general authorizations into a role in the form of templates. So you can assign general authorizations to users.

You can also create your own templates in the transaction SU24.

### Prerequisites

In order to edit models in Transaction SU24 you need the User Master Maintenance and User Group (S\_USER\_GRP) authorizations, with value \* in the CLASS and ACTVT fields.

### Procedure

You can assign general authorizations to users in one of two ways:

## Generating Authorization Profiles

1. Create a role which only contains general authorizations (such as printing). Then assign this role to all users. This is the best thing to do if all users are to be allowed to print from any printer, for example.
2. Use a template to import the required objects into the role and then maintain missing field contents. This is the best thing to do if each user assigned to a role may use only one particular printer, for example.

In the authorization data maintenance, choose *Edit* → *Insert authorizations* → *From template*. Choose the SAP\_PRINT template. Authorization data is now included in the authorization profile, but you still need to fill in missing details such as which printers are to be used.

If you want to create your own templates, choose *Edit templates* in Transaction SU24. You can then either create your own templates or make copies of SAP templates and change these. Unlike changes to defaults, changes to templates are not passed on when you compare roles.



The names of SAP templates begin with *s*. If you create any templates yourself, they should not begin with *s*.

## Generating Authorization Profiles

### Use

Authorization profiles must be generated before they can be assigned to users. An authorization is generated for each authorization level in the browser view, and an authorization profile for the whole role as represented in the browser view.


### Prerequisites

Before generating an authorization profile, the system checks that you are authorized for the object *Maintain User Masters: Authorization Profile* (S\_USER\_PRO).

If the changed profile is already assigned to some users:

You should only generate profiles after the users of the role you want to edit have logged off the system. If the users are logged on, they must logon again after generation to have the current authorizations.

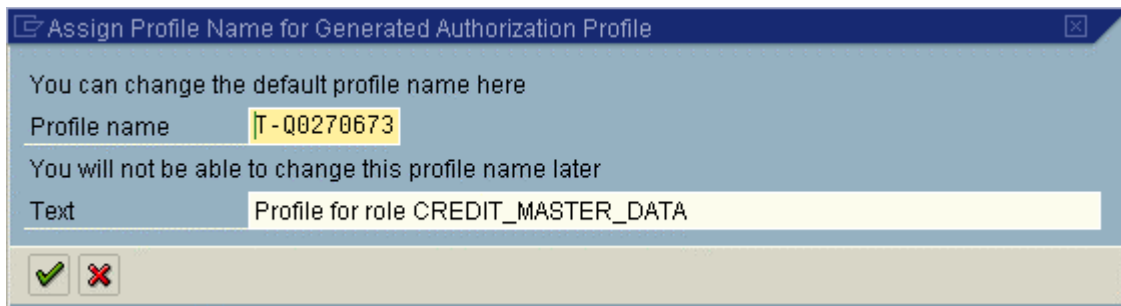
### Procedure

When you have maintained all fields and organizational levels, generate the authorizations or the profile of this role, by choosing  or *Authorizations* ® *Generate*.

The following dialog box appears:



## Regenerate the Authorization Profile Following Changes



You can change the profile name and text.



When you generate an authorization profile the technical names of the authorizations are automatically reorganized.

You can display the technical names by choosing *Utilities* → *Technical names on*. They comprise the activity profile name and a number in the range 00 - 99: T\_<role>nn, for example T\_5002995604

To avoid problems with number assignment, you should reorganize the numbers nn from time to time. Choose *Utilities* → *Reorganize*. This restarts the number assignment starting at 00.

You can display an overview of the existing authorization profiles for this role by choosing *Authorizations* → *Profile overview*.

The overview contains profile names and their maintenance status (not generated, maintenance version, active version).

## Result

Whenever you assign the role to a user, you can also assign the generated authorization profile to that user (see [Assigning Profiles \[Page 15\]](#)).

The system then displays the current status of the authorization profile: *generated*.

**See also:**

[Regenerating Authorization Profiles Following Changes \[Page 57\]](#)

[Check roles for existing profiles \[Page 59\]](#)

## Regenerate the Authorization Profile Following Changes

When you change a role, you must regenerate the authorization profile. In this case, the tab index *Authorizations* is marked in red or yellow. The status text displayed on the tab explains the status of the profile in more detail.

If a red symbol appears on the tab index, you must compare and adjust the profile. The menu has changed since the profile was last generated. If the display is yellow, the profile has been changed and saved since it was generated. This means that the generated profile is no longer current.

## Regenerate the Authorization Profile Following Changes

On the maintenance screen *Change role: Authorizations*, you can make the necessary changes and regenerate the profile.

If you select *Expert mode for profile generation* under the *Authorization* tab, you can choose the option with which you want to maintain the authorization values (this option is automatically set in normal mode).

In expert mode, you can:

- *Delete and recreate profile and authorizations*  
All authorizations are recreated. Values which had 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 using the saved values. It is not worth doing this if the assignment of transactions to roles has changed.
- *Read old status and compare with new data*  
The Profile Generator compares the old data to the current data in the role. It is worth doing this if the role menu has changed. Unchanged data is marked as *Old*, new data as *New*.

Note the following when you execute the comparison:

- The maintained organizational levels remain. If new levels are added, they need to be maintained. Superfluous organizational levels are deleted.
- If authorizations in an authorization object have changed, a manual comparison is necessary: you must decide whether you want to retain the old modified data, or use the current version. Delete or maintain the authorizations you no longer require.
- Maintained authorizations are filled automatically, as far as possible, with the values you have maintained.



The transactions in the role determine the following activities in an authorization: *Create, Change, Display* [Authorization group \[Ext.\] 0001](#) (maintained by you).

This is the old, maintained status. You change the role to have the following actions: *Change, Display* and *Delete*. The value 0001 is then copied for the authorization group activities *Change* and *Display* as these were already maintained. *Insert* is no longer displayed on the screen. You still need to maintain the authorization group for the *Delete* activity, since this was not maintained in the old status.

- Wherever the *New* attribute appears, you need to check whether the new authorizations make sense. If necessary, you can compare them manually with the old values.
- Manually entered authorizations are not deleted.
- The values for authorization object T\_CODE are always filled automatically with the current transactions from the role, but receive the attribute *Old*.

Choose one of the three options. The system displays a browser view.

The status line contains the authorization profile status: *unchanged, saved, changed or generated*.

## Mass Generation of Profiles

### Use

The mass profile generation transaction tells you which roles already have authorization profiles.

You can generate roles *en masse* or generate the missing role authorization profiles in the background.

You can limit the choice of roles.

### Prerequisites

You will need the following authorizations to use Transaction SUPC:

- User master maintenance: Authorization Profile (S\_USER\_PRO)
- User master maintenance: Authorizations (S\_USER\_AUT)
- Authorization system: Check for roles (S\_USER\_AGR)

### Procedure

1. Choose *Environment* → *Mass Generation* in the role maintenance (transaction SUPC).
2. Specify selection criteria.

## Assign Users

**Roles: Mass generation of profiles**

Which roles do you want to output?

Only roles that can be generated

Also roles to be adjusted

Also roles w/o auth. data

All roles

Additional restrictions

Role  to

Last changed by  to

Presentation in the list

Creation and change date

Display role texts

Generate all profiles to be generated?

Generate automatically

If you do not want to generate all profiles automatically (last checkbox), you can further restrict the role selection in the next screen.

## Assign Users

### Use

You have created a menu for the new role and setup the authorizations. You must finally assign the roles to users.

### Procedure

You have created a menu for the new role and setup the authorizations. You must finally assign the roles to users. Proceed as follows:

1. Choose the *User* tab.

The status display in the tab tells you whether the roles have already been assigned to users. If the display is red, no users are assigned. Green means that at least one user is assigned. Yellow means that users are assigned but the user master comparison is not up-to-date.

## Assign Users

The status of composite roles only refers to user assignment.

User ID	User name	From	to
MILLER	John Miller	15.02.2000	31.12.9999

2. Enter the user name in the list.

Enter the user name either directly or from the possible entries help. You can make a multiple selection with the *Select* pushbutton, e.g. all users in a user group.

You can specify a validity period for the assignment in the other columns. When you assign users to the role, the default start date is the current date and the default end date is the 31.12.9999. You can change these default values.

3. Make a user comparison if necessary.

The generated profile is not entered in the user master record until the users have been compared. Changes to the users assigned to the roles and the generation of an authorization profile also require a comparison.

There are various ways of comparing users:

- Choose *User comparison* in the *User* tab. The users are compared for the role you created. The status displayed for this key specifies whether a new comparison must be made.
- Choose *Utilities* → *Settings* and *Automatic comparison at save*. When you save the role, a user comparison is performed automatically.
- Wait until the user comparison is made with the program PFCG\_TIME\_DEPENDENCY.

You should schedule PFCG\_TIME\_DEPENDENCY periodically (preferably daily) as a background job. This ensures that user authorizations are regularly updated. The program performs a complete user master comparison for all roles. The authorizations are updated in the user master records. The authorization profiles of user assignments which have become invalid are removed from the user master record. The authorization profiles of valid user assignments to the role are entered.



Users who are assigned to a composite role are displayed on a gray background in the roles in the composite role. The entries cannot be changed. They should only be changed in the composite role.

If you perform a user master comparison for the composite role, it performs a user master comparison for all roles in the composite role.

## Personalization

# Personalization

## Use


You can set certain system person or role defaults in this tab. Tasks in a role can have person or role default values.

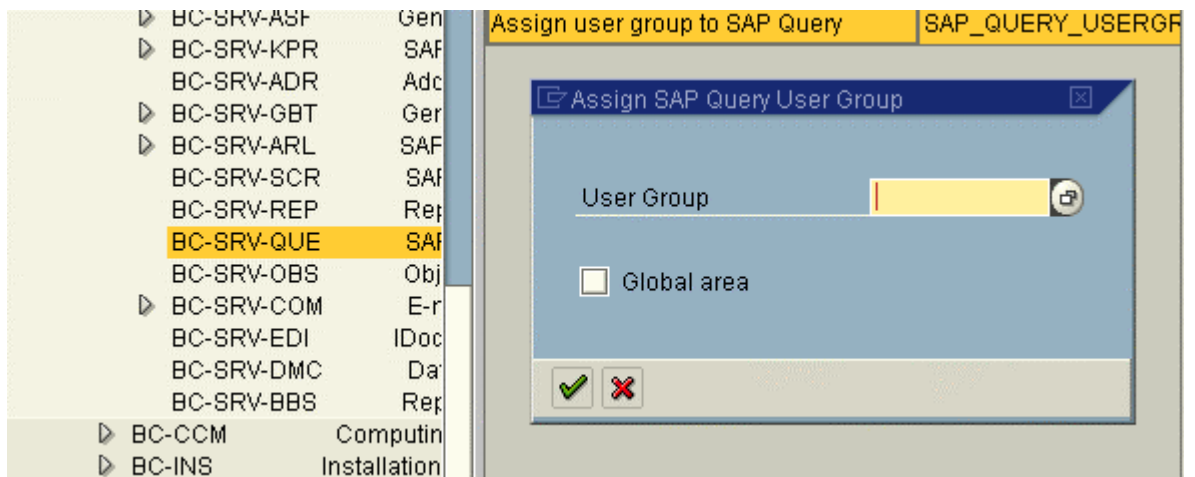
## Integration

You can call the *Personalization* tab in the role or user maintenance.

## Activities

To assign personalization data to the user or role:

5. Choose the *Personalization* tab.
6. Choose  to display the application components on the left-hand side of the screen.
7. Choose a component whose personalization data is to be maintained. The personalization objects for the component are output on the right-hand side.



8. Double-click on a personalization object. A default value entry dialog box appears.

## Create Composite Roles

## Use

Composite roles can simplify the user administration.

They consist of roles. Users who are assigned to a composite role are automatically put in its roles when you compare. Composite roles do not themselves contain authorization data.

Composite roles are useful for example if some of your staff need authorization for several roles. You can create a composite role and assign the users to it instead of putting each user in each role.

## Procedure

To create a composite role:

1. Enter a name in the *Role* field in the role maintenance (transaction PFCG).



The SAP System does not distinguish between the names of simple and composite roles. You should adopt your own naming convention to distinguish between simple and composite roles.

2. Choose *Create collective role*.
3. You can define the composite role in the following screen.
4. Save your entries.
5. Enter the roles in the composite role in the *Roles* tab. You can display all the simple roles in the system with the possible entries help.



Composite roles cannot contain composite roles.

6. You can restructure the role menus which you read in with *Read menu*, in the *Menu* tab. See [Create roles \[Page 38\]](#).

This does not affect the menus of the roles.

The  key in the *Menu* tab contains composite role menu notes.

7. Either enter the names of the users individually in the *User* tab (manually or from the possible entries help) or choose *Selection*. You can define selection criteria (e.g. all users in a user group)

If you select a username and choose *Display*, detailed user information is displayed.

Choose *Compare users*. The user data is updated after the comparison.

Users which are assigned to a composite role are displayed on a gray background in its roles (not changeable). The user assignment should only be changed in the composite role.



You can display an overview of the roles in composite roles with *Role hierarchy in composite roles* in the role maintenance initial screen. You can select a role in the hierarchy display for editing by double-click.

## Derive Roles

### Use

There are two possible reasons for deriving a role from an existing role:

- The role menus are identical but the authorizations for the menu actions are different in the derived role.

## Compare Roles

- The menu and authorizations of the derived role are identical, but the organizational levels are different in the derived role.

## Prerequisites

Roles derived from another cannot have any additional menu entries.

## Procedure

To create a reference to another role:

1. Create a role.
2. Enter a role description text.
3. Enter the name of the role from which all transactions including the menu structure are to be copied in the *Derive from role* field in the *Description* tab.

When you save, you have created a role whose menu is derived from another role.

To copy the authorizations to the derived role:

1. Change the role from which the authorizations are to be derived, in the role maintenance. Choose the *Authorizations* tab and the *Change authorization data* pushbutton.
2. Choose the menu entry *Authorizations* → *Adjust derived* → *Generate derived roles*.

The authorization data is copied to the derived roles.



The organization level data is only copied the first time the authorization data is adjusted for the derived role. If organization level data is maintained in the derived role, it is not overwritten by subsequent adjustments.

You need complete authorization for the authorization object S\_USER\_VAL and change authorization for the derived roles to adjust the authorization data of derived roles.

To delete the inheritance relationship between two roles, choose the *Delete inheritance relationship* pushbutton in the *Description* tab.

You can display an overview of the inheritance of roles by choosing *Role* → *Where-used list*. You can go to another role by double-click.



You cannot derive functions from the delivered user roles in your own roles.

## Compare Roles

### Use

You can compare and adjust roles between:

- two roles in a system



- two roles in different systems
- a role and its template
- a newly-delivered role and its previous customer version

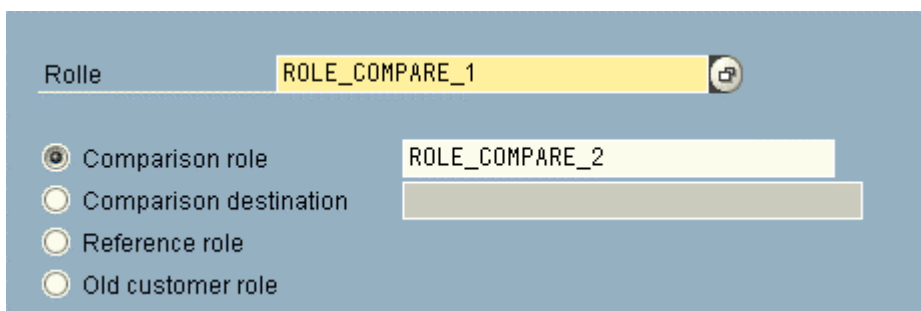
## Prerequisites

To compare two roles in different systems, their RFC destinations must be maintained.

## Procedure

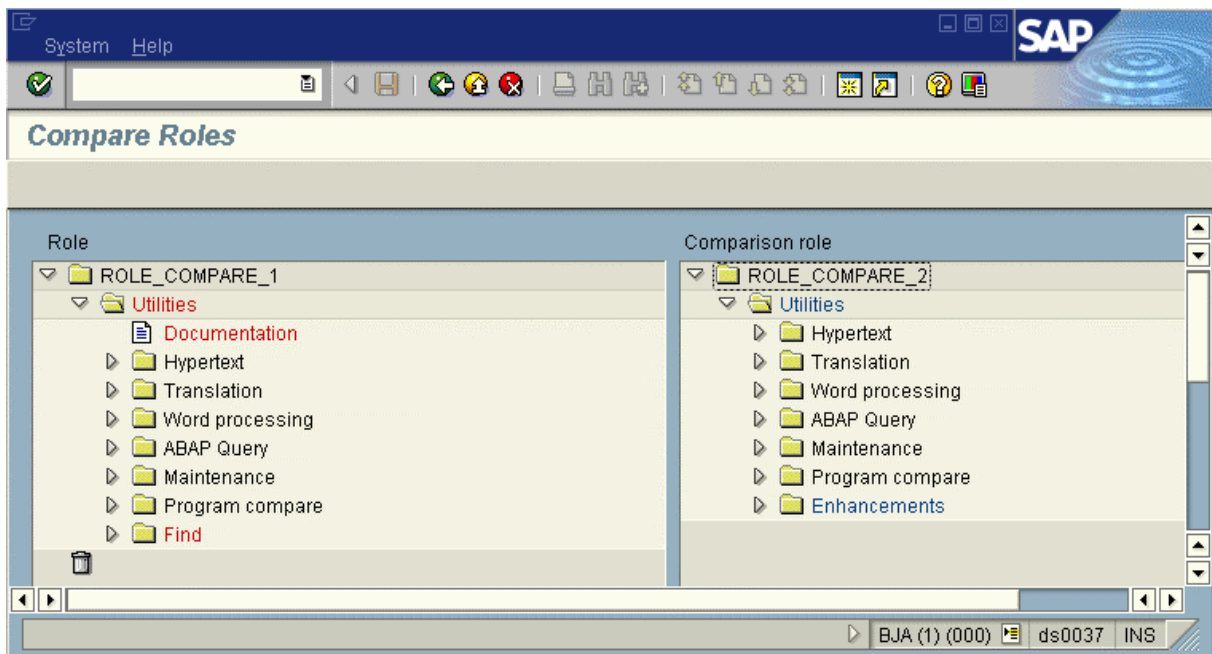
Role comparison example:

1. Choose *Environment* → *Role comparison tool* in role maintenance, or the transaction `ROLE_CMP`.
2. Enter the name of the role to be compared in the *Role* input field. Enter the comparison role.



The screenshot shows the input fields for the role comparison tool. The 'Rolle' field contains 'ROLE\_COMPARE\_1'. Below it, there are four radio buttons: 'Comparison role' (selected), 'Comparison destination', 'Reference role', and 'Old customer role'. The 'Comparison role' field contains 'ROLE\_COMPARE\_2'.

3. Choose *Compare*.



## Transport/Distribute Roles

Two entries in the menu of roles to be compared are output in red. This means that two entries have been added in comparison with the role *Role\_Compare\_2*. You can select and delete these entries.

The entry *Business Add-Ins* in the role *Role\_Compare\_2* is displayed in blue. This entry is missing in the role to be adjusted and can be copied to the appropriate place in the role to be adjusted by Drag & Drop.

4. Save your entries. You have created maintenance version.

You can discard the comparison in the initial screen of the transaction with *Role* → *Delete maintenance vers.*

5. Choose *Activate* to create an active version of the compared role.

## Transport/Distribute Roles

### Transport Roles

You use Transaction PFCG to transport a role. Enter the role and choose *Transport*. The system displays a dialog box that queries whether the user assignment should also be transported. Next, enter a transport request. The role is entered in a Customizing request. Use Transaction SE10 to display this.

The authorization profiles are transported along with the roles. Unlike in previous releases, the profiles no longer have to be regenerated in the target system using Transaction SUPC. However, you must compare the user master records for all roles that are imported into the target system.

If the user assignments are also transported, they will replace the entire user assignment of roles in the target system. If you want to lock a system against importing user assignments of roles, you can specify this in the Customizing table PRGN\_CUST. You maintain this using Transaction SM30. Add the line USER\_REL\_IMPORT and the value NO.



You should only transport user assignments to roles if you are not using central user administration.

After the import into the target system, you must compare the user master records for all roles involved. You can do this in two ways:

- Start report PFCG\_TIME\_DEPENDENCY
- In Transaction PFCG, choose *Goto* → *Mass compare*. Enter the role in the *Role* field. Choose *Complete compare* and start the report.

You can also prevent authorization profiles from being transported with the roles using a Customizing entry. In the transport source system, make an entry in table PRGN\_CUST called PROFILE\_TRANSPORT with the value NO. In this case, you must regenerate the profiles in the target system using Transaction SUPC.

## Distribute Roles

You can distribute roles in the *Menu* tab in the role maintenance if the target system has Release 4.6C.

## Upload/Download Roles

To upload or download a role, choose *Role* → *Upload* or *Role* → *Download* in the role maintenance.

Role upload loads all role data, including authorization data from a file into the SAP System. The role user assignment and the generated role profile are not loaded. The authorization profile must be regenerated after the upload.

You can save several roles on the PC with *Environment* → *Bulk download* in the role maintenance initial screen.

To avoid inconsistencies, all roles from which a role is derived are also downloaded. When you download composite roles, all the roles which they contain are also downloaded.

## Role Maintenance: Example

### Prerequisites

You are using the SD and MM applications but not HR or HR-ORG.

You are not using warehouse management within materials management.

Your company has five plants and you want to create material master data for them. A separate employee is responsible for each plant, who must not be able to change the data for other plants.



In order to understand this scenario and to be able to adapt it for your own purposes, you will need a basic knowledge of the SAP authorization concept, authorization objects, authorizations and authorization profiles.

The following assumes that none of the predefined user roles satisfies your requirements.

### Procedure

#### Preparation

##### Activate the Profile Generator and permit authorization checks to be suppressed

The system parameter `auth/no_check_in_some_cases` must be set to the value 'X'. This is the case for new installations.

Check the setting in your system using report RSPARAM.

---

**Role Maintenance: Example****Copy SAP default settings for check indicators and authorization field values**

Copy the SAP default check indicator settings for the authorization objects in transactions and the authorization field values for the Profile Generator using Transaction SU25.

You can then edit the default check indicators using Transaction SU24.

For more information, see [Preparatory Steps \[Page 76\]](#).

**Creating and Maintaining an Authorization Profile for a User**

Create a user-specific menu with appropriate authorizations.

The user needs to be able to:

- Maintain material master data for plant 0001 in company code 0001, all sales organizations and distribution channels
- Display material master data for all plants and company codes.

The user needs a range of authorizations to be able to do this. These are grouped together in an authorization profile.

To create an authorization profile for a user, do the following:

1. Create a role and generate an authorization profile
2. Assign the role to a user
3. Change the role (optional)
4. Change the check indicator defaults (optional)
5. Copy the general authorizations from SAP defaults (optional)
6. Regenerate the Authorization Profile Following Changes
7. Check the authorization profile

These steps are described in detail below.

**1. Create a role and generate an authorization profile**

You use roles to define the functions (transactions) for which a user receives authorizations.

1. On the *User maintenance: Initial screen* (Transaction SU01), choose *Environment* → *Maintain role*.
2. Create a role. Enter MATST\_0001 as the identification code and choose *Create*.
3. On the following screen, enter an appropriate description.
4. Choose the *Menu* tab and *SAP Menu*.
5. Expand the *Logistics, Materials management* and *Material master* levels.
6. Flag the checkbox next to *Material*. If you expand this branch further, the transaction which you have selected is displayed: including *Create/Display/Change material*.
7. Confirm your selection. The system now compiles the authorization data using the transactions you have selected.
8. Under the *Authorizations* tab, choose *Change authorization data*.

## Role Maintenance: Example

9. In the next dialog box, you are required to maintain the organizational levels. Organizational levels are fields in the authorization system, determined by SAP, that relate to the enterprise structure. These fields occur in many authorizations. You only need to maintain them once. This is done in the *Maintain organizational levels* dialog box.

Corresponding to our scenario, you would need to enter the following values (each time in the *From* field):

- Company code: 0001
- Warehouse number / complex (no entry since there is no warehouse management.
- Sales organization: \* (all)
- Distribution channel: \* (all)
- Plant: 0001

Choose *Enter*.

10. The authorization data is displayed hierarchically in the following screen: the role at the highest level, the object classes of the authorization objects for this role below.

Expand a few levels of the hierarchy. By choosing *Color legend*, you can display an explanation of the colors used in the authorization component hierarchy.

At the lowest level for example are the authorization field values: most fields have default values, either from SAP, or your organizational level values.

The traffic lights indicate whether there are fields whose values you have not yet maintained.

Red - You have not maintained the organizational levels.

Yellow: - You have not assigned values to fields (not organizational levels).

11. Expand the levels with red traffic lights: this includes an authorization for the object *Material master record: Warehouse number*. Since you are not using warehouse management in your company, no employee needs authorization to maintain this data.

12. Deactivate this authorization by choosing the relevant icon.

The authorization is flagged as *Inactive*. When you generate authorization profiles later, this authorization will not be copied into the profile.

There are now no more red traffic lights, since no active authorizations with unmaintained organizational levels remain.

13. There are, however, a lot of yellow traffic lights. For each of these you need to supply values in the authorization fields by choosing *Maintain*.

You can display help as follows:

By double-clicking the text of an authorization object

By double-clicking the text of an authorization field

14. Assign full authorization

To assign full authorization (\*), click on the star symbol next to an authorization field.

You can assign full authorization for all unmaintained (empty, open) fields in an organizational level by clicking on the traffic light. Once you have confirmed the

## Role Maintenance: Example

operation, full authorization (\*) is assigned for all empty fields in the subordinate levels of the hierarchy. Note how the traffic light reacts.

You can display detailed information on the individual icons by choosing *Color legend*.

15. When you have finished maintaining the data, save your changes. Here you can also change the default name for the authorization profile to be generated.
16. Generate the authorization profile by choosing *Generate*. To do this, you need the appropriate authorization. An active authorization profile is generated from the authorization data.

### 2. Assign roles and authorization profiles to a user

Assign role MATST\_0001 to users by entering names in the lists displayed under the Users tab. These users have the proper authorizations to execute the role transactions. See the online documentation for more information on assigning users in *Users*.



The generated profile is not entered in the user master record until the user master records have been compared. To do this, choose *Compare users*.

You can also assign a role to a user in the user maintenance transaction (SU01) in *Roles*. For more information, see [Assigning roles \[Page 15\]](#).

Log onto the system again with the user name that you have entered. The user should now have all of the authorizations necessary to maintain material masters in plant 0001 / company code 0001. It should also be possible to display data for all plants. This does not yet work.

### 3. Change the role (optional)

You change a role as follows:

1. In the initial screen of role maintenance, enter the name of the role you want to change and choose *Change*.
2. By choosing *Menu* and *Menu selection*, you can also activate the menu functions *Stock overview*, *Close period*, *Allow posting to a previous period*. Save your entries.
3. Under the *Authorizations* tab, choose *Authorization data* to access authorization maintenance. Two new organizational levels have now appeared in the dialog box: *Purchasing group* and *Purchasing organization*. Maintain these (enter \* for example) and choose *Continue*.

Some new authorizations have been added to the group because new functions have been added. These are marked as *New*. Some of these will already contain values, others will need to be maintained manually (yellow traffic light). The warehouse management authorization is still inactive. New authorizations (for the period closing program, for example) may already be filled if they only affect organizational levels that already contain values.

If you also want to assign authorization to display data for all plants, proceed as follows:

1. Expand the authorization for the *Material Master: Plant* object. Choose *Copy* to copy the authorization.

## Role Maintenance: Example

2. Maintain the activities in the authorization you have copied. Delete all authorizations except *Display*.
3. Maintain the *Plant* field by choosing the field maintenance symbol. Choose *Full authorization*.  
Notice that the authorization status has changed to *Changed*. This means that you have changed activities and / or organizational levels that no longer correspond to the default authorizations for the selected functions.



Note that when you change an organizational level by choosing *Org. Levels*, this affects all fields in the organizational level. Exception fields whose status have changed.

If, on the other hand, you maintain an organizational level by choosing the maintain field icon, the changes only apply to the field. The field then has the status *Changed*.

4. Generate the authorization profile.

#### 4. Change the check indicator defaults (optional)

You will have noticed that you need to maintain the warehouse management data in order to set the red and yellow traffic lights to green. You can avoid this by changing the transaction defaults.

1. To do this, call Transaction SU24.
2. Choose *Edit check indicators in all transactions* and enter M\_MATE\_LGN as the object. Choose *Execute*.
3. On the next screen, the system displays all the transactions which check this authorization object. You can assign the [Check Indicators \[Ext.\]](#) globally for the object. In this case it is a good idea to check this object in all transactions, but not to copy the defaults into the Profile Generator.

Select all transactions, set the check indicator in the top line to P and choose *Save*. All transactions are set to P. Save the data.

4. Return to maintaining role MATST\_0001. In *Authorizations*, choose *Change authorization data*. You can see from the overview that all data for the M\_MATE\_LGN authorization object has disappeared.
5. You can also change the check indicator for each individual transaction. For example, from the initial screen of Transaction SU24, enter Transaction MMPV *Close Periods*. If you do not want the default value 51 *Initialize* for object M\_MATE\_PER *Material master: Allow backposting* to be copied into the role, change the proposal for transaction MMPV by maintaining the field values. You can reactivate the SAP defaults at any time, restoring the default values delivered when you installed the system.

It is sensible to change the defaults whenever several roles are affected, whether they already exist (and must as such then be compared) or you will create in the future.

#### 5. Copy the general authorizations from SAP defaults (optional)

Notice that the generated profile does not give users general authorizations such as those required for printing. It does not make sense to copy general authorizations to each transaction with the check indicator CM.

## Role Maintenance: Example

Instead, you can do either of the following:

1. Create a role which only contains general authorizations (such as printing). Then assign this role to all users. This is the best thing to do if all users are to be allowed to print from any printer, for example.

Then compare the user master records.

2. Use a template to import the required objects into the role and then maintain missing field contents. This is the best thing to do if each user assigned to a role may use only one particular printer, for example.

In the authorization data maintenance, choose *Edit* → *Insert authorizations* → *From template*. Choose the SAP\_PRINT template. The system inserts authorization data, which you must then complete yourself (printers to be used, and so on).

If you want to create your own templates, choose *Edit templates* in Transaction SU24. You need the authorization *User master maintenance: User groups*, S\_USER\_GRP. You can create your own templates or you can copy the SAP templates and edit them. Unlike changes to defaults, changes to templates are not passed on when you compare roles. Your own templates must not begin with S.

### 6. Regenerate the Authorization Profile Following Changes

Regenerate the authorization profile so that your changes take effect in the system.

### 7. Check the authorization profile

Test your generated authorization profile

If any authorizations are missing or superfluous, you have two options:

1. Change the role: change activities, create authorizations manually, deactivate authorizations
2. Change the defaults using Transaction SU24 as described above and compare the roles.

If an authorization check fails during a transaction, you can see which authorization is missing by choosing *System* → *Utilities* → *Display auth. check* (Transaction SU53).

Test this example until you are happy with the result and the user can perform exactly the correct action in the plant/company code 0001. Change the organizational level to plant 0002 and company code 0002 and generate the authorization profile. You can then assign this role to the users who are to execute material master maintenance for plant 0002.

## Installing a new module

Suppose you later want to install warehouse management. You need to undo all the changes you have made that affect authorization object M\_MATE\_LGN.

You should then check whether the functions in your role are still correct. Is the menu selection still current, for example? Always compare your authorization data.



## Role Maintenance: Tips and Tricks

### Limiting Activities by Time

Even if you are not using HR-Org, you can still take advantage of the option to assign roles to users for a limited period of time. This is useful, for example for your end of year procedure, where inventory activities should only be permitted for a limited time.

Choose *Tools* → *Administration* → *User maintenance* → *Roles*.

Under the tab *User*, you can set the assignment validity period.



To put a time-delimited assignment of an activity group to a user master record into effect, you must first execute a comparison.

The authorization profile is only entered or deleted in the user master record automatically if you have scheduled the background report to run periodically.

Job scheduling is also important for ensuring role consistency after an import.

SAP recommends that you schedule background program `PFCG_TIME_DEPENDENCY` for these cases.

### User assignment

Never insert generated profiles directly into the user master record (Transaction SU01). Assign the role to the user in the *Roles* tab in transaction SU01 or choose the *User* tab in role maintenance (PFCG) and enter the user to whom you want to assign the role or profile.

If you then compare the user master records, the system inserts the generated profile in the user master record.

### Do not assign any authorizations for modules you have not yet installed

If you intend to gradually add modules to your system, it is important you do not assign any authorizations for those modules you have not yet installed. This ensures that you cannot accidentally change data in your production system you may need at a later stage.

Leave the corresponding authorizations or organizational levels open. Do not set the [Check Indicator \[Ext.\]](#) in Transaction SU24 to *No check*.

### Initial authorization assignment

You want to create a user in the test system who can do “almost anything”: typically, such users cannot create a user master record or change authorization profiles.

The fastest way to set up this user is as follows:

1. Create a role.
2. In *Authorizations*, choose *Change authorization data* and then *Edit* → *Insert* → *Full authorization*.
3. Expand the *Basis administration* object class.  
This contains the authorization objects generally regarded as critical.

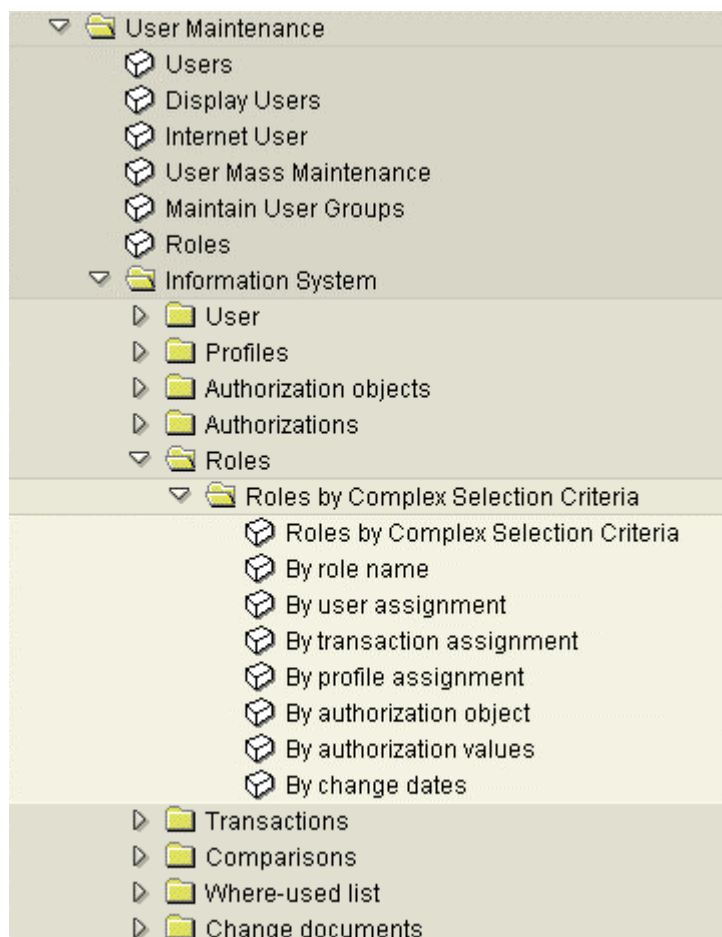
## Using the Infosystem

4. Deactivate all authorizations which begin with *User master maintenance* and any others which you regard as critical. You need the authorization *User master maintenance: User groups* (S\_USER\_GRP) with the value \* in the fields CLASS and ACTVT for transaction SU24.
5. Generate the profile and assign the authorizations to a user under *User*.
6. You assign the role you have just created to users entering them in *Role*.

## Using the Infosystem

Go to the info system from the SAP menu in SAP Easy Access with *Tools* → *Administration* → *User maintenance* → *Infosystem* or with *Info* → *Infosystem* in the user maintenance.

You can specify selection criteria for one or more of the following objects in the menu:



## Reducing the Scope of Authorization Checks

When SAP transactions are executed, a large number of [Authorization Objects \[Ext.\]](#) are often checked, since the transaction calls other work areas in the background. In order for these checks to be executed successfully, the user in question must have the appropriate authorizations. This results in some users having more authorizations than they strictly need. It also leads to an increased maintenance workload.

For an authorization check to be executed, it must be included in the source code of a transaction and must not be explicitly exempt from the check.

You can suppress authorization checks without changing the program code, as check indicators control authorization checks.

You also use check indicators to control which objects appear in the [Profile Generator \[Page 36\]](#) and which field values are displayed there for editing before the authorization profiles are generated automatically.

SAP supplies defaults for check indicator and authorization field values, which you should copy. You can then edit these copied defaults. You should only do this once you have defined your company's authorization concept.

You can reduce authorization checks within a transaction or exclude an authorization object globally from the check.

For more information, see:

[Preparatory Steps \[Page 76\]](#)

[Globally Deactivating Authorization Checks \[Page 77\]](#)

[Reducing Authorization Checks in Transactions \[Page 77\]](#)

[Editing Templates for General Authorizations \[Page 79\]](#)

[Comparing Check Indicators and Field Values After a Release Upgrade \[Page 80\]](#)



Authorization objects from the Basis (S\_\*) and Human Resource Management applications (P\_\*, PLOG) **cannot** be excluded from authorization checks. The field values for these objects are always checked.

You cannot exclude authorization objects used in **parameter transactions** from a check directly, only using the corresponding target transaction.

## Preparatory Steps

# Preparatory Steps

When you activate the Profile Generator, you permit specified authorization checks to be deactivated. The Profile Generator is active in the standard system (the system profile parameter `auth/no_check_in_some_cases` is set).

This setting has the following effect:

- When a transaction is called, the system always checks to see whether the authorization checks contained within it are to be suppressed.
- The authorization Profile Generator is activated. The system displays *Authorizations* on the initial screen for Transaction PFCG (*Role Maintenance*).

Perform the following steps in the Implementation Guide (IMG):

### 1. Copy SAP default settings for check indicators and authorization field values

Using Transaction SU25 (step 1), copy the default values delivered by SAP. This is how you import the SAP check indicator default values for the authorization objects within a transaction, and the authorization field values for the Profile Generator into the customer tables (tables USOBX\_C and USOBT\_C). You can edit these in Transaction SU24.

You can change both configurations to meet your requirements.

To import an upgrade, follow steps 2a to 2d.



It may take a few minutes to copy the SAP defaults into the customer tables.

See the documentation in Transaction SU25.

### 2. Schedule Background Job for Time Limits

You can set a time limit on the assignment of users to roles. To ensure that these changes are reflected in the user master record, you need to schedule a background job to make the relevant adjustments daily.

See [Comparing user master record profiles with roles \[Page 27\]](#).

To maintain the default check indicator settings, use Transaction SU24 (see the following topics). To do this you need the *User Master Maintenance: User Groups* (S\_USER\_GRP) authorization, with the value "\*" in the CLASS and ACTVT fields.

You can edit the default authorizations for the Profile Generator on the initial screen of the Profile Generator (see [Elements in the Browser View \[Ext.\]](#)).

## Globally Deactivating Authorization Checks

You can globally deactivate authorization checks with Transaction AUTH\_SWITCH\_OBJECTS. The system does not execute any authorization checks for deactivated authorization objects.

You deactivate authorization objects in the tree display by selecting the checkbox to the left of the object. The deactivated authorization objects are then displayed in red. The authorization checks are not ignored in the system until you save your settings.



You cannot globally deactivate authorization objects that begin with "S\_" (Basis) or "P\_" (HR) in Transaction AUTH\_SWITCH\_OBJECTS.

Globally deactivating authorization checks considerably reduces authorization maintenance. The system does not insert any authorization data in the Profile Generator for deactivated authorization objects. With Release upgrades, transactions whose authorization data is to be postprocessed are not displayed for postprocessing if the corresponding authorization object is globally deactivated.

If you activate authorization objects that were previously deactivated, note that you may have to postprocess the authorization data for many roles.

If you reactivate authorization objects, these objects are not contained in any roles. In this case, call Transaction PCFG and choose *Read old status and compare with the new data* in the tab *Authorizations in expert mode to generate profiles*. Maintain any authorization values that are missing and then regenerate the profile.

You can transport the settings in Transaction AUTH\_SWITCH\_OBJECTS. During the transport, for reasons of security the system transports the inactive (saved) version of the deactivated authorization objects. You activate the deactivated authorization objects by choosing *Authorization objects* → *Activate data*.



To save or activate deactivated authorization objects, you require authorization for object S\_USER\_OBJ. For reasons of security, you should assign authorizations for saving and activating the deactivated authorization objects for various users. It makes sense to deactivate the authorization checks only if at least two people agree on this.



The option to globally deactivate authorization checks is controlled by system parameter auth/object\_disabling\_active. This parameter is set by default.

## Reducing Authorization Checks in Transactions

You can display the authorization objects associated with each transaction. You can also exclude any of these authorization objects individually from the authorization check. You should have a thorough knowledge of this application and its context before you start.

Proceed as follows:

## Reducing Authorization Checks in Transactions

1. From the initial screen of Transaction *SU24*, choose *Maintain check indicators for transaction codes*.
2. Enter either a single transaction code (for example, *SE01*) or an interval for a range of codes (for example, *SE10* to *SE38*).

The system displays either a single transaction or a list of transactions. See the note below regarding parameter transactions. If you are dealing with a parameter transaction, the target transaction appears in the right hand column under *Tcode (original)*.

3. Select the required transaction and then choose the appropriate pushbutton.

The system displays a list of the authorization objects involved along with their [Check Indicators \[Ext.\]](#).

Using the pushbuttons, you can display field values for individual objects as well as the SAP-default values for check indicators. SAP-default values you have changed are displayed in color.

Choose the *Info Auth. obj* pushbutton to display a help text for the object that is currently marked.

4. Set the check indicator to *N* to stop the check. See the note below regarding parameter transactions.
5. Save your settings.



The default values and the check indicator of an authorization object are important for the Profile Generator. These values are only displayed for changing in the Profile Generator if you have set the check indicator to *CM* (check / maintain).

If you have set authorization checks for your own transactions, you need to enter the authorization objects which you have used into Transaction *SU24* manually and also maintain the check indicators.



Authorization objects used in **parameter transactions** cannot be excluded from a check directly, only using the authorization objects in the corresponding target transaction.

If you want to set the check indicator of parameter Transaction *XYZP* to *N*, you need to change the check indicator for the target Transaction *XYZE*. You can find the name of this transaction in the right-hand column of the transaction overview in Transaction *SU24*. If you double-click the transaction code, the system goes directly to check indicator maintenance.

If the authorization object for parameter Transaction *XYZP* is set to *C* (check) but under the target transaction it is set to *CM* (check/maintain), the field values which have been maintained for *XYZE* will be proposed in the Profile Generator. If the authorization object is also set to *CM* in *XYZP*, the field values maintained for *XYZP* will be proposed in the Profile Generator, and the entries for *XYZE* will be overridden.

When using Transaction *SU24* for parameter transactions you can only maintain and/or overwrite the field values of the target transaction.

## Editing Templates for General Authorizations

It does not make sense to include general authorizations (printing, archiving and so on) in every transaction.

You can adopt authorization objects from templates created by SAP when you maintain roles (transaction PFCG).

You can then maintain these templates from the initial screen of Transaction SU24. Choose *Edit templates*.

The system then displays a list of the SAP templates. These cannot be changed directly.

You can, however, copy these and use them as a pattern for your own settings, or you can create completely new templates. You need the authorization *User master maintenance: User groups* (S\_USER\_GRP).

The names of SAP templates begin with *s*. If you create any templates yourself, they should not begin with *s*. SAP\_ALL contains all authorizations.

Ensure that changes to templates are not passed on when you compare roles.

If you want to transport your template you must specify a development class when you create it (not \$TMP, local objects). You can find details on this in the **BC - Change and Transport Organizer** documentation in [Maintaining Development Classes \[Ext.\]](#).



You want to create a Basis user who can do “almost anything”: such users can typically not create user master records or change authorization profiles.

Proceed as follows:

- Create a role by choosing *User maintenance* → *Roles*
- Do not enter any transactions, choose *Authorizations* and then *Change authorization data*.
- Do not copy any templates, but choose *Edit* → *Add authorization*. → *Full authorization*.
- Expand the *Basis administration* object class.  
Here you find the authorizations which are generally regarded as critical.
- Deactivate all authorizations which begin with user master maintenance and any others which you regard as critical.
- Using the Profile Generator, generate a new profile and save it under a new name (refer to [Naming Convention for Pre-Defined Profiles \[Page 90\]](#)

If you choose *User Maintenance* → *Users*, you can assign the role you have just created to the user. See [Assigning roles \[Page 15\]](#).

---

**Comparing Check Indicators/Field Values After Upgrade**

## Comparing Check Indicators/Field Values After Upgrade

After a Release upgrade you can compare the default check indicators and the field values of the previous and new Releases. To do this, call Transaction SU25 (steps 2a to 2d).

If you have made changes to check indicators or field values in Transaction SU24, you can compare these with the new SAP default values. The previous and new settings are displayed in a list. You can decide whether you want to use each new setting or retain the previous one.

In the next step, the system displays a list of roles affected by changes to the authorization data. Edit and regenerate their authorization profiles.



To save time if you utilize a large number of roles, you can skip editing and assign the profile SAP\_NEW to the users manually. The profile SAP\_NEW is delivered with every new Release and contains the authorizations for all new checks in existing transactions. Remove any subprofiles from the profile SAP\_NEW that are not relevant to your users. You can tailor the authorization profiles the next time they need to be changed (for example, when the role menu changes).

Step 2d display a list all roles containing any transactions that have been replaced by one or more other transactions.

In the last section, you can adjust authorization checks. This includes changing check indicators (Transaction SU24) and globally switching off authorization objects.

You can create roles from manually created authorization profiles in step 6. You must then adjust and check them.

## Transporting Authorization Components

There are two different processes for transporting authorization components, roles and user master records, depending on the type of transport:

- Transports between clients (within an SAP System)
- Transports between R/3 Systems

The procedures for both kinds of transport are detailed below.

### Transport Between Clients

User master records and authorization components are client-dependent. You need to maintain separate user master records and authorization components for each client in your R/3 System.



---

## Transporting Authorization Components

In the target client, choose *Tools* → *Administration* → *System administration, Administration* → *Client admin.* → *Client copy* → *Local copy* (Transaction SCCL). Here you can transport user master records and authorization profiles from other clients. To do this, enter the profile SAP\_USER or choose from the possible entries.



Schedule the transport for background processing during the night. This ensures that data remains consistent.

## Transport Between SAP Systems

You can copy authorization components, roles and user master records from one SAP System to another. The method of transport depends on the component that you want to transport.

## Transport Roles

You use Transaction PFCG to transport a role. Enter the role and choose *Transport*. The system displays a dialog box that queries whether the user assignment and the personalization data should also be transported. Next, enter a transport request. The role is entered in a Customizing request. Use Transaction SE10 to display this.

The authorization profiles are transported along with the roles. Unlike in previous releases, the profiles no longer have to be regenerated in the target system using Transaction SUPC. However, you must compare the user master records for all roles that are imported into the target system.

If the user assignments are also transported, they will replace the entire user assignment of roles in the target system. If you want to lock a system against importing user assignments of roles, you can specify this in the Customizing table PRGN\_CUST. You maintain this using Transaction SM30. Add the line USER\_REL\_IMPORT and the value NO.



You should only transport user assignments to roles if you are not using central user administration.

After the import into the target system, you must compare the user master records for all roles involved. You can do this in two ways:

- Start report PFCG\_TIME\_DEPENDENCY
- In Transaction PFCG, choose *Goto* → *Mass compare*. Enter the role in the *Role* field. Choose *Complete compare* and start the report.

You can also prevent authorization profiles from being transported with the roles using a Customizing entry. In the transport source system, make an entry in table PRGN\_CUST called PROFILE\_TRANSPORT with the value NO. In this case, you must regenerate the profiles in the target system using Transaction SUPC.

## Transport Manually-Created Profile

To transport selected profiles, proceed as follows:

1. Choose *Tools* → *Administration* → *User maintenance* → *Manual maintenance* → *Edit profiles manually*. Create a profile list and then choose *Profile* → *Transport*.
2. Select the profiles you want to transport in the list displayed. You can also select all profiles.

## Transporting Authorization Components

3. Enter the transport request number for each profile or profile group in the dialog box.
4. The system asks whether you want to transport just the profile, or the authorizations it contains as well. You can either transport the profile by itself, or include all of its components in the transport request.

The system also transports the documentation for the profiles and authorizations.

5. When you have finished your selection, you can execute your transport request using the Workbench Organizer.

## Transport Manually-Created Authorizations

The procedure for transporting authorizations is the same. First start the authorization maintenance function. Do this by choosing *User maintenance* → *Authorization*. Choose an object class and then *Authorization* → *Transport*.

## Transporting Authorization Objects and Authorization Object Classes

Whenever you create or change authorization object classes, the system displays a dialog box in which you can enter a change request. Release this request for the desired target system.

## Transporting User Master Records

You copy user master records using either the tools described above or via central user administration.

## Transporting Check Indicators and Field Values

You can use Transaction SU25 (Step 3) to transport all check indicators and field values.



Note that the transport overwrites all existing check indicators and field values in the target system.

You can use Transaction SU24 to maintain individual check indicators. You can use the Workbench Organizer to record your changes. By executing the corresponding transport request, you distribute your check indicators to other systems.

## Transporting Templates

All SAP templates are automatically identical in all systems following an upgrade. You cannot change SAP templates.

The Workbench Organizer records changes to your own templates. Transport the request. The objects in the transport request have the following syntax:

```
R3TR SUSV <Template Name>
```

The system transports the template name (in all languages) as well as the maintained data.

## Transporting Globally Deactivated Authorization Checks

For information on transporting globally deactivated authorization checks, see [Globally Deactivating Authorization Checks](#)

## Analyzing Authorization Checks

Should you not find any documentation for an authorization, the system offers two ways to find out which authorizations are required:

- System trace

You can use the system trace to record authorization checks in your own sessions and in other users' sessions. The trace records each authorization object that is tested, along with the object's fields and the values tested.

For more information, see [Tracing Authorizations with the System Trace \[Page 83\]](#).

- Authorization error analysis

By entering Transaction SU53 in the command field, you can analyze an access-denied error in your system that just occurred.

You can use Transaction SU53 from any of your sessions, not just the one in which the error occurred. You cannot analyze an authorization error in another user's logon session from your own session.

Example: Upon selecting a function, the system responds with the message "You are not authorized for this function." If you enter SU53 or InSU53 in the command field, the system displays the authorization object that was just tested and the authorizations, if any, that you possess for that object.



To deactivate this function, set the system profile parameter `auth/check_value_write_on` to 0.

## Analyzing Authorizations using the System Trace

To start tracing authorizations, proceed as follows:

1. Choose *Tools* → *Administration, Monitor* → *Traces* → *System trace*.
2. Choose the trace component *Authorization check* and then *Trace on*. The system then automatically writes the trace to disk.
3. To restrict the system trace to your own sessions, choose *Edit* → *Filter* → *General*. In the dialog box displayed, enter your user ID in the field *Trace for user only*.
4. After you have completed your analysis, choose *Trace off*.
5. To display the results of the analysis, choose *Goto* → *Files/Analysis* or choose the pushbutton *File list*. Position the cursor on the file that you want to analyze and choose *Analyze file*.

## Authorization Checks in Your Own Developments

You will see authorization tests entries in the format <Authorization object>:<Field>=<Value tested>.

You can display a formatted view of an authorization check by double-clicking an entry. (You may need to scroll down in the display to reach the formatted view of the entry.)

If no authorization entries exist or the system displays the message *Authorization entries skipped*, check that you have set the trace switches correctly. If the switches are correct, then choose *Trace file* → *Analyze file* and ensure that *Trace for authorization checks* is selected.

## Authorization Checks in Your Own Developments

Each time a transaction is started, the system automatically checks for authorization object S\_TCODE. This check is also executed for any transactions that you created yourself.

If you use the [Profile Generator \[Page 36\]](#) to generate your authorization profiles automatically, the authorizations for the authorization object S\_TCODE are contained in the profiles.

Furthermore, you can add your own authorization checks to protect critical points in your ABAP programs.



The authorization check is not executed when the transaction is called indirectly, that is, from another transaction. Authorizations are not checked, for example, if a transaction calls another with the CALL TRANSACTION statement.

You should make sure that any security-critical transactions you call are always subject to authority checks.

## Adding Authorization Checks to Programs

In order to maintain authorization objects and fields, you need access to the authorization object *Authorizations* (S\_USER\_AUT).

To add authorization checks to programs, you need to do the following:

1. [Create an Authorization Field \[Page 85\]](#)
2. [Create an Authorization Object \[Page 85\]](#)
3. [Assign an Authorization Object to an Object Class \[Page 85\]](#)
4. Program authority checks

Use the ABAP AUTHORITY-CHECK statement. Specify alphabetic values in uppercase letters: ABC. Test values from user master records are converted to uppercase before being passed to AUTHORITY-CHECK.

See the ABAP programming documentation for more information.

## Creating Authorization Fields

In authorization objects, authorization fields represent the values to be tested during authorization checks.

To create authorization fields, choose *Tools* → *ABAP Workbench* → *Development* → *Other Tools* → *Authorization Objects* → *Fields*.

To create an authorization field, proceed as follows:

1. Choose *Create authorization field*.
2. On the next screen, enter the name of the field. Field names must be unique and must begin with the letter Y or Z.
3. Assign a data element from the ABAP Dictionary to the field.
4. If desired, enter a check table for the possible entries. For more information about check tables, see [Connection to the Check Table \[Ext.\]](#). The connection provides possible field values. Values ranges can also be defined using the domain with which a field is associated.

For more information about AUTHORITY-CHECK, see the keyword documentation of the ABAP Editor.



You can often use the fields defined by SAP in your own authorization objects. If you create a new authorization object, you do not need to define your own fields. For example, you can use the SAP field ACTVT in your own authorization objects to represent a wide variety of actions in the system.

## Assigning an Authorization Object to an Object Class

Each authorization object must be assigned to an object class when it is created.

Choose *Tools* → *ABAP Workbench* → *Development* → *Other tools* → *Authorization objects* → *Objects*. You can also create authorization objects in the Object Navigator (SE80).

## Creating / Choosing Object Classes

The system displays a list of existing object classes.

Object classes are organized according to the components of the system.

Before you can create a new object, you must define the object class for the component in which you are working. The objects are not overwritten when you install new releases.

---

## Creating/Maintaining Authorizations/Profiles Manually

You can also define your own object classes. If you do so, select class names that begin with **Y** or **Z** to avoid conflicts with SAP names.

### Creating an Object

Enter a unique object name and the fields that belong to the object. Object names must begin with the letter **Y** or **Z** in accordance with the naming convention for customer-specific objects.

You can enter up to ten authorization fields in an object definition. You must also enter a description of the object and create documentation for it.

Ensure that the object definition matches the **AUTHORITY-CHECK** calls that refer to the object.



Do not change or delete authorization objects defined by SAP. This disables SAP programs that use the objects.

You can regenerate the profile **SAP\_ALL** after creating an authorization object.

For further information, see the documentation in the transaction.

## Creating/Maintaining Authorizations/Profiles Manually

This section describes how to create and maintain authorizations manually.



You can generate authorizations and profiles on the basis of selected transactions. See [Role maintenance \[Page 36\]](#).

[Administration Tasks \[Page 87\]](#)

[Maintaining Authorization Profiles \[Page 87\]](#)

[Maintaining Authorizations \[Page 91\]](#)

[Adding Authorization Checks To Your Own Developments \[Page 84\]](#)

[Analyzing Authorization Checks \[Page 83\]](#)

## Line-oriented Authorizations

### Use

You can restrict access to tables by business organizational units using the line-oriented authorizations introduced in Release 4.6C. You could previously only use the authorization objects **S\_TABU\_DIS** and **S\_TABU\_CLI** to allow or prevent access to complete tables.

The introduction of organizational criteria allows you to restrict user access to parts of a table. The authorization object **S\_TABU\_LIN** has been introduced for this purpose.

One possible use for line-oriented authorizations would be that a user can only display and change the contents of a particular work area, e.g. a country or plant, in a table.

See the IMG documentation under *Basis*® *System administration*® *Users and authorizations*® *Line-oriented authorizations*.

## Administration Tasks

If you want to create and maintain authorizations in the SAP System, you should create and activate two types of authorization components.

- These components are authorizations to allow specific system authorizations.  
Maintain authorizations under *Tools* → *Administration* → *User maintenance* → *Manual maintenance* → *Edit authorizations manually*.
- Authorization profiles, to enter authorizations in user master records.  
Maintain authorization profiles under *Tools* → *Administration* → *User maintenance* → *Manual maintenance* → *Edit profiles manually*.

The SAP System includes predefined authorizations and profiles. These can often be given to your users without modification, which greatly reduces the effort required to maintain authorizations and profiles.

You can also decide how to organize maintaining user master records and authorizations. You can have a single superuser conduct all user and authorization maintenance, or divide maintenance among decentralized administrators. You can have a single superuser conduct all user and authorization maintenance, or divide maintenance among decentralized administrators. See [Organizing User and Authorization Maintenance \[Page 115\]](#).

## Maintaining Authorization Profiles

This section describes how you manually create, maintain, activate, and delete [Authorization Profiles \[Ext.\]](#).



Note that it is faster and easier to create profiles using the Profile Generator.

You access profile maintenance by choosing *Tools* → *Administration* → *User administration* → *Manual maintenance* → *Edit authorization profile manually*..

---

## Simple and Composite Profiles

[Simple and Composite Profiles \[Page 88\]](#)

[Defining Profiles and Authorizations \[Page 88\]](#)

[Alternative Authorizations \[Page 89\]](#)

[Choosing Authorization Objects \[Page 89\]](#)

[Maintaining Composite Profiles \[Page 90\]](#)

[Activating Profiles \[Page 90\]](#)

[Naming Convention for Predefined Profiles \[Page 90\]](#)

## Simple and Composite Profiles

You can manually create two types of profiles:

- Simple (or single-level) profiles contain authorizations. Each authorization is identified by the name of an authorization object and the name of the authorization created for the object.
- Composite profiles contain other profiles. A composite profile assigns all of the simple or composite profiles it contains to a user.

## Defining Profiles and Authorizations

You can maintain both profiles and authorizations from the profile maintenance functions.

Use the default profiles provided by SAP as templates for your own profiles:

1. Use the SAP naming convention to select default profiles for the application with which you are working.

Example: Searching for profiles with **F\_\*** selects profiles for the Financial Accounting application.



From Release 4.5A, SAP recommends you use the Profile Generator to create profiles and copy predefined user roles. Only use the profiles predefined by SAP if the documentation explicitly informs you to do so.

SAP does not guarantee that standard authorizations delivered with the R/3 System will remain the same in future releases or updates. You should therefore make your



own copies of predefined profiles. Otherwise, you must check your authorizations after installing a release or update.

2. Copy the profile that most closely matches the profile you need.

Use a systematic naming convention. You can change the SAP naming convention, for example.

SAP recommends substituting a different character for the underscore found in the second position in SAP profile names. That way, the profile name makes the source of the profile immediately clear.

Example: To create your own profile for customer accounts clerks, you could copy the default profile F\_CUSTOMERS to F: CUSTOMERS. Changing only the second character makes the new profile name unique, but you can easily tell where the profile came from.

3. Maintain the profile and the authorizations it contains.

Delete the authorizations that you do not require by deleting the corresponding lines from the profile.

If you need to change an authorization, then you should first create a copy of it. Delete the original authorization from your profile and insert your copy in its place. You can then edit the authorization by double-clicking on it. Do not edit the original authorization, as your changes may be overwritten when you update your system with a new Release.

You can create new authorizations. Choose *Simple auth.* When you select an object class and an object, existing authorizations are displayed.

4. Activate all the authorizations that you have changed.
5. When you have finished editing authorizations, activate the profile. It is then ready for use.

## Alternative Authorizations

If you want to assign a user alternative authorizations, you can enter a single authorization object in a profile as often as you like. Enter a different authorization each time the object occurs.

The system tests the alternative authorizations using OR logic. If any of the authorizations permits the user's action, the user passes the authorization test. The system uses the first authorization that meets all of the requirements of the access test.

## Choosing Authorization Objects

You can choose the objects of a particular work area or component by copying the predefined profile and modifying it. However you can also use authorization object classes and the information system to find the authorization objects that are used in a particular component of the R/3 System.

---

**Maintaining Composite Profiles**

## Maintaining Composite Profiles

To create or maintain a composite profile, choose *User maintenance* → *Manual Maintenance* → *Edit profile manually*.

Then proceed as follows:

1. Generate a work area (profile list) by choosing *Generate work area*, or entering the name of the composite profile you want to create or maintain.  
The system displays a list of profiles. This list is empty when you create a composite profile.
2. Choose *Create*, *Change*, *Delete* or *Copy*.  
If you choose *Create*, you should then choose the profile type *Composite profile* in the dialog box.
3. From the list of profiles, choose the name of the single or composite profile to be included in the composite profile using *Add profile*. To do this, use the pushbutton, *Add profile*.  
You can add a virtually unlimited number of profiles to a composite profile.  
When creating composite profiles, you can enter profiles that have not yet been created or activated. However, you must create and activate the missing profile(s) before you can activate the composite profile.

## Activate profiles

New or modified profiles must be activated before they can be assigned to users or become effective in the system.

Activation copies the maintenance version of a profile to the active version. If the activated profile already exists in a user master record, the changes to it become effective as each affected user logs onto the system. Changes are not effective for users who are already logged on when the profile is activated.

To activate a profile, choose *Profile* → *Activate* on the *Profile List* screen. If an active version of the profile exists, you will see the active and maintenance versions of the profile so that you can verify the changes.

## Naming Convention for Predefined Profiles

From Release 4.5A, SAP recommends you use the Profile Generator to create profiles and copy predefined user roles. Only use the profiles predefined by SAP if the documentation explicitly informs you to do so.

SAP does not guarantee that standard authorizations delivered with the R/3 System will remain the same in future releases or updates. You should therefore make your own copies of predefined profiles. Otherwise, you must check your authorizations after installing a release or update.

## Naming Your Own Profiles

To avoid conflicts between profiles that you define and those supplied by SAP, you should not use any name that has an \_ (underscore) character in the second position. Substitute the underscore in the second position for a different character of your choice.

## Maintaining Authorizations

This topic describes how you create, edit, activate and delete authorizations. You access authorization maintenance by choosing *Tools* → *Administration* → *User Maintenance* → *Manual Maintenance* → *Edit Authorizations Manually*. You can also maintain authorizations from the profile maintenance screen.

[Creating and Maintaining Authorizations \[Page 91\]](#)

[Entering Values \[Page 91\]](#)

[Activating Authorizations \[Page 93\]](#)

[Naming Conventions for SAP Authorizations \[Page 93\]](#)

## Creating and Maintaining Authorizations

To create or maintain an authorization, proceed as follows:

- Select an authorization object according to class and description.
- Add a new authorization, or choose one from the authorizations that already exist.

A new authorization name should be unique only among the authorizations for the same authorization object.



Generated authorizations (type •) cannot be maintained manually.

## Entering Values

Define or change single values and / or value ranges for each field in the object. A user who has these values is authorized to execute the corresponding actions.

The system automatically displays the fields for which you must define values. A description of each field is included in the display so that you can easily identify its functions.

## Entering Values

You can display the documentation or possible entries for a field by positioning the cursor on the field and choosing *Maintain values* or *Field documentation*. When you maintain values a dialog box appears. Choose the possible entries help (F4) for an overview of the values you can enter here.

## Rules for Entering Values

- Enter single values in *From* fields only. Do not enter any values in the accompanying *To* field.
- Enter value ranges using the formats below.

### Formats for Entering Values in an Authorization

From	To	Authorization
1	3	Values 1, 2, and 3
S_USER*		Any character format beginning with "S_USER"
AB	C*	All values beginning with AB, AC,... or B or C
0	9*	Any numeric value

- To exclude a value from a range, specify multiple ranges that do not include the value. For example, the ranges below allow access to all values except those that begin with the string "S\_U", for S\_USER\_ (user maintenance) authorizations.

### Excluding Values From a Range of Values

From	To	Authorization
A	S_T*	Values beginning with A through S_T
S_V	Z*	Values beginning with S_V through Z

- To authorize a user to leave a field blank, Enter ' ' (a space enclosed in single quotation marks, or ' or simply ' in shorter fields).
- For many fields, you can display the values that may be entered by choosing *Possible entries*.



Cross-system value ranges: If you have a heterogeneous R/3 environment, you should specify value ranges for numbers and letters separately. Example: A to Z and 0 to 9.

You need to define separate ranges as the values are sorted according to the character set used. To include all numbers and letters in a range, for example, you would need different range definitions in ASCII and EBCDIC systems:

- ASCII: the value range 0 to Z\* includes all numbers and letters, as well as some other printable characters
- EBCDIC: the value range A to 9\* includes all numbers and letters.

### Example

The object displayed below controls actions users belonging to a user group may execute:

#### Sample Authorization

Object	Fields	Values
User groups	User master maintenance: User group	S*
	Administrator action	03 (display)

The sample authorization for object *User groups* would allow a user to display any user master record belonging to a group whose name begins with S.

## Activating Authorizations

You must activate new or modified authorizations to make them effective in the system. Activation copies the maintenance version of an authorization to the active version.

An activated authorization becomes effective immediately in all active profiles in which it exists. The authorization is effective even for users who are logged on when the activation takes place.

To activate an authorization, choose *Authorization* → *Activate*.

If an active version of the authorization exists, you will see the active and maintenance versions so that you can verify the changes that you are about to put into effect. You can cancel an activation if the changes are not correct.

## Naming Convention for SAP Authorizations

The R/3 System is supplied with a set of predefined authorizations. You can display the predefined authorizations by using the user and authorization information system.

For predefined authorizations, you can also use the naming convention described in [Predefined Profiles: Naming Convention \[Page 90\]](#).



In any case, SAP recommends that you do not create profiles and authorizations manually. Use the Profile Generator instead.

---

## Central User Administration

# Central User Administration

An SAP system group consists of several SAP Systems with several clients. The same users are frequently created and maintained in each client.

Using central user administration, you can maintain these users centrally in one system. The information is then automatically distributed to the dependent systems.

For more information, see:

[Setting Up Central User Administration \[Page 94\]](#)

[Setup distribution field distribution parameters \[Page 100\]](#)

[Migration of existing users into the central system \[Page 102\]](#)

[Central user distribution \[Page 103\]](#)

[Distribution Logs \[Page 104\]](#)

[Global User Manager \[Page 105\]](#)

## Setting Up Central User Administration

An ALE environment is necessary to distribute the data. It can exchange data and keep it consistent. An ALE system group is used by the central user administration to distribute user data between a central system and systems linked by ALE.

Central user administration data is exchanged asynchronously between the application systems in an ALE environment. This ensures that it still reaches the target system even if it was unreachable when the data was sent.

One system in the central user administration ALE environment is defined as the central system. The links to the subsidiary systems emanate from the central system. The subsidiary systems are not linked to each other.

Perform the following steps to setup the central user administration:

### Create system users

Create a system user. A user account is required for the internal communication between the systems in an ALE group. It is only used internally for this communication and not in dialog. This user must be created in all systems in the ALE environment with the same user name and password. Assign the type *System* and appropriate authorizations (e.g. SAP\_ALL) to the user.

See [Create and maintain user master records \[Page 10\]](#).

### Name logical systems

1. Call the transaction SALE.
2. Choose *Prepare sender and target systems -> Create logical systems -> Name logical system*.
3. To put new logical systems in the list, choose *New entries*.

As the logical system table is cross-client, settings made here apply to all clients in an R/3 System. If the ALE environment only comprises the logical systems of an R/3

---

**Setting Up Central User Administration**

System, you only need to define the logical systems once. For several R/3 Systems, you must setup all logical systems in each instance completely.

4. Enter the short name under by which the system is to be known in the ALE group, in upper-case letters under *Log.system*. Enter a meaningful text name for the logical systems under *Name*.



We recommend a combination of system name and client number for the short name. For example BIZCLNT008 was chosen for the system BIZ and client 008.

Note that you must also enter any logical systems which are not in the current R/3 System. All logical systems must be defined in each R/3 System in the ALE environment.

5. Choose *Save* when you have entered all logical systems.

Naming the logical systems does not assign these logical system names to existing clients in your R/3 Systems.

### Assign logical systems to clients

1. Assign logical systems to clients in the transaction SALE under *Prepare sender and target systems -> Create logical systems -> Assign logical system to a client*. Mark the client to which you want to assign a logical system and choose *Detail*. The system displays the detail screen. In the field *Logical System*, enter the name of the logical system you want to assign to the client. Then save your settings. This is case-sensitive.
2. Assign all central user administration logical systems to a client.

### Define target systems for RFC calls

Define the RFC destinations for the logical systems under *Prepare sender and target systems -> Configure systems in network*. The remote function call is controlled by the RFC destination parameters.



An RFC destination is always created from the client to which you are logged on. To define an RFC link from client 008 to client 322, you must be logged on to client 008. Central user administration RFC links must always be two-way. To define the RFC link completely, you must also logon to client 322 and define client 008 as RFC destination.

1. Enter the RFC destination name. The name of the RFC destination should match the name of the corresponding logical system (e.g:B20CLNT323). This is case-sensitive.
2. Specify link type 3 for links to another R/3 System.
3. Enter the target client number under *Client* and the system user created at the beginning for internal system communication in the ALE environment, under *User* and *Password*. Save your entries.



The top of the screen changes when you save. You can specify whether you want to use load-sharing. This is recommended but not obligatory. Choose *Load-sharing* →

## Setting Up Central User Administration

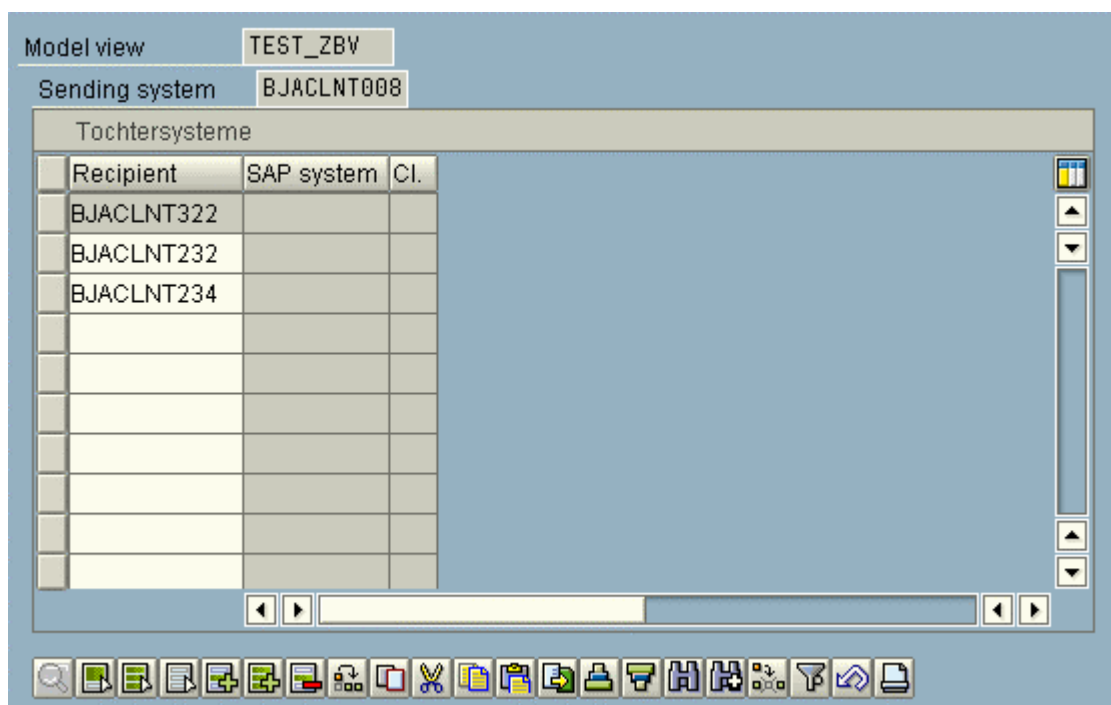
Yes and enter the message server under *Target machine* and the message server system number under *System number*.

Use the transaction RZ03 in the target system to get the target system message server name. Several servers are usually listed. The message server is the one which offers the service M. The message server name is the part of the server name before the first underline. The two-digit number at the end of the server name is the system number.

### Create distribution model

When you have created the ALE environment, create the distribution model. The distribution model describes the ALE message flow between logical systems.

1. Logon to the system which is to be the central system, and call the transaction SCUA.
2. Create a distribution model. Enter a name and choose *Create*. Enter the target system in the next screen.



3. Save your entries.

The following actions are performed automatically when you save:

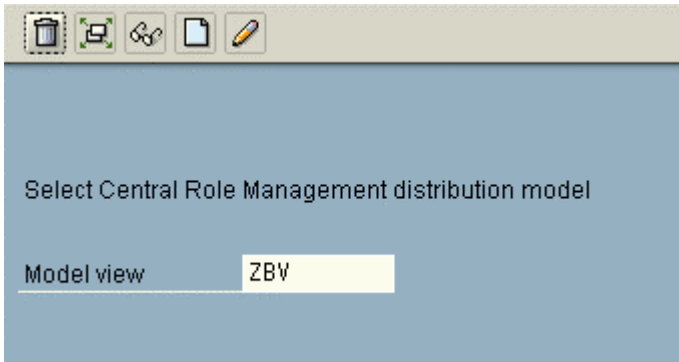
- The message flow is defined for each recipient system by specifying sender and recipient systems and the Business objects USER (create user from models in other systems) or USERCOMPANY (maintain company address) and the method CLONE.
- The partner profiles are generated for the subsidiary systems and the central system.
- The distribution model is sent to the subsidiary systems.

Several partner profile generation logs appear. Check whether the partner profiles were created successfully.




## Setting Up Central User Administration


Save the model view again in the *Maintain system environment* screen to confirm the distribution model as the basis for the central user administration.



The complete distribution model is distributed automatically to all subsidiary systems when you save the model assignment for the central user administration. You cannot create any more users after distribution to the subsidiary systems. A system is now defined as central system and the other systems are subsidiary systems for the central user administration.

If the central user administration is to use another already existing distribution model, delete the model view name with the  icon. Enter another name and save. The distribution model is not deleted, it is no longer the basis for the Central user Administration.

You can delete a distribution model with *Distribution model* → *Delete all data*.

You can also send the distribution model to the subsidiary systems with the  icon.

You can edit distribution models completely in the transaction BD64.



You must partially perform the actions which are performed internally when you save the distribution model in the transaction SCUA manually in Releases before 4.6C, i.e., if you want to create an ALE environment for systems with different Releases, see: [Setting up CUA for systems with different Releases \[Page 98\]](#). This contains background information if you have problems setting up the Central User Administration with transaction SCUA.

## Testing Central User Administration

1. Create a test user in user maintenance (SU01).
2. Choose the *System* tab. Enter the logical name of the central system and all subsidiary systems.
3. Choose the *Roles* tab.
4. Choose *Compare text from subsidiary systems*.



The text comparison is necessary to tell the central system the names of the roles in the subsidiary systems. You can only display and select roles from subsidiary

## Setting-up CUA for Systems with different Releases

systems in the central system from the possible entries help after this step. You cannot assign roles from subsidiary systems manually without a text comparison.

5. Assign a role to the test user in each logical system in the system group. (Enter all logical systems in the *System* column and the role to be assigned to the test user in the *Role* column. One role per system is sufficient for testing).
6. The distribution procedure runs automatically when you save. The user is created with its roles in all defined systems.
7. You can check the result in the transaction SCUL.

### See also:

For information on configuring the system landscape, see documentation [ALE-Introduction \[Ext.\]](#) and [ALE integration technology \[Ext.\]](#).

## Setting-up CUA for Systems with different Releases

As setting up the distribution model in the simplified form with transaction SCUA is only suitable for Release 4.6C systems, the complete Central User Administration setup procedure is described below.

Perform the following activities:

- Create system users
- Name logical systems
- Assign logical systems to clients
- Define target systems for RFC calls

See [Setting up Central User Administration \[Page 94\]](#).

Proceed as follows:

1. Define the system environment in the SAP Reference IMG under *Basis* → *Distribution (ALE)* → *Model and implement Business processes* → *Maintain Distribution Model* (Transaction BD64).

The distribution model is used to specify which applications communicate with each other in your distributed systems. The distribution model contains all of your company's cross-system message flow information. The distribution model consists of several model views. In each model view, you can define related message flows. Each model view is maintained in a central system and distributed from there to the other systems.

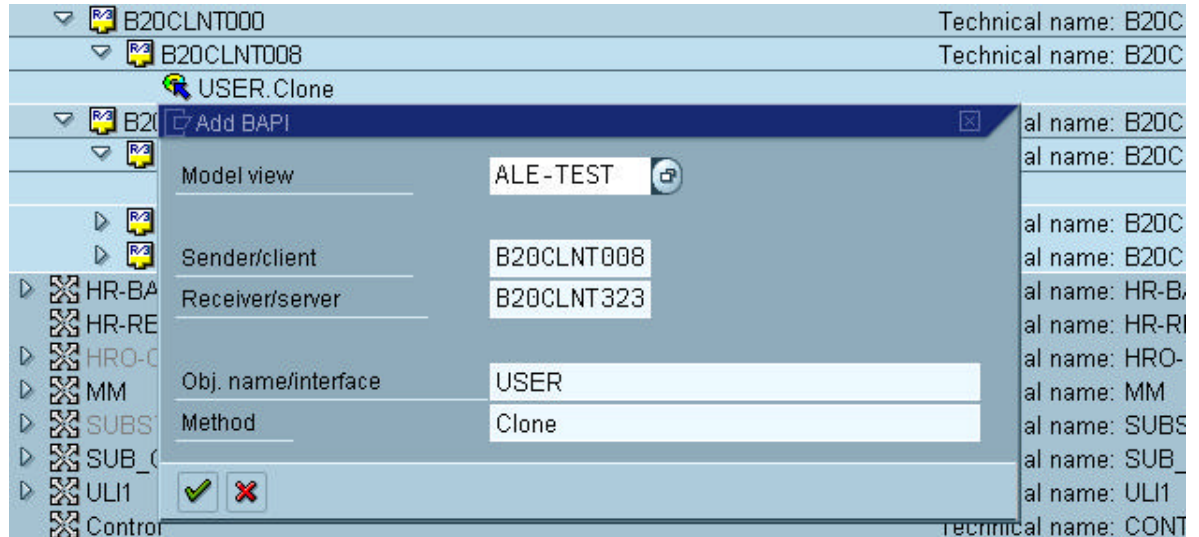
For each model view, you can specify a descriptive short text, the validity period of the message flows in the view, as well as the view maintenance system. When a model view is created, the system in which the view is created is automatically specified as the maintenance system. If possible, designate one system as the central maintenance system for all model views. The names of the model views must be unique in the entire distributed environment within your company.

Do the following:

- Choose *Create Model view* and enter a name and a short description.

Setting-up CUA for Systems with different Releases

- Create a BAPI for the object *User* and the method *Clone* (*Create user with reference from other systems*). Use F4 help for possible objects and methods. Also specify which system is the sending system and which is the target system.



- Create a second BAPI for the object *UserCompany* and the method *Clone*. This method is used for company address distribution.
5. Distribute the system landscape by choosing *Edit* → *Model view* → *Distribute*. The system displays a dialog box in which the systems relevant for you are already selected. Normally, you can just confirm the selections.
  6. In Transaction BD64, generate the partner profiles for all dependent systems (choose *Goto* → *Partner profile ### Generate*).



For information about partner profiles, see the IMG documentation (*Cross-application Components* → *Distribution (ALE)* → *Communication*)

7. Generate the partner profiles in all dependent systems for the central system.
8. Define the system landscape for central user administration in the Reference IMG under *Basis* → *Distribution (ALE)* → *Configure predefined ALE Business Processes* → *Cross-application Business Processes* → *Central User Administration* → *Select Model View for Central User Administration* (transaction SCUA). Use the F4 help (possible entries) to choose the distribution model you require and then choose *Save*. When you save the distribution landscape, the information is automatically distributed to the dependent systems.



The Central user Administration is only completely available in from Release 4.6A. Some functions are restricted in previous Releases.

After installing Central User Administration, you must check another system setting with the transaction WE20 as follows, if you use the Workplace Server:

1. Go to transaction WE20.
2. Display the subnodes of *Partner type LS* in the tree structure.

---

### Setup field distribution parameters

3. Choose a system in the tree structure.
4. Double-click on the entry USERCLONE in the table *Export parameter*.
5. Change the entry basis type to USERCLONE01 in the IDOC type group.
6. Save your changes.
7. Do the same for the other R/3 components in the Workplace.

## Setup field distribution parameters

With a central user administration system, certain fields must be maintained centrally. It may be useful to maintain additional fields locally. If you maintain fields locally, you can decide whether these fields should be automatically redistributed.

The transaction SCUM under *Basis* → *Distribution (ALE)* → *Model and implement business processes* → *Configure predefined ALE business processes* → *Cross-application business processes* → *Create central user administration* → *Setup field distribution parameters* displays a list of fields whose distribution parameters you can set. Select a distribution model in the initial screen and save it. You go to the following screen.



By choosing *Next page*, you can display any additional fields.

Choose additional tab indexes so that you can also maintain the parameters of the other groups. To save your settings, choose *Save*. The settings are then automatically distributed to the dependent systems.



When setting up central user administration, you should try and set the individual field options you choose in this transaction only once. You should not frequently change the field maintenance flags.

Setup field distribution parameters

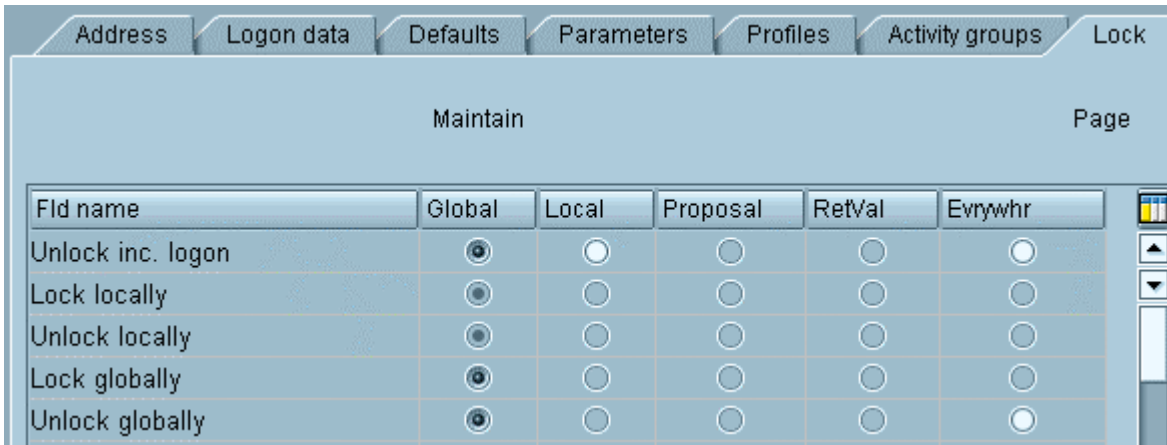
Maintain						Page
Fld name	Global	Local	Proposal	RetVal		
Title	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>		
Last name	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>		
First name	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>		
Acad. title	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>		
Name prefix	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>		
2nd acad. title	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>		
Name prefix	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>		
Name at birth	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>		

Under the individual tabs, you can choose from among the following options (some options may not make sense for all tabs):

Global	Data can only be maintained in the central system and is completely distributed.
Proposal	A default value is maintained in the central system. This value is distributed when a user is created and is then maintained locally.
Redistribution	Data is maintained both centrally and locally. Each time data is changed locally, this change is redistributed to the central system and from there distributed to the other dependent systems.
Local	Data can only be maintained in the dependent system. Data changes are not distributed to other systems.
Everywhere	Data is maintained both centrally and locally. However, data changes are not redistributed to other systems.

The last tab *Lock* contains the following options for locking a user: you can specify that the user can only be locked/unlocked either locally or globally. For local/global unlocking, you can also choose the option *Everywhere*. You can also specify where a user can be unlocked following an incorrect logon.

Migration of Existing Users into the Central System



If you make the settings for locking/unlocking users as above, a user can e.g. be unlocked globally. If the user is not unlocked in the local system, the lock still applies in the local system.

## Migration of Existing Users into the Central System

If you include a new system in the distribution model selected, you must make sure that the user master records in the new system are transferred to the central system.

Proceed as follows:

1. In the Implementation Guide (IMG), execute *Transfer Users from New Systems* (Transaction SCUG) under *Central User Administration*.

The system displays a tree structure containing the systems in the distribution model. The systems flagged with *New* may contain user master records not yet included in central user administration.

2. Position the cursor on one of these systems and choose *Transfer users*.

are:

New users	These users are not yet contained in central user administration. By choosing <i>Transfer users</i> , you can transfer the selected users into the central system. This transfers all user parameters such as address and logon data, as well as profiles and roles. In the future, the user will be maintained centrally.
Identical users	These are users with identical user IDs (that is, their name and user name is the same). You can transfer these users into the central system. Local data is overwritten.
Different users	These users are already in central user administration but under different user IDs. Rename these users in the dependent system to the correct user name that is centrally maintained, or correct the name of the user in the user address, so the user can be transferred in the next step.

## Central User Distribution

Already central users	These users are already in the central user administration under the same name. This user is already maintained centrally.
-----------------------	--

## Central User Distribution

You maintain users within central user administration using the user maintenance transaction (Transaction SU01). If central user administration is activated, you maintain users in the transaction differently:

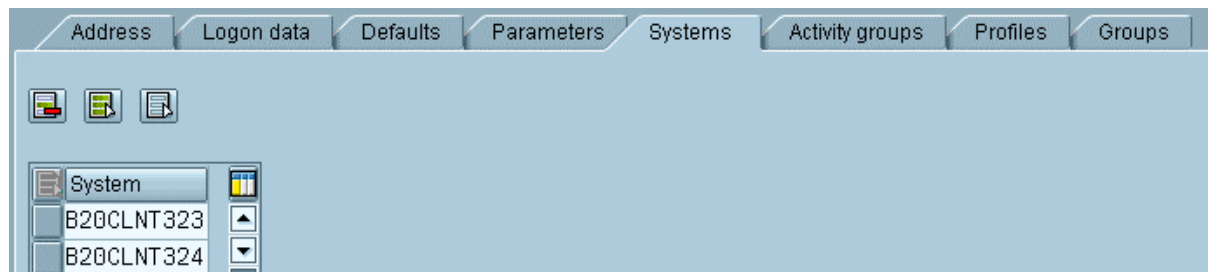
- Whether fields are ready for input or not depends on the distribution attributes that were assigned to the field in Transaction SCUM. See [Setup field distribution parameters \[Page 100\]](#).

Only the fields that may be maintained in the system are ready for input.



In the central system, you can only change a field that is to be maintained globally. This field is not ready for input in the dependent systems.

- In the central system, the user maintenance transaction also displays the tab *Systems*. Here you enter the systems to which users are to be distributed. Use the possible entries help. The systems selected in the distribution model are displayed. Each time you save, the system distributes the user data to these listed systems.



- The *Roles* and *Profiles* tabs each contain an additional column, specifying the system for which the user is assigned the role or profile.

By choosing *Compare text from dependent systems* in the *Roles* and *Profiles* tabs, you can update the texts for roles and profiles that were changed in the dependent systems, for example. The texts in the dependent systems are stored temporarily so that they are available in the central system. Since the comparison requires some time, it is executed asynchronously. The current texts may not be immediately available.

You can only assign profiles to users for the systems in which they are distributed. If you enter a new system when you assign profiles to users, the system displays a warning that the user was assigned a new system. The entry is automatically transferred into the tab *Systems*. After this, the user master record is also distributed in the new system.

All user master records are created in the user master records. Users can then only log onto the central system if the central system itself is entered in *Systems* tab of the corresponding user master record.

## Distribution Logs



You can display global user data from a dependent system in the [Infosystem \[Page 74\]](#).

## Additional Notes

As well as the authorizations already mentioned, you also need another authorization in the central system for object S\_USER\_SYS. You can only assign new systems to a new user with this authorization.

If you make any incorrect entries when you maintain roles and profiles, you can only see this in the log (Transaction SCUL).

When a user is deleted in the central system, the system entry for the user is retained until the deletion is confirmed. If an error occurs, the deletion can be repeated by withdrawing the systems (in the subsidiary system).

In the dependent systems, the RFC user is output as the last person to make changes. Choose an appropriate name when you set up the RFC user.

## Distribution Logs

To display the distribution logs, choose *Environment* → *Distribution log* (transaction SCUL) in the user maintenance (transaction SU01).

The system displays a selection of pushbuttons you can use to display the logs. The pushbutton texts form the evaluation criteria for the logs displayed.

For example, if you choose *Systems*, the system displays the status of the users, sorted by subsystem. You display the users in the subsystem by expanding the tree. The color of a node corresponds to the worst error within a node.



To display the color legend, choose *Utilities* → *Color legend*.

If you display the incorrect user master records, the system displays a short text that explains the cause of the error. If this short text is insufficient, you can display a long text by clicking on the field *User*.

By choosing *Transport*, you can execute the transport again at this level and trigger data distribution.

The system also offers you a summary of errors, warnings, successful and unconfirmed distributions. The system logs unconfirmed distributions, for example, if the data could not be distributed due to an incorrect RFC connection.



## Global User Manager

The *Global User Manager* is an additional tool with which you can considerably simplify the central user administration. Use of the *Global User Manager* is not obligatory. You can still make assignments at individual user level with the existing user and role maintenance transactions.

The *Global User Manager* gives you various grouping possibilities at user and system level for maintaining user and system assignments in a system group in the central system, in addition to the previous individual user view.

The *Global User Manager* contains these maintenance possibilities because the user master record data hardly changes once the user has been created. System assignments and authorizations change more frequently.



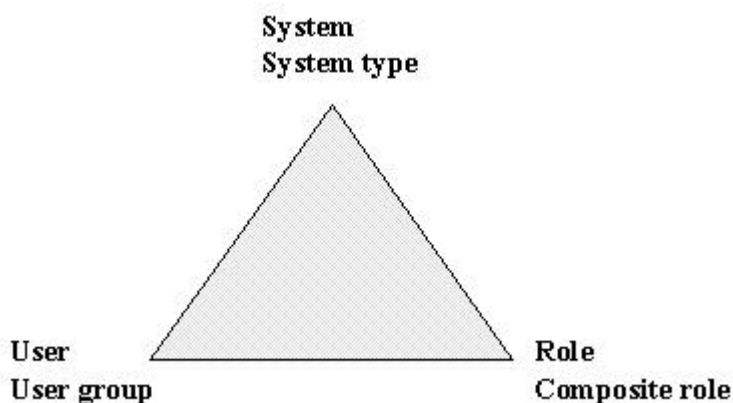
Do not distribute the user data in the *Global User Manager* until you have completely modeled the data for all users. Everything which is not defined in the *Global User Manager* is deleted in the target systems.



You cannot assign an authorization profile to users or user groups directly in the *Global User Manager*. The authorizations are assigned in roles. If you want to create a role automatically from an existing authorization profile, call the transaction SU25 and choose item 6: *Copy data from existing profiles*.

An advantage of the *Global User Manager* is that you do not need to consider the full complexity of the system environment when modeling authorizations. You consider only one part of the whole in each work step, two of the axes of an assignment triangle.

Source	Target
User/user group	System/System type
System/System type	Role/Composite role
Role/Composite role	User/user group



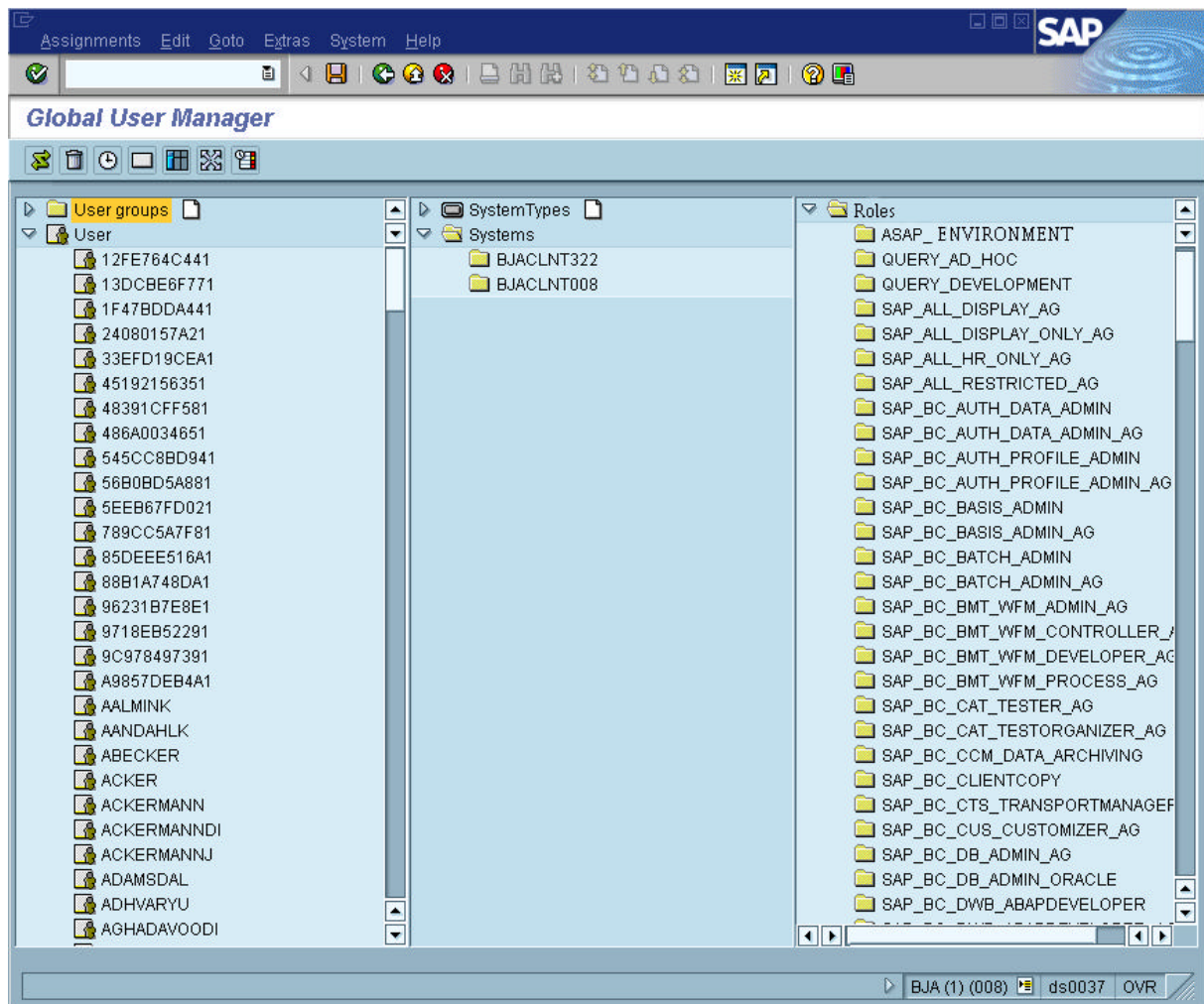
## Global User Manager

To model a complete assignment to be distributed into the target systems, you must create a closed assignment triangle as shown in the graphic. The Global User Manager reduces the complexity of this procedure so that you only need to make the two other assignments from each corner. When you have done so from all corners, the assignment is complete.

## The Global User Manager Screen

The Global User Manager only runs in the central system of the central user administration.

Call the transaction SUUM to display the Global User Manager.



All users and user groups in the system group are displayed at the left-hand side of the screen. The systems and system types are displayed in the middle, and the roles and composite roles in the system group on the right.



Choose *Extras* ® *Compare systems* in the Global User Manager to display the roles and composite roles of the subsidiary systems. You can alternatively choose *Compare texts in subsidiary systems* in the *Roles* tab in the user maintenance

transaction SU01. The data may not be immediately available because it is distributed asynchronously.

## Using the Global User Manager

If you want to use the Global User Manager, the procedure depends on whether your system environment already contained users before the installation of the central user administration. If users already exist, you should migrate the current user master records into the Global User Manager, so that previously existing assignments are not deleted the first time you distribute user data with the Global User Manager.

### System environment with existing users

To use the Global User Manager in a system environment with existing productive users:

1. Choose *Extras @ Migration @ Users* to get the current user master records of all systems in the Global User Manager.
2. Choose *Extras @ Migration @ Roles* to automatically assign the roles to the systems in which they exist, in the Global User Manager.



The data is compared with the current system status at individual user level in the Global User Manager after the migrations. To ensure that you do not lose any existing data, do not start to model user groups and system types until the migrations are finished.



Role names must be unique in the system environment. The system environment behaves like a single system, and a role can only exist once in this system. If a role with the same name exists in several systems in the system group, it appears several times in the Global User Manager role list.

You can make assignments at both individual user level and user group level in the Global User Manager. This can have unwanted effects after a user migration. Example: You have migrated all developers in your system in the Global User Manager as described above. You have then defined a user group for all developers containing the same authorizations which they had previously as individual users. When you assign all developers to the user group, the authorizations are assigned twice. So if you remove a developer from the user group, he or she still has the individual authorizations and can continue to develop. You should remove the individual user assignments after a migration as soon as you assign the users to their user groups. Use individual user assignments to give a user additional authorizations which differ from the standard authorizations of the user group.

### System environment without (existing) users

If there are no active users in your system environment, you do not need to migrate the existing user master records. You can start to create new users in transaction SU01 and model the authorizations in the system environment in the Global User Manager. Each user must only be created once in the central system and can then be assigned to other systems in the Global User Manager. The Global User Manager creates the users in these systems and assigns roles to them.

Proceed as follows:

1. Create a user in the transaction SU01.

## Global User Manager



Only assign something in the *System* and *Role* tabs when it is only for this individual user. Define other authorization for user groups in the Global User Manager.

2. Enter a user group for the current user in the *Groups* tab, if one has already been created in the Global User Manager. You will not need to make this assignment again in the Global User Manager.



All data that you enter in SU01 is also in the Global User Manager. Conversely, all assignments made and distributed in the Global User Manager are also in SU01.

## Definition on system types and user groups

Proceed as follows:


1. Create a system type/user group by choosing the appropriate pushbutton.
2. Assign systems or users to the system type/user group respectively by Drag & Drop.



A system can only be assigned to one system type. A user can belong to several user groups.

## Modeling in the Global User Manager

To specify the systems and roles for a user group:

1. Mark the user group and choose  *Display assignments*.

The current system/system type and role assignments of the selected user group are displayed. No systems or roles should be assigned to the user group yet.

2. To assign systems or system types to the user group, Drag & Drop a system or a system type to the entries under *Assignments to user groups*. Assign roles or composite roles to the user group similarly.


To restrict the number of entries displayed in a list (users, roles, etc.), choose the selection icon next to an entry and restrict the value range.

You have now defined two of the three sides of the above assignment triangle. This example focuses on the user group and we have so far assigned systems and roles. The axis which connects system and role is still missing. If you migrated the roles, this assignment is made automatically and the triangle is complete. If not, you must define it for each role.

You can display and change assignments from any corner of the triangle. When you display the assignments to a role you can edit the systems and user groups for this role. When you display the assignments to a system type you can define the users and roles for the systems of this system type.

## Distributing data with the Global User Manager


Display and check your distribution data in a list before distributing it. Proceed as follows:

1. Choose  *Display distribution data*.
2. Check whether the data for selected users is correctly flagged for distribution.

## Preparatory Steps

Only delete the user data when you have checked a sample of it in the list display.

You can distribute data from the Global User Manager immediately manually, or schedule a regular background job.

3. To distribute data immediately, choose  *Distribute immediately*.




The data is distributed immediately. It can take a few minutes until the data reaches the target system because it is distributed asynchronously.

Immediate distribution can damage the performance of your system. To avoid this, schedule a periodic background job to distribute the data, e.g. at night.

The data is distributed according to the modeling in the Global User Manager in the SU01 of the central system and from there to the subsidiary systems. Only the users are created and the roles assigned in the subsidiary systems. Other data is not distributed, it is retained in the central system. There is no log in the transaction SCUL.

Only changes since the last distribution are distributed. This minimizes the amount of data to be distributed.

To distribute data in a periodic background job, choose *Extras @ Schedule distribution*.

1. Enter a meaningful name for the background job under *Job name*.
2. Choose a job class to specify processing priority.
3. Choose the central system of the central user administration under *Target server*.
4. Choose  *Step* to schedule the ABAP program RSUSR500.
5. Choose  *Startbedingung* to specify when the job is to run.
6. Choose  *Save*.

### See also:

[Preparatory Steps \[Page 109\]](#)

[Global User Manager authorizations \[Page 111\]](#)

[Global User Manager functions \[Page 111\]](#)

## Preparatory Steps

You must perform some preparatory measures before you can manage the users centrally in the Global User Manager. They depend on whether you are installing the authorization concept for the first time or you already used the central user administration before the upgrade.

It is assumed that you have a central and several subsidiary systems. The roles are created locally in the subsidiary systems.



A subsidiary system is intended for the application MM, another for SD. Different roles are created locally in each system in Customizing.

## Preparatory Steps

When you migrate the roles into the central system the System - Role assignment is copied into the Global User Manager. The roles must be assigned to user groups to which users are assigned, in the Global User Manager. The Role -System assignment determines which systems the user can access.

The following cases can be distinguished:

Your system has been upgraded. The central user administration was not used in the previous Release.

- Setup the central user administration by connecting the systems for which users are to be managed centrally. See [Installing Central user administration \[Page 94\]](#).
- Copy the users from the systems into the central system ([Copy users from new systems \[Page 102\]](#))
- Create the system administrator for the Global User Manager. See [Global User Manager authorizations \[Page 111\]](#).
- Call the Global User Manager and choose *Extras* → *Migration* → *Roles* or *Extras* → *Migration* → *Users*.

Your system has been upgraded. The central user administration was used in the previous Release.

- Create a system administrator for the Global User Manager. See [Global User Manager authorizations \[Page 111\]](#).
- Call the Global User Manager and choose *Extras* → *Migration* → *Users* or *Roles*. The migration copies the current assignments into the Global User Manager. You can then model the user data based on the existing links between roles, users and systems. See *Extras* → *Migration* in [Global User Manager functions \[Page 111\]](#)

The SAP System has been installed for the first time.

- Install the Central user management. See [Installing Central user administration \[Page 94\]](#).
- Create all users who are to be active in the individual systems in the system group, in the central system. When you create the users, specify the user groups to which they are to be assigned. You can then assign the systems for all groups in the Global User Manager.
- Create the roles in the systems in which they are used (possibly with Customizing functions).
- Create a system administrator for the Global User Manager. See [Global User Manager authorizations \[Page 111\]](#).
- Call the Global User Manager and choose *Extras* → *Migration* → *Roles*. The data can only be modeled after migration.



Users are only migrated if the systems were also assigned in the user maintenance when the users were created. This is not recommended because the users are assigned to the systems directly and not via the groups.

## Global User Manager authorizations

You can set up the authorizations for the Global User Manager using the authorization objects S\_USER\_GRP, S\_USER\_SYS and S\_USER\_AGR. For security reasons, we recommend setting up two system administrators for the Global User Manager. One of the system administrators models the user data. The second system administrator checks the model (4 eyes principle) and performs the distribution. This administrator also requires the authorizations for user maintenance (SU01). See [Organizing user and authorization maintenance \[Page 115\]](#).

The following authorizations are available for use in the Global User Manager:

Actions	Object	Activity	S_USER_GRP	S_USER_SYS	S_USR_AGR
Create, display, and delete assignments	User User group System System type Role	Model (68), Display (03)	User group of the user User group	System System type	Role
User in user group		Assign (78)	User group of the user User group		
Change system type		Assign (78)		System System type	
Create user group		Create (01)	User group		
Migration		Migrate (90)		* Logon: not possible to specify individual systems	



There is no authorization check for creating system types.

As the migration is only executed the first time the Global User Managers is used, the authorization for migration should be later revoked. This prevents the migration from accidentally being executed later leading to inconsistent data.








When the user data distribution is triggered, the system only distributes data for which the system administrator who triggered the distribution has authorizations. The system does not report whether the distribution was incomplete. It is not possible to compare or distribute only some of the data.

## Global User Manager Functions

The Global User Manager has the following functions:




- Display assignments	The assignments are output when you double-click on an object in user administration.
-----------------------	---

## Global User Manager Functions

 - Delete	You can delete the assignments to user groups and system types with the <i>Delete</i> pushbutton.
 - Change validity period	A validity period is assigned to each role in the standard. You can change it with the <i>Change period</i> pushbutton.
 - HR-ORG in user group	This function puts organizational units from organization management (HROrg) into groups. You do not need to name users explicitly. This function prompts you to specify which organizational units you want to include, in dialog boxes.
 - Display distribution data	<p>A tabular list of the user data (SU01) is output.</p> <p style="text-align: center;"></p> <p style="text-align: center;">The distribution into the subsidiary systems is based on the assignments and objects in the distribution data table.</p>
 - Distribute immediately	<p>When you trigger distribution, the user data in the dependent systems is compared according to your model. This function can only be executed by a system administrator with the appropriate authorizations (<a href="#">Authorizations for the Global User Manager [Page 111]</a>).</p> <p>Only data that has changed since the last distribution is transferred to the dependent systems. If large changes were made, the distribution may increase system load considerably. In this case, you should consider whether the distribution should run at night as a background job.</p>
 - Schedule distribution	<p>If you schedule RSUSR500 to run as a background job, all users in all dependent systems are compared according to the defined model.</p> <p>After you call the function, the initial screen for defining a background job appears. Enter data as required. In the <i>Server</i> field, enter the server of the central system. Enter the start time for the job on the next screen. The job step is the calling of the ABAP program RSUSR500.</p>
System comparison	Using <i>Extras</i> → <i>System comparison</i> , the names of the roles in the individual dependent system are temporarily stored in the central system. You can then assign them to users or systems there. The system comparison generates a current status (changes may have been made to roles in the dependent systems). Since the comparison requires some time, it is executed asynchronously. The current data may not be immediately available after the function is executed.



First Installation Procedure

Migration	<p>Using <i>Extras</i> → <i>Migration</i> → <i>Users</i>, the existing user data is transferred to the Global User Manager. The migration only makes assignments to individual users. To model the data after the migration, assign the users to one or more groups using drag and drop and make sure that the group has the same relationships as the individual users. You can then delete the individual user assignments. This is how you move step by step from maintenance of individual users to modeling.</p> <p style="text-align: center;"></p> <p>Another possibility would be to create the complete model and define all the groups. This means you do not have to delete the individual assignments. In this case, the first distribution should only be made once you are sure that all users have been included. If you decide to use this procedure, do not migrate.</p> <p>Using <i>Extras</i> → <i>Migration</i> → <i>Roles</i>, you ensure that all roles in the individual systems are assigned to these systems. To ensure the migration is as complete as possible, execute a system comparison prior to the migration. Execute the migration when you start using the Global User Manager and model the user data based on the migration.</p>
 - Create user groups	Create a user group by choosing the <i>Create</i> icon next to the list of user groups and entering the required data.
 - Create system types	Create a system type by choosing the <i>Create</i> icon. Enter data as required.

## First Installation Procedure

To create authorizations for your SAP System:

Procedure	Optional
<p>1. Get an overview of the various tasks of your staff.</p> <p>If your company uses various applications, you must liaise with the various departments to decide which workplaces to define in each department, and which authorizations the staff is to be given. Each workplace should be defined (in writing). The authorization managers need to know which employees can access which data, call which transactions and programs, etc.</p>	
<p>2. Install the Central User Administration. (This step is optional and depends on how many clients and system users must be maintained. You should use the Central User Administration if more than one system with several users is used).</p> <p>See <a href="#">Installing Central User Administration [Page 94]</a>.</p>	X

## First Installation Procedure

<p>3. Organize the management tasks.</p> <p>Install the system administrator for authorization maintenance.</p> <p>See <a href="#">Organizing User and Authorization Maintenance [Page 115]</a>. See also <a href="#">Security in system networks [Page 121]</a>.</p>	
<p>4. Reduce the extent of authorization checks if possible, before using the profile generator.</p> <p>If the profile generator is active, an authorization check is only executed if it is in the source code of a transaction and is not explicitly excluded from the check.</p> <p>SAP supplies proposals for check indicator and authorization field values, which you must copy. You can then edit these copied defaults.</p> <p>Copy the SAP check indicator and field values in step 1 in the transaction SU25.</p> <p>Then change the check indicator if necessary. You also use check indicators to control which objects are not to be checked, which appear in the Profile Generator and which field values are displayed there for editing before the authorization profiles are generated automatically.</p> <p>You can also globally deactivate authorization objects in the transaction SU25 (item 5).</p> <p>See <a href="#">Reduce extent of authorization checks [Page 75]</a>.</p>	X
<p>5. Create roles in the development system (of the child systems).</p> <p>See <a href="#">Create roles [Page 38]</a>.</p>	
<p>6. Define test user and assign roles to them according to their job descriptions. Test the defined jobs in the quality assurance system with the help of the departments concerned (in the child systems). Make any corrections which may be necessary during the test.</p> <p>See <a href="#">Create and maintain user master records [Page 10]</a>.</p>	
<p>7. Create the users in the production or central system and assign them their roles. If you use the central user management, compare the systems or migrate first in the Global User Manager.</p> <p>See <a href="#">Create and maintain user master records [Page 10]</a> or <a href="#">Global User Manager functions [Page 111]</a>.</p>	

Organizing User and Authorization Maintenance

<p>8. Update the validity of the profiles in the user master record.</p> <p>This is only necessary if you make indirect assignments of users to roles in Organization management (HR-Org) or time-dependent assignments of roles to users.</p> <p>You cannot restrict the validity of authorization profiles in a user master record by time.</p> <p>But you can assign roles to a user master record for a time period.</p> <p>You must periodically compare these profiles with the corresponding roles in the user master record to ensure that they are up-to-date. Use the program PFCG_TIME_DEPENDENCY.</p> <p>You should check regularly as administrator whether background job errors have occurred in the job log of the program PFCG_TIME_DEPENDENCY.</p> <p>Resolve such errors manually.</p>	
<p>9. Assign table maintenance authorizations</p> <p>You can specify which table types can be maintained by which employees.</p> <p>Choose <i>Edit</i> → <i>Assign Authorizations</i> → <i>Manual entry</i> and enter the object "S_TABU_DIS" in the Profile generator authorization maintenance (transaction PFCG, <i>Authorization</i> tab, "Change authorization data").</p> <p>The selected object is inserted in the authorization maintenance hierarchy display with its authorizations and fields (activity and authorization group).</p> <p>Each table or view can be assigned to an authorization group.</p> <p>SAP delivers authorization groups and assignments of tables/views to groups.</p> <p>You can also assign row-orientes authorizations for tables. See <a href="#">Row-oriented authorizations [Page 86]</a>.</p>	
<p>10. Define not-allowed passwords.</p> <p>You can prevent users from choosing passwords that you do not want to allow. To prohibit the use of a password, enter it in table USR40.</p> <p>See <a href="#">Specifying Impermissible Passwords [Ext.]</a>.</p>	<p>X</p>

See [Security in system networks \[Page 121\]](#).

## Organizing User and Authorization Maintenance

This section describes how you organize user and authorization maintenance in your R/3 System.

[Managing users and roles \[Page 116\]](#)

[Distributed Administration \[Page 116\]](#)

[Create administrator \[Page 117\]](#)

## Managing users and roles

# Managing users and roles

The authorization system allows you great flexibility in organizing and authorizing the maintenance of user master records and roles:

- If your organization is small and centralized, you can have all maintenance of user master records and authorization components executed by a single superuser.

For more information on setting up superusers, see [Protecting Special Users \[Page 118\]](#).

- If you want to maximize system security and accommodate decentralized system administration, you can divide up maintenance among user and authorization administrators who have limited authorizations.

As you can precisely restrict authorizations for user and authorization maintenance, the administrators do not have to be privileged users. You can assign user and authorization maintenance to ordinary users.

This topic explains how to:

- how to authorize users to maintain user master records, profiles and authorizations.
- how to increase security by setting up separate administrators for maintaining user master records and roles.

## Distributed Administration

If you are using the Profile Generator, you can automatically generate authorization profiles based on selectable R/3 transactions. You can also generate these type of profiles for administrators using templates.

For reasons of system security, you should divide up system administration tasks between different administrators as described below.

The superuser sets up user master records, profiles and authorizations for administrators in one or more areas.

An area may be a department, a cost center or any other organizational unit.

Within an area, administration tasks are divided among the following three administrators:



- User administrator

User administrators have authorizations to do the following:

- Create and change users (Transaction SU01)
- Assign user roles
- Assign profiles beginning with T to users
- Display authorizations and profiles
- Call user information system (*Tools → Administration → User maintenance → Infosystem*)



They are *not* authorized to:

- Change role data
- Change or generate profiles
- Authorization administrator
  - Authorization data administrators have authorizations to do the following:
    - Create and change roles (PFCG)
    - Change the transaction selection and authorization data in roles
    - Call user information system
  -  They are *not* authorized to:
    - Change users
    - Generate profiles
- Authorization profile administrator
  - Authorization profile administrators have authorizations to do the following:
    - Display roles and their data
    - Generate authorizations and authorization profiles beginning with T based on existing roles.
    - Compare user master (transaction SUPC)
    - Call user information system
  -  They are *not* authorized to:
    - Change users
    - Change role data
    - Generate authorization profiles containing authorization objects beginning with S\_USER.

For information about assigning administration tasks to the various users see [Setting Up Administrators \[Page 117\]](#).

You can use authorization objects S\_USER\_AGR, S\_USER\_TCD and S\_USER\_VAL to further differentiate the roles of the administrators.

## Setting up Administrators

You should proceed as follows:

1. Create an role for each administrator.
2. Do not choose any transactions, choose *Change authorization data* in the *Authorizations* tab. The system displays a dialog box asking you to choose a template.
3. Choose one of the following templates:

## Protecting Special Users

Template:	Administrator:
SAP_ADM_PR	Authorization profile administrator
SAP_ADM_AU	Authorization administrator
SAP_ADM_US	User administrator

4. Generate an authorization profile for each.

Use a profile name which DOES NOT begin with T.

5. Assign the roles to the appropriate users.

Using user administration, you can restrict the authorization to particular user groups.

Using profile administration, you can exclude further authorization objects, for example, for HR data. If you want your generated authorization profiles to begin with a letter other than T, you should inform your profile administrator.

## How the Three Administrators Work Together

The **authorization data administrator** creates a role, chooses transactions and maintains authorization data. In the Profile Generator, authorization data administrators merely save the data since they are not authorized to generate the profile, and accepts the default profile name T\_....

The **Authorization profile administrator** calls the transaction SUPC and chooses *All roles*. He or she then restricts the selection, for example by entering the ID of the role to be processed. On the following screen, the administrator selects *Display profile* to check the data. If the data is correct, the administrator generates the authorization profile.

Finally, the **user administrator** assigns the role to a user (using *User maintenance*). The authorization profile is added to the user master record.



No authorization profile beginning with T may contain critical (S\_USER\* objects) authorization objects.

## Protecting Special Users

Clients 000, 001 and 066 are created when your SAP System is installed. Two special users are defined in clients 000 and 001. Since these users have standard names and standard passwords, you must secure them against unauthorized use by outsiders who know of their existence.

Note that no special user is created in client 066.

The two special users in the SAP System are as follows:

- The SAP System superuser, SAP\*

SAP\* is the only user in the SAP System that does not require a user master record, but that is instead defined in the system code itself. SAP\* has by default the password PASS, as well as unlimited system access authorizations.

## Securing User SAP\* Against Misuse

When you install your SAP System, a user master record is defined for SAP\* with the initial password 06071992 in Clients 000 and 001. The presence of a SAP\* user master record deactivates the special properties of SAP\*. It has only the password and the authorizations that are specified for it in the user master record.

To secure SAP\* against misuse, you should at least change its password from the standard PASS. For security reasons, SAP recommends that you deactivate SAP\* and define your own superuser.

- The maintenance user for the ABAP Dictionary and software logistics, user DDIC.

The user master record for user DDIC is automatically created in clients 000 and 001 when you install your SAP System. The default password for this user is 19920706. The system code allows user DDIC special privileges for certain operations. For example, DDIC is the only user that is allowed to log on to the SAP System during an upgrade.

To secure DDIC against unauthorized use, you must change the initial password for the user in clients 000 and 001 in your R/3 System.

- The user EarlyWatch is delivered in client 066 and is protected using the password SUPPORT. The EarlyWatch experts from SAP use this user. It should not be deleted. Change the password. This user should only be used for EarlyWatch functions (monitoring and performance).

See:

[Securing User SAP\\* Against Misuse \[Page 119\]](#)

[Protecting user DDIC against unauthorized access \[Page 120\]](#)

## Securing User SAP\* Against Misuse

The SAP System has a default superuser, SAP\*, in the clients 000 and 001. A user master record is defined for SAP\* when the system is installed. However, SAP\* is programmed in the system and does not require a user master record.

If you delete the SAP\* user master record and log on again as SAP\* with initial password PASS, then SAP\* has the following attributes:

- The user is not subject to authorization checks and therefore has all authorizations.
- The user has the password "PASS", which cannot be changed.



If you want to deactivate the special properties of SAP\*, set the system profile parameter *login/no\_automatic\_user\_sapstar* to a value greater than zero. If the parameter is set, then SAP\* has no special default properties. If there is no SAP\* user master record, then SAP\* cannot be used to log on.

You should set the parameter in the global system profile, DEFAULT.PFL, so that it is effective in all instances of an SAP System. You should ensure that there is a user master record for SAP\* even if you set the parameter. Otherwise, resetting the parameter to the value 0 would once again allow you to log on with SAP\*, the password "PASS" and unrestricted system authorizations.

See [Profile maintenance \[Ext.\]](#) for system profile parameter details.

---

## Protecting User DDIC Against Unauthorized Access

If a user master record exists for SAP\*, it behaves like a normal user. It is subject to authorization checks and its password can be changed.

### Deactivating User SAP\*

As SAP\* is a known superuser, SAP recommends that you deactivate it and replace it with your own superuser. In the SAP\* user master record, you should proceed as follows:

- Create a user master record for SAP\* in all new clients and in client 066.
- Assign a new password to SAP\* in clients 000 and 001.
- Delete all profiles from the SAP\* profile list so that it has no authorizations.
- Ensure that SAP\* is assigned to the user group SUPER to prevent accidental deletion or modification of the user master record.

The SUPER user group has a special status in the predefined user profiles. (They are described later in this topic.)

The users that are assigned to group SUPER can be maintained or deleted **only** by the new superuser that you define, provided that:

- you use the predefined profiles, and
- you follow SAP's other user and authorization maintenance recommendations.

### Defining a New Superuser

To define a superuser to replace SAP\*, you need only give a user the SAP\_ALL profile. SAP\_ALL contains all R/3 authorizations, including new authorizations released in the SAP\_NEW profile.

SAP\_NEW assures upward compatibility of authorizations. The profile ensures that users are not inconvenienced when a release or update includes new authorization checks for functions that were previously unprotected.

## Protecting User DDIC Against Unauthorized Access

User DDIC is a user with special privileges in installation, software logistics, and the ABAP Dictionary. The user master record is created in clients 000 and 001 when you install your R/3 System.

You should secure the DDIC user against misuse by changing DDIC's initial password *19920706* in clients 000 and 001.

User DDIC is required for certain installation and setup tasks in the system, so you should not delete it.



## Security in System Groups

### The development system

When the development system is first installed the R/3 users are mainly the project team members, including developers and system administrators. Most users of a newly-installed SAP System initially have the authorization profile *SAP\_ALL*, which allows them to perform all R/3 tasks, in their user master record. As the R/3 project progresses it is necessary to restrict user access. Development system users usually have greater access rights as quality assurance or production system users.

Authorization administrators should make themselves acquainted with the SAP authorization concept in this phase. First define the role or profile *<company>\_ALL* based on *SAP\_ALL* without superuser authorization, as follows:

1. Create a role with *Tools* → *Administration* → *User maintenance* → *Roles*.
2. Do not enter any transactions, choose *Authorizations* and then *Change authorization data*.
3. Do not copy any templates, choose *Edit* → *Add authorization*. → *Full authorization*.
4. Expand the *Basis administration* object class.  
Here you find the authorizations which are generally regarded as critical.
5. Deactivate all authorizations which begin with *User master maintenance* or have *S\_USER\_\** in the object name, and any others which you regard as critical.
6. Generate a new profile with the Profile Generator and save it under a new name (see [Predefined profile: Naming convention \[Page 90\]](#)).

You can assign the role you have just created to the user in user maintenance. See [Assigning roles \[Page 15\]](#).

This control ensures the integrity and stability of the system.

The Basis authorization objects are documented in the transaction *AUTH\_OBJECTS\_DISPLAY*. The authorization objects in the object class *Basis - Administration* are called *S\_USER\_\**. Position the cursor on an authorization object and choose *Information*.



For further information about Basis System and SAP work area authorizations, see *Tools* → *AcceleratedSAP* → *Customizing* → *Edit project* and the *SAP Reference IMG* pushbutton. Search for the entries *User* or *Authorization* to call the authorization sections.

The following [standard roles \[Page 30\]](#) are delivered:

- Basis: Authorization data administrator
- Basis: Authorization profile administrator
- Basis: User administrator
- Basis: System administrator
- Basis: Batch administrator
- Basis: Database administrator
- Basis: Customizing project member
- Basis: ABAP developer
- Basis: Uncritical basis authorizations for all users

## Security in System Groups

The authorization administrator creates profiles and authorizations for end users in the development system. These authorizations and profiles are transported to the final test in the quality assurance system before being put in the production system. The user master records are usually created in the production system shortly before it goes live. The roles are assigned to the end users in the production system together with the transported authorization data, as required.

The authorization administrator must know which clients are to be created in the customer systems. Roles are not automatically copied when new clients are created. As users, roles, authorization profiles and authorizations are client-specific, the client copy administrator must also know which user master records are to be copied.

If the SAP standard changes and user developments are made, you must clarify:

- Which development classes are to be created?
- Which authorization groups are to be created for programs?
- When are development requests transported?
- Into which clients are they transported?

etc.

[SAP Standard changes \(BC\) \[Ext.\]](#) contains information about how to proceed with new developments and changes to the SAP Standard.



New customer program code should be assigned to an authorization group in the ABAP Editor (SE38) *Program attributes* screen. Use the authorization object *ABAP Development Workbench* (S\_DEVELOP) to assign an authorization group for programs to users.

### The quality assurance system

The authorization administrator can start to transport the roles from the development system into the quality assurance system when it has been setup.

For example a member of the FI project team can check the following in the accounts payable accounting with a model user ID:

- whether the user has access to the transactions in the roles assigned to him or her
- whether these transactions correspond to the role defined by the company for the accounts payable accounting
- whether the model user ID has unallowed access authorization for certain transactions

The end users can logon in a test environment and simulate production processing to test the user authorizations.

A training client is usually created in the quality assurance system because it contains the newest configuration. Larger installations have a separate training system. In both cases the authorization administrator should contact the project team members responsible for training to familiarize him or herself with the creation of user IDs and roles.

### The production system

When the roles and authorization profiles have been completely tested in the quality assurance system and approved by the end users or project team, the roles can be transported into the production system. The user IDs can then be created. A form is distributed to all departments.

---

**Upgrade Procedure**

When all the information required for the creation of user IDs has been entered, it is signed by all relevant persons.

You should never make changes to a production R/3 System. You should therefore not assign following authorizations to users in a production system:

- Authorizations for the ABAP Development Workbench (authorization objects *ABAP Development Workbench* (S\_DEVELOP) and *Transport Organizer* (S\_TRANSPRT))
- SAP System operating system command execution authorizations (transaction SM52) (*System Authorizations* (S\_ADMI\_FCD) value *UNIX*).
- Authorizations to deactivate authorization checks (transaction AUTH\_SWITCH\_OBJECTS) with the authorization object S\_USER\_OBJ.

## Upgrade Procedure

You should perform the following activities in an upgrade from a Release before 4.6A to Release 4.6A or later:

### 1. Migrate report trees

The report tree data structure has changed. Existing report trees must be adjusted to the changed data structures if they are to continue to be used. The migration is performed by the transaction RTTREE\_MIGRATION. You only need to run the transaction in the clients which contain the production versions of the report trees. Transaction codes are assigned to all reports in a tree during the migration. This allows you to put reports in the user menu in the role maintenance. You can define a company-specific transaction code prefix in the SAP Reference IMG under *Basis* → *System administration* → *Report tree migration namespace*.

### 2. Reconcile the default check indicator and field values in the previous and new releases in transaction SU25 (steps 2a - 2d).

If you have made changes to check indicators or field values in Transaction SU24, you can compare these with the new SAP default values. The previous and new settings are displayed in a list. You can decide whether you want to use each new setting or retain the previous one.

In the next step, the system displays a list of roles affected by changes to the authorization data. Edit and regenerate their authorization profiles.



To save time if you utilize a large number of roles, you can skip editing and assign the profile SAP\_NEW to the users manually. The profile SAP\_NEW is delivered with every new Release and contains the authorizations for all new checks in existing transactions.

Step 2d display a list all roles containing any transactions that have been replaced by one or more other transactions.

---

## Upgrade Procedure

In the last section, you can adjust authorization checks. This includes changing check indicators (Transaction SU24) and globally switching off authorization objects.

### 3. Activate the Profile Generator



This step is not necessary in new installations or when upgrading from Release 4.5B or 4.6A to 4.6B, as the parameter is already set.

Make the following setting in the system profile maintenance:

**auth/no\_check\_in\_some\_cases=Y**

This parameter setting has the following effect:

- When a transaction is called, the system checks to see whether its authorization checks are to be suppressed.
- The authorization profile generator is activated in the role maintenance basic data screen (the *Authorizations* tab appears).

*Help* → *Application help* in transaction RZ10 contains system profile parameter maintenance information.

- ### 4. Install the Central User Administration and perform the user administration with the Global User Manager if several systems must be managed. See [Central user administration \[Page 94\]](#).