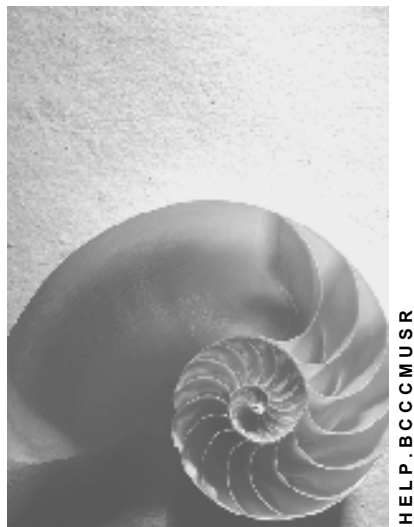


Users and Roles (BC-SEC-USR)



Release 6.20



Copyright

© Copyright 2002 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®, WINDOWS®, NT®, EXCEL®, Word®, PowerPoint® and SQL Server® are registered trademarks of Microsoft Corporation.

IBM®, DB2®, DB2 Universal Database, OS/2®, Parallel Sysplex®, MVS/ESA, AIX®, S/390®, AS/400®, OS/390®, OS/400®, iSeries, pSeries, xSeries, zSeries, z/OS, AFP, Intelligent Miner, WebSphere®, Netfinity®, Tivoli®, Informix and Informix® Dynamic Server™ are trademarks of IBM Corporation in USA and/or other countries.

ORACLE® is a registered trademark of ORACLE Corporation.

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

Citrix®, the Citrix logo, ICA®, Program Neighborhood®, MetaFrame®, WinFrame®, VideoFrame®, MultiWin® and other Citrix product names referenced herein are trademarks of Citrix Systems, Inc.






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

JAVA® is a registered trademark of Sun Microsystems, Inc.

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

SAP, SAP Logo, R/2, RIVA, R/3, SAP ArchiveLink, SAP Business Workflow, WebFlow, SAP EarlyWatch, BAPI, SAPPHIRE, Management Cockpit, mySAP, mySAP.com, and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world. MarketSet and Enterprise Buyer are jointly owned trademarks of SAP Markets and Commerce One. All other product and service names mentioned are the trademarks of their respective owners.

Icons

Icon	Meaning
	Caution
	Example
	Note
	Recommendation
	Syntax

Typographic Conventions

Type Style	Description
<i>Example text</i>	Words or characters that appear on the screen. These include field names, screen titles, pushbuttons as well as menu names, paths and options. Cross-references to other documentation.
Example text	Emphasized words or phrases in body text, titles of graphics and tables.
EXAMPLE TEXT	Names of elements in the system. These include report names, program names, transaction codes, table names, and individual key words of a programming language, when surrounded by body text, for example, SELECT and INCLUDE.
Example text	Screen output. This includes file and directory names and their paths, messages, source code, names of variables and parameters as well as names of installation, upgrade and database tools.
EXAMPLE TEXT	Keys on the keyboard, for example, function keys (such as F2) or the ENTER key.
Example text	Exact user entry. These are words or characters that you enter in the system exactly as they appear in the documentation.
<Example text>	Variable user entry. Pointed brackets indicate that you replace these words and characters with appropriate entries.

Users and Roles (BC-SEC-USR)	7
Changes to User and Role Maintenance	8
Creating and Maintaining User Master Records	12
Maintain Logon Data	14
SNC	16
Assign Roles	17
Assigning Profiles	18
Assign User Groups	19
Personalization	19
License data	20
User Maintenance Functions	20
Mass Changes	23
Logon and Password Security in the SAP System	25
Password Rules	26
Profile Parameters for Logon and Password (Login Parameters)	27
Setting Password Controls	29
Limiting Logon Attempts and Setting up Clients	30
Logging Off Inactive Users	30
Maintaining User Defaults and Options	31
Comparing User Master Records	32
The Effect of Changes on User Master Records	34
Assign Standard Roles	34
Role Maintenance	37
Role Maintenance	38
Change and Assign Roles	41
Create Roles	42
Editing Predefined Authorizations	47
SAP Authorization Concept Modules	49
Authorization Check Scenario	53
Symbols and Status Text in Authorization Maintenance	54
Copying Authorizations From Templates	57
Generating Authorization Profiles	57
Regenerate the Authorization Profile Following Changes	58
Mass Generation of Profiles	60
Assign Users	61
Assign MiniApps	62
Personalization	62
Create Composite Roles	63

Derive Roles	64
Compare Roles	65
Transport/Distribute Roles	67
Upload/Download Roles	67
Role Maintenance: Example	68
Role Maintenance: Tips and Tricks	73
Indirect Role Assignment Using HR-ORG	74
Assign Role Indirectly	74
Distribution of the HR-ORG Model	75
Create HR-ORG Distribution Model	76
Generating Partner Profiles of the HR_ORG Distribution Model	77
Activate the Change Pointer	78
Create Outbound Filert with Customer Exit	79
Distribute HR-ORG-Model (Initial Distribution)	81
Distribute Changes to the HR_ORG Model	81
Infosystem	82
Reducing the Scope of Authorization Checks	83
Preparatory Steps	83
Globally Deactivating Authorization Checks	84
Reducing Authorization Checks in Transactions	85
Editing Templates for General Authorizations	86
Comparing Check Indicators/Field Values After Upgrade	87
Transporting Authorization Components	87
Analyzing Authorization Checks	89
Analyzing Authorizations using the System Trace	90
Authorization Checks in Your Own Developments	90
Creating Authorization Fields	91
Assigning an Authorization Object to an Object Class	92
Creating/Maintaining Authorizations/Profiles Manually	92
Line-oriented Authorizations	93
Administration Tasks	93
Maintaining Authorization Profiles	93
Simple and Composite Profiles	94
Defining Profiles and Authorizations	94
Alternative Authorizations	95
Choosing Authorization Objects	95
Maintaining Composite Profiles	95
Activate profiles	96
Naming Convention for Predefined Profiles	96
Maintaining Authorizations	96

Creating and Maintaining Authorizations	97
Entering Values	97
Activating Authorizations	98
Naming Convention for SAP Authorizations	98
First Installation Procedure	100
Organizing User and Authorization Maintenance	103
Managing users and roles	103
Distributed Administration.....	103
Setting up Administrators	105
Protecting Special Users.....	106
Securing User SAP* Against Misuse	106
Protecting User DDIC Against Unauthorized Access.....	107
Security in System Groups.....	108
Upgrade Procedure	110
Source Release with the Profile Generator (> SAP R/3 3.0F)	112
Migrate Report Trees	114



Users and Roles (BC-SEC-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. 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 Workplace offers users a role-based portal to perform his or her tasks via a web browser. You can find documentation about this topic on the Workplace CD.

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 *SAP Security Guide* for more information. You can find the SAP Security Guide in the SAP Service Marketplace under <http://service.sap.com/securityguide>.



Changes to User and Role Maintenance

New Development for SAP Web Application Server 6.20

The Global User Manager was deactivated	For more information, see SAP Note 433941.
Additional system parameters for logon	Parameter <code>login/password_change_for_SSO</code> checks whether the user must change his or her password when the user logs on with Single Sign-On

New Development for SAP Web Application Server 6.10

Additional system parameters for logon	<p>You can determine the logon options for the SAP system using login parameters.</p> <p>The following login parameters were extended:</p> <ul style="list-style-type: none"> Deactivation of Password Logon <code>login/disable_password_logon</code> <code>login/password_logon_usergroup</code> Limited validity period for initial passwords <code>login/password_max_new_valid</code> <code>login/password_max_reset_valid</code> Extended password checks <code>login/min_password_digits</code> <code>login/min_password_letters</code> <code>login/min_password_specials</code> Password change <code>login/min_password_diff</code> Multiple Logon: <code>login/disable_multi_rfc_login</code> <p>For more information, see Login Parameters [Page 27].</p>
Generation and Deactivation of Passwords	<p>An initial password can be generated for users. For alternative logon variants, such as Single Sign-On [Extern], you can deactivate passwords in user maintenance.</p> <p>You can change and deactivate passwords for child systems in the central system.</p> <p>For more information, see the <i>Initial Password</i> section in Maintain logon data [Page 14] and the <i>Change Password</i> section under User Maintenance Functions [Page 20].</p>

Synchronization of the SAP Database with the LDAP Directory	<p>Directory services allow different applications in the IT landscape to access shared information at a central location.</p> <p>The information is stored on a central directory server, which the various systems in your IT landscape can access. In this way, the directory server acts as an "IT address book" for commonly shared information, such as:</p> <ul style="list-style-type: none"> • Personnel data (Name, Department, Organization) • User data and security information (User account, authorizations, Public Key Certificates) • Information about system resources and system services (System ID, application configuration, printer configuration) <p>An LDAP [Extern] directory allows central management of objects (such as users). In this way data in a system landscape can be kept consistent more easily.</p> <p>For more information, see Synchronization of the SAP Database with the LDAP Directory [Extern].</p>
---	--


Changes in SAP R/3 Release 4.6D



The term *activity group* was replaced with the term *role* in SAP R/3 Release 4.6C.

Role maintenance:

Delivery of Roles	<p>SAP delivers a large number of predefined roles. You can use the roles as they are delivered by SAP or you can copy and change them and assign them to users.</p> <p>The delivered roles include:</p>
<p>Authorization data administrator</p> <p>Authorization profile administrator</p> <p>User administrator</p> <p>System administrator</p> <p>Database administrator</p> <p>Customizing project member</p> <p>ABAP developer</p> <p>Workplace end user</p>	<p>SAP_BC_AUTH_DATA_ADMIN</p> <p>SAP_BC_AUTH_PROFILE_ADMIN</p> <p>SAP_BC_USER_ADMIN</p> <p>SAP_BC_BASIS_ADMIN</p> <p>SAP_BC_DB_ADMIN</p> <p>SAP_BC_CUS_CUSTOMIZER</p> <p>SAP_BC_DWB_ABAPDEVELOPER</p> <p>SAP_WPS_USER</p>
	<p>See Assign standard roles [Page 34].</p>
Flexible user menus	<p>In role maintenance (transaction PFCG), the administrator can construct the user menu for a role by adding transactions, reports, Internet/intranet links, and so on to the menu. The structure and terminology of the contained functions can be freely chosen.</p> <p>You can specify transactions to add to the user menus or choose transactions from the SAP menu.</p>

	 <p>The company menu is no longer available as of Release 4.6A.</p> <p>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.</p> <p>See Create roles [Page 42].</p>
Composite roles	<p>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.</p> <p>Users assigned to a composite role are automatically assigned to the roles included in the composite role.</p> <p>You can edit the complete menu structure that is the sum of the individual roles included in the composite role.</p> <p>Composite roles determine the appearance of the user work place LaunchPad in mySAP 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.</p> <p>See Composite roles [Page 63].</p>
Distribution of Roles in Target System	<p>You can distribute role menus to target systems provided that the target system has at least SAP R/3 Release 4.6A. The authorizations of the roles are then extended in the target system.</p> <p>See Create roles [Page 42].</p>
Read roles from other systems	<p>You can copy component system role menus 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.</p>
Comparison of Role Menus	<p>You can compare and adjust role menus across systems from Release 4.6C with the transaction <code>ROLE_CMP</code>.</p> <p>See Compare roles [Page 65].</p>
New authorization functionality: Mass generation of derived roles	<p>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.</p> <p>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.</p> <p>See Derive roles [Page 64].</p>
Use of MiniApps	<p>MiniApps are simple intuitive Web applications. The assignment of MiniApps to a role determines which MiniApps the user sees in his or her mySAP Workplace.</p> <p>See Assign MiniApps [Page 62].</p>
Link a role to Knowledge Warehouse	<p>You can link a role to a document in the Knowledge Warehouse with <i>Utilities</i> → <i>Info object</i> → <i>Assign</i> in the role maintenance <i>Change roles</i></p>

documentation	screen.
---------------	---------

User Maintenance:

Central User Administration	<p>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.</p> <p>For more information, see the section Central User Administration [Page 99].</p>
User groups	<p>Previously, user groups were used to distribute user administration among several administrators. As of Release 4.6A, the <i>User group</i> category (additional tab in user maintenance) can be used to improve the distribution of users thus increasing the speed of user administration.</p> <p>See User groups [Page 19].</p>
Global User Manager	<p>The Global User Manager was deactivated</p> <p>From Release 4.6D 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&Drop. These changes take affect after being distributed to the dependent systems.</p> <p>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 assigned once for each user group.</p>
Global User Manager for the Workplace	<p>The Global User Manager was deactivated</p> <p>The Global User Manager for the Workplace administers users on the Workplace server from Release 4.6D.</p>
Mass changes in user administration	<p>Most changes which can be made for one user in the user management can also be made for a set of users.</p> <p>Logon data, constants, parameters, roles and profiles can be changed for a set of users.</p> <p>You select users in the user administration Infosystem. Users can be selected, for example, according to address data or authorization data.</p> <p>See Mass changes [Page 22].</p>
Alias names for users	<p>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 name also provides authentication of a dialog user for Internet Services (logging on to the SAP GUI with the alias name is not currently possible).</p> <p>See Create and maintain internet user [Extern] for more information.</p>
Reference user	<p>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.</p> <p>See Create and maintain internet user [Extern] for more information.</p>



You can find information about alternative logon methods, such as Single Sign-On, SAP Logon Ticket, X.509 Certificate, and the Trust Center Service in the *Security* section on the mySAP Workplace CD and in the SAP Service Marketplace under <http://service.sap.com/security>.



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, that is, 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, create and maintain the users in the central system. See [Central User Administration \[Extern\]](#).

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 \[Page 102\]](#).

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 \[Page 20\]](#).

The system administrator or the user can [Maintain user values and options \[Page 31\]](#).



See:

[Compare user master records \[Page 32\]](#)

[The Effect of User Master Record changes \[Page 34\]](#)

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 or alias 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 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 name is currently only used for logon for Internet transactions. If users logon in the Internet using the [Internet Transaction Server \[Extern\]](#), (for example, when ordering items), the alias name must be entered with the corresponding password. With registration, the user can create a new account for him- or herself in the Internet. A new user with the corresponding alias is then created in the SAP system. The 12 character user name is automatically generated in this case.

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. This data belongs to the [Business Address Services \(BC-SRV-ADR\) \[Extern\]](#).

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



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

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

Users can change the data on these tabs and their address information later by choosing *System → User profile → Own data* (see [Maintaining User Defaults and Options \[Page 31\]](#)). Use a [transaction variant \[Extern\]](#), if you want to restrict the fields that can be maintained by the end users.

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

The application toolbar contains the following pushbuttons:

<i>License data</i>	You can enter measurement data. See the <i>SAP 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. For more information, see http://service.sap.com/licenseauditing .
<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 Business Object Builder [Extern]. Master data is an example of an object type (customer, material, vendor, and so on)</p> <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 \[Page 14\]](#)

[SNC \[Page 16\]](#)

[Assigning roles \[Page 17\]](#)

[Assigning Profiles \[Page 18\]](#)

[Assigning user groups \[Page 19\]](#)

[Personalization \[Page 19\]](#)



[License Data \[Page 20\]](#)



Maintain Logon Data

When you create a user, you must enter an *Initial Password* on the *Logon Data* tab page, or deactivate the password. All other entries on this screen are optional.

You can maintain the following fields:

Alias	<p>Enter an alias name.</p> <p>You have 40 characters available for alias 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.</p> <p>The alias name is used for logon for certain Internet transactions. If users logon in the Internet using the Internet Transaction Server, for example, when ordering items, the alias name must be entered with the corresponding password. With registration, the user can create a new account for him- or herself in the Internet. A new user with the corresponding alias is then created in the SAP system. The 12 character user name is automatically generated in this case.</p> <p>The <i>Alias</i> field in the initial user maintenance screen is mainly for finding internet users whose internal technical user name is not known.</p> <p>It is currently not possible to use alias names for SAP GUI and RFC logons to the system.</p>
Initial password	<p>You are required to enter the password twice to eliminate the possibility of typing errors.</p> <p>The user must change the password at the next dialog or Internet logon (but not at an RFC logon) (see Password Rules [Page 24]).</p> <p>You can set many password rules using Login Parameters [Page 27].</p> <p> To generate a password, choose <i>Wizard</i>.</p> <p> To deactivate a password, choose <i>Deactivate</i>. This means that the user can no longer log on using a password, but only with Single Sign-On variants (X.509 certificate, logon ticket).</p> <p>In the Workplace environment, password-based logon (to a Workplace component system) is no longer required if the logon to this system is done in other ways (for example, with logon tickets, see SAP Note 177895). For security reasons, you should deactivate password logon for these systems. In particular because passwords in these systems are usually still initial.</p> <p>Although the deactivation of passwords cannot be made retrospectively, the administrator can define an initial password for the user at any time.</p> <p>The deactivation of the password on the <i>Logon Data</i> tab page refers to the local system. If Central User Administration is in use, you can</p>

	<p>change or deactivate system-specific passwords with the <i>Change Password</i> function in the initial screen of the user maintenance.</p> <p>For more information, see the <i>Change Password</i> section of User Maintenance Functions [Page 20].</p>
User group	<p>Enter the name of the user group to which this user is to belong.</p> <p>You can assign the user to a user group to divide the user maintenance between different user administrators. The system administrator can assign the authorization to create and change users of a group to the appropriate user administrator. User groups can be assigned to different administrators with the authorization object <i>User Master Maintenance: User Groups</i> (S_USER_GRP).</p> <p>Users that are not assigned to any group can be maintained by all administrators.</p> <p>User groups are created using the function <i>Environment → User Groups → Maintain</i>. If you are using Central User Administration, the user groups must be created in every system.</p>
User type	<p>Choose a user type:</p> <p>Dialog</p> <p>A normal <i>dialog user</i> is used by exactly one person for all logon types.</p> <p>During a dialog log on, the system checks whether the password has expired or is initial. The user has the option to change the password himself or herself.</p> <p>Multiple dialog logons are checked and, where appropriate, logged.</p> <p>System</p> <p>The <i>System</i> user type is used for background processing and for communication within the system (internal RFC calls).</p> <p>A dialog logon is not possible with this user type. Due to a lack of interaction, no request for a change of password occurs.</p> <p>Communication</p> <p>The <i>Communication</i> user type is used for dialog-free communication between systems (for RFC and CPIC Service users of various applications, such as ALE, Workflow, TMS, CUA).</p> <p>A dialog logon is not possible with this user type. Due to a lack of interaction, no request for a change of password occurs.</p> <p>Service</p> <p>A <i>Service</i> user is a dialog user available to a larger, anonymous group of users. Only greatly limited authorizations should normally be assigned.</p> <p>Service users are used, for example, for anonymous system accesses through an ITS service. After an individual authentication, an anonymous session begun with a service user can be continued as a person-related session with a dialog user.</p> <p>During a log on, the system checks whether the password has expired or is initial. Only the user administrator can change the password (transaction SU01, <i>Goto → Change Password</i>).</p> <p>A multiple logon is permissible.</p> <p>Reference</p> <p>A <i>Reference user</i> is, like a service user, a general user not related to a person. You cannot log on with a reference user. The reference user</p>

	<p>only to assign additional authorization. Reference users are used to provide Internet users with identical authorizations.</p> <p>You can easily assign a large number of authorizations using reference users. If you do not want to use the concept of reference users,</p> <p>You can specify a reference user for additional authorizations for a dialog user, in the <i>Roles</i> tab page. In general, the application controls the assignment of reference users. The reference user name can be assigned using variables. Variables begin with "\$". Variables are assigned to reference users in the transaction SU_REFUSERVARIABLE.</p> <p>This assignment is valid for all systems in a CUA landscape. If the assigned reference user does not exist in a CUA child system, then the assignment ignored.</p>
<i>Valid from...Valid to...</i>	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.
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>



Purpose

This component integrates an external security product into SAP systems. You increase the security of your SAP system by integrating an external security product with additional security functions that are not directly available in SAP systems.

SNC protects the data communication connections between the different components of the SAP system. There are well-known cryptographic algorithms that have been implemented by various security products; with SNC you can use these algorithms on your data, in order to increase security.

Implementation

In some countries there are regulations that limit the use of encryption in software applications. Follow the regulations that in place in the area where you will be using the software.

Features

Using SNC for your applications has, among others, the following advantages:

- Security at application level and End-to-End security. All communication between two components protected with SNC is secure (for example, between the SAPgui and the application server of the SAP system).
- You can use additional security functions that are not directly included in the SAP system (such as Single Sign-On or the use of Smartcards).
- You can upgrade the security product at any time without affecting the business applications of the SAP system.

Constraints

The security product that you use must fulfil the following requirements:

- The product must provide the full range of functions of the standard interface GSS-API V2 (Generic Security Services Application Programming Interface Version 2). SNC communicates with the external security product using this interface.
- It must be possible to dynamically load the functions.
- The product must be available on platforms supported by SAP.
- The product must be certified by SAP.

For more information about the certification and availability of products, see SAP Note 66687.

See also:

- *SNC User Manual*: This manual describes in detail how you can use SNC in connection with SAP systems. You can find it in the SAP Service Marketplace under <http://service.sap.com/systemmanagement> → *Security* → *Secure Network Communications*
- SAP Note 66687: Use of Network Security Products



Assign Roles

The *Roles* field 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.

Collective roles are automatically broken down. The individual roles contained within them are entered.

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.

You can specify a *Reference user for additional authorizations* for a user, in the *Roles* tab. You assign a reference user to extend authorizations. See [Create and maintain internet user \[Extern\]](#) for more information.

If you are using Central User Administration, the *Roles* and *Profiles* tabs each contain an additional column, specifying the system for which the user is assigned the role or profile.

With the pushbutton *Text comparison from Child Systems*, the names of the roles and profiles in the child systems are read into the central system. You can only display and select roles from child systems in the central system from the possible entries help after this step. You cannot assign roles from child systems manually without a text comparison.

You can choose the roles obtained through the *Text comparison* for external systems. If these are composite roles, the composite roles in the target system must consist of local single roles. For your own system, you can enter the roles that can be maintained with role maintenance. These can include system-linked single roles (single roles with a target system attribute), and composite roles with system-linked and local single roles.



Assigning Profiles

You can assign authorization profiles that you have first manually created to a user in the *Profiles* tab.

You can assign a large number of authorization profiles to a user.

Profiles give users authorizations.

You can manually maintain profiles by choosing *Tools* → *Administration* → *Manual maintenance* → *Edit profiles manually* (see [Creating and Maintaining Authorizations and Profiles Manually \[Page 92\]](#)). You can also enter composite profiles (a combination of several profiles) in the user master records when manually maintaining profiles.

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

You assign roles to a user in the *Roles* tab. This simultaneously assigns the associated authorization profiles to the user. See [Assigning roles \[Page 17\]](#) and [Comparing profiles with roles in the user master record \[Page 32\]](#).

If you choose automatic maintenance, the [Profile Generator \[Extern\]](#) generates an authorization profile based on a role.

The SAP System contains predefined profiles:

- SAP_ALL: assign the profile SAP_ALL to users who are to have all SAP R/3 authorizations including superuser authorization. This profile can be generated using the report RSUSR406.
- 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 after an upgrade. You can then decide which users should be assigned which rights. Delete the single profiles from SAP_NEW that refer to releases that you have already included in your authorization concept. Delete the profile SAP_NEW when you no longer require it.



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 and revise all authorization profiles which have been generated using the Profile Generator. Choose *Environment* → *Installation/Upgrade* in the role maintenance (transaction SU25).

- SAP_APP: This profile contains all application authorizations. This profile is not contained in the standard system, but can be generated with the report REGENERATE_SAP_APP. You can decide when executing the report if authorizations for the Basis and HR areas should be included or not.

Assign User Groups

Use

The classification of users to user groups in the *Groups* tab groups users, above all, for mass maintenance (SU10).

User groups are created using the function *Environment* → *User Groups* → *Maintain*.

If you are using Central User Administration, the user groups must be created in every system.



By assigning the user to a user group for authorization checks in the *Logon Data* tab, you can divide the user maintenance between different user administrators. The system administrator can assign the authorization to create and change users of a group to the appropriate user administrator. User groups can be assigned to different administrators with the authorization object *User Master Maintenance: User Groups* (S_USER_GRP). All administrators can maintain users that are not assigned to any group.

Personalization

Use


You can make person-specific settings with personalization objects in the *Personalization* tab.

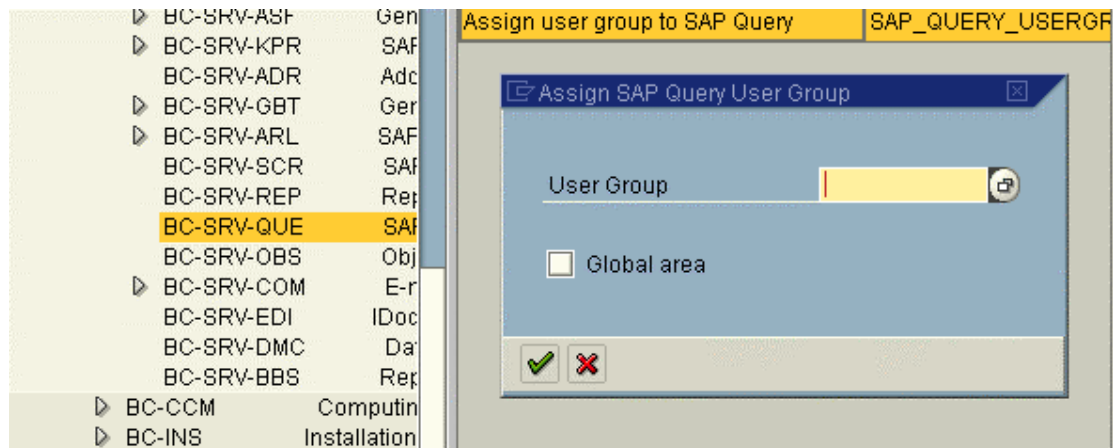
Integration


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

Activities


To assign personalization data to the user:

1. Choose the *Personalization* tab.
2. Choose  to display the application components on the left-hand side of the screen.
3. Choose a component for which 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 or choose . A dialog box for entering default values appears.

Choose  to reset the values for a personalization object.

You can display the documentation of a personalization object with .

The opportunity to create personalization objects provides a framework for application development with which user-dependent data can be easily saved for an application.

To use the framework, you must simply create a key, under which the user-dependent data is to be saved. The data can then be stored in the application simply by calling an interface direct to a generic data repository. You can specify if changing the data for this key should also be performed with the user administration. To do this, the application must provide a dialog that can be called for the personalization key in user administration.

In addition to the generic storage of personalization data, it is possible to connect your own tables with user-dependent data to user administration using the framework.

For more information about user-dependent data, see under [Central Repository for Personalization Data \[Extern\]](#).



License data

Use

The SAP software contains a measurement program with the help of which every system produces the information required for payment for the installation.





The measurement program determines the number of users and the utilized units of the SAP products. The results are evaluated in accordance with the contractually agreed conditions.


Refer to the current version of the *Guide to System Measurement* documentation in the SAP Service Marketplace (service.sap.com/licenseauditing).



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 Create and maintain user master records [Page 12] .
 - Change	Enter an existing user name or an alias and choose <i>Change</i> . See Create and maintain user master records [Page 12] .
 - Display	Enter a user name or an alias and choose <i>Change</i> . The maintenance description contains information about the contents of the tab displayed.
 - Copy	Choose <i>Copy</i> . Enter the name of a source user and the new user name. You can specify whether you want to copy only some of the user data or all of it. Logon data (password, SNC) is, of course, not copied. On the following screen you can edit the new user master record as required.

	<p>You can also rename user master records (User → Rename) if you simply want to replace one record with an identical one of a different name.</p>
 - <i>Sperren/Entsperren</i>	<p>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.</p> <p>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.</p> <p>You can set the number of permissible unsuccessful logon attempts in a system profile parameter. See Limiting Logon Attempts and Predefining Clients [Page 29] for further details.</p> <p>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.</p>
Change password	<p>Enter the user name and choose <i>Change password</i>.</p> <p>This new password must fulfill the standard conditions regarding permissible passwords. See Maintain logon data [Page 14] or choose F1.</p> <p>The new password is effective immediately. If users forget their password, they can use the new one as soon as it has been set.</p> <p>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.</p> <p>If you are using Central User Administration, a dialog window with a list of target system appears when you are changing passwords in the central system. You can change and deactivate the password here. Follow the instructions under Maintaining Logon Data [Page 14] to deactivate passwords.</p> <p>The selections in the dialog window are set so that if you are changing the password the child system is selected, and if you are deactivating the password, the central system is selected. This can be changed.</p>
<i>Edit → Address</i>	<p>Choose a component (telephone number, fax number, and so on) and make changes as needed.</p>
<i>Environment → Mass changes</i>	<p>Most changes which can be made for one user in the user management can also be made for a set of users. See Mass changes [Page 22].</p>
<i>Environment → Archive and read</i>	<p>Displaying Change Documents</p> <p>Choose <i>Info → 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"> • Direct authorization changes for a user (that is, changes to the profile list in the user master record). <p>Indirect changes are changes to profiles and authorizations contained in the user master record. These</p>

	<p>changes cannot be seen in the display. You can, however, see them in the change documents for profiles and authorizations.</p> <ul style="list-style-type: none"> • Changes to user passwords, user type, user group, validity period and account number <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>Archiving Change Documents</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"> • Changes to authorizations (archiving object US_AUTH) • Changes to authorization profiles (archiving object US_PROF) • Changes to the authorizations assigned to a user (archiving object US_USER) • Changes to a user's password or to defaults stored in the user master record (archiving object US_PASS) <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 Archiving user and authorization changes [Extern].</p>
<i>Environment</i> → <i>User groups</i>	Users can be assigned to one or more user groups. See User groups [Page 19] .
<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* → *Bulk 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. For more information, see [Distributing users \[Page Error! Bookmark not defined.\]](#).

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* tab pages for each change. In this way, you can ensure that your changes, such as the deletion of a field content are accepted for the corresponding fields.

Select users	<p>You select users in the user administration Infosystem.</p> <ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 1. Enter names in the <i>User</i> column. 2. Choose Create . <p>Maintain the user data as in the user maintenance (SU01). For more information, see Create and maintain user master records [Page 12].</p> <p></p> <p>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.</p>
Change users	<ol style="list-style-type: none"> 1. Choose Change . 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	<p>Choose Delete .</p>
Lock/unlock users	<p>Choose <i>Lock</i> () or <i>Unlock</i> (.</p> <p></p> <p>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 Setup field distribution parameters [Page Error! Bookmark not defined.].</p>

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.

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 (see [Password Rules \[Page 26\]](#) and [Defining Password Rules \[Page 29\]](#)).

When a new user logs on for the first time, he or she must change the password. To do this, the user enters the old password once and then the new password twice.

Logon with User ID and Password

To be able to access the SAP system and the data contained in it, the users of the SAP system must log on. To do this, they enter their user ID and password. A user must enter both user ID and password; it is not possible to have an empty password. (Alternatively, you can use the logon with [Single Sign-On \(BC-SEC\) \[Extern\]](#))

Before the user is granted access after entering his or her password, the system checks

- whether the user has been locked and is therefore not allowed to log on
As user administrator, you can lock a user to prevent a logons. You can find further details in [Locking and Unlocking User Master Records \[Extern\]](#).
- whether the current password for the user is valid or whether the user must create a new password

You can specify how long passwords remain valid in the system profile. By default, there is no limit on the validity of passwords.

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.

Password Checks

Password Checks for Password-Based Logon

For every failed password check, the failed logon counter for the affected user master record is increased. If the user changes his or her password, the system first checks the current password. If this check fails, the system increases the incorrect logon counter.

If the user exceeds the limit set by the profile parameter `login/fails_to_user_lock`, the user is locked. This operation is logged in the Security Audit Log and in the Syslog. If a lock is set, subsequent password checks are immediately terminated (without a statement about the correctness of the password).

The lock is regarded as invalid after the end of the current day. (Exception: see profile parameter `login/failed_user_auto_unlock`)

The failed logon counter is reset by a successful password check at logon or password change; this is also logged in the Security Audit Log. Non-password-based logons do not affect the failed logon counter; active logon locks are taken into account at each logon or password change.

Password Checks for Non-Password-Based Logon

For non-password-based logon variants (SSO: SNC, X.509, PAS, logon ticket), the system checks whether the user has a password that must be changed.

The administrator can use the profile parameter `login/password_change_for_sso` and its parameters to display various dialog boxes. For more information about this, see the documentation for the profile parameter in transaction RZ11.

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.

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 three; you can, however set a value of between 1 and 99 for both password parameters (see [Defining Password Rules \[Page 29\]](#)).

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.



Password Rules

The following table describes the specifications that are to be followed for passwords. It also shows whether these guidelines are predefined in the system or whether you can change them.

Rule	Comment
The password must be at least 3 characters long	Changeable
The password cannot be more than 8 characters long	Predefined in SAP System
Validity Period	Changeable Number of days after which a password must be changed can be set. According to the default setting, the password does not need to be changed.
All characters of the syntactical character set can be used; that is, all letters, digits, and some special characters. No distinction is made between upper and lowercase letters	Predefined in SAP System
The first character may not be a quotation or question mark, or a space	Predefined in SAP System
The first three characters may not appear in the same order in any position in the user ID	Predefined in SAP System
First three characters may not be identical	Predefined in SAP System
First three characters may not be spaces	Predefined in SAP System
The password may not be in a list of impermissible passwords	Changeable The default value is that all passwords, except PASS and SAP* are allowed.
Password may not be PASS or SAP*	Predefined in SAP System

Password may not be changed to any of a user's last five passwords	Predefined in SAP System
The password can only be changed during the logon process	Predefined in SAP System
The user can only change the password a maximum of once a day	Predefined in SAP System

You can change many of these rules using [profile parameters \[Page 27\]](#) or by [defining \[Page 29\]](#) them yourself.



Profile Parameters for Logon and Password (Login Parameters)

The following table presents the profile parameters with which you can set password and logon rules. For information about the procedure for changing profile parameters, see [Changing and Switching Profile Parameters \[Extern\]](#).

To display the documentation for a parameter, specify the parameter name in the maintenance transaction for profile parameters (RZ11), and choose *Display*. On the following screen, choose the *Documentation* pushbutton.

Password Checks

Parameter:	Meaning
login/min_password_lng	Defines the minimum length of the password
login/min_password_digits	Defines the minimum number of digits in the password
login/min_password_letters	Defines the minimum number of letters in the password
login/min_password_specials	Defines the minimum number of special characters in the password
login/password_expiration_time	Defines the validity period of passwords
login/password_change_for_SSO	If the user logs on with Single Sign-On, checks whether the user must change his or her password

Multiple Logon

Parameter:	Meaning
login/disable_multi_gui_login	Controls the deactivation of multiple dialog logons
login/disable_multi_rfc_login	Controls the deactivation of multiple RFC logons
login/multi_login_users	List of excepted users (multiple logon)

Incorrect Logon

Parameter:	Meaning
login/fails_to_session_end	Defines the number of unsuccessful logon attempts before the system does not allow any

	more logon attempts. Default value 3. You can set it to any value between 1 and 99 inclusive.
login/fails_to_user_lock	Defines the number of unsuccessful logon attempts before the system locks the user. Default value 12. You can set it to any value between 1 and 99 inclusive.
login/failed_user_auto_unlock	Defines whether user locks due to unsuccessful logon attempts should be automatically removed at midnight

Initial Password: Limited Validity

Parameter:	Meaning
login/password_max_new_valid	Defines the validity period of passwords for newly created users
login/password_max_reset_valid	Defines the validity period of reset passwords

Deactivation of Password Logon

Parameter:	Meaning
login/disable_password_logon	Controls the deactivation of password-based logon
login/password_logon_usergroup	Controls the deactivation of password-based logon for user groups

SSO Logon Ticket

Parameter:	Meaning
login/accept_sso2_ticket	Allows or locks the logon using SSO ticket
login/create_sso2_ticket	Allows the creation of SSO tickets (Workplace Server)
login/ticket_expiration_time	Defines the validity period of an SSO ticket
login/ticket_only_by_https	Sets the logon ticket when logging on over http(s)
login/ticket_only_to_host	When logging on over http(s), sends the ticket to the server that created the ticket

Other Login Parameters:

Parameter:	Meaning
login/disable_cplic	Refuse incoming connections of type CPIC
login/no_automatic_user_sapstar	Controls the SAP* user
login/system_client	Specifies the default client. This client is automatically filled in on the system logon screen. Users can type in a different client.
login/update_logon_timestamp	Specifies the exactness of the logon timestamp



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.
The standard value is 3 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.

The list of [profile parameters for logon and password \(Login Parameters\) \[Page 27\]](#) contains other options for changing password rules.

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

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.

For more information about options for restricting passwords and the logon, see [profile parameters for logon and password \(Login Parameters\) \[Page 27\]](#).



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.

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 \[Page 12\]](#)). Users can maintain the following user data: *Password*, *Constants*, *Addresses* and *Parameters*.

The following sections describe the user options that every user can set himself or herself.

Maintaining Own User Data

Users can maintain their own data by choosing *System* → *User profile* → *Own data*. Choose **F1** to display Help on the fields. You can display selectable input values with the possible entry help (**F4**).

Password

Users can change their current password using the *Password* button. The password can only be changed once every day.

Defaults

Users can set the following default values and can call up information about this with **F1**:

- Start menu

The user 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.



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 displays the credit management transactions.



The system-wide initial menu can be specified in the transaction SSM2.

- Logon language

The default system language at logon. Users can however choose another language on the logon screen

- Output device
- Spool control
- Personal time zone (different from the company time zone on the *Address* tab page, crucial with RFC)
- Date format
- The format for decimals
- CATT check indicators

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 SAP 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. For more information, choose **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.*

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.



Assign Standard Roles

Use

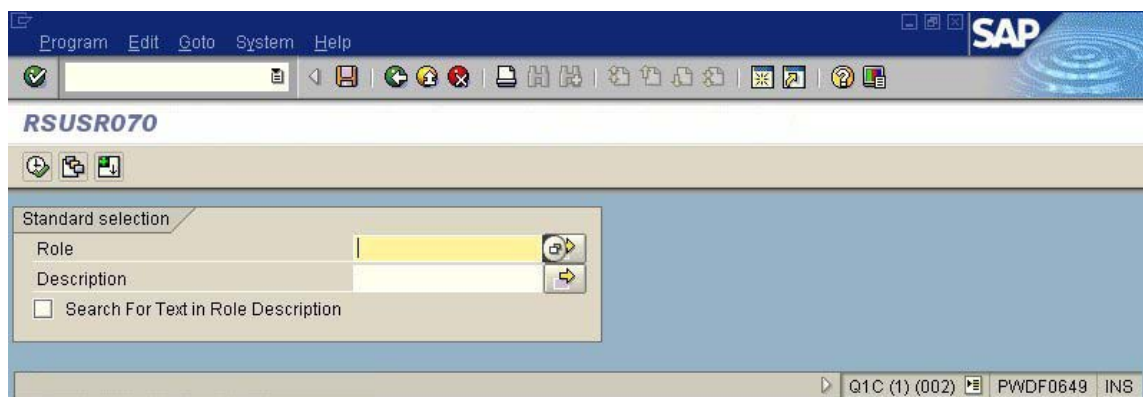
If you assign a role predefined by SAP to a user, he or she is automatically given the user menu required for his or her daily work and the authorizations required for it, when he or she logs on to the SAP system.

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 and intranet applications from the Favorites or the job structure tree.

Before you start to create your own roles for your staff, check whether you can use the roles delivered by SAP 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 start report RSUSR070 using transaction SE38.



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 and begin with the prefix "SAP_".

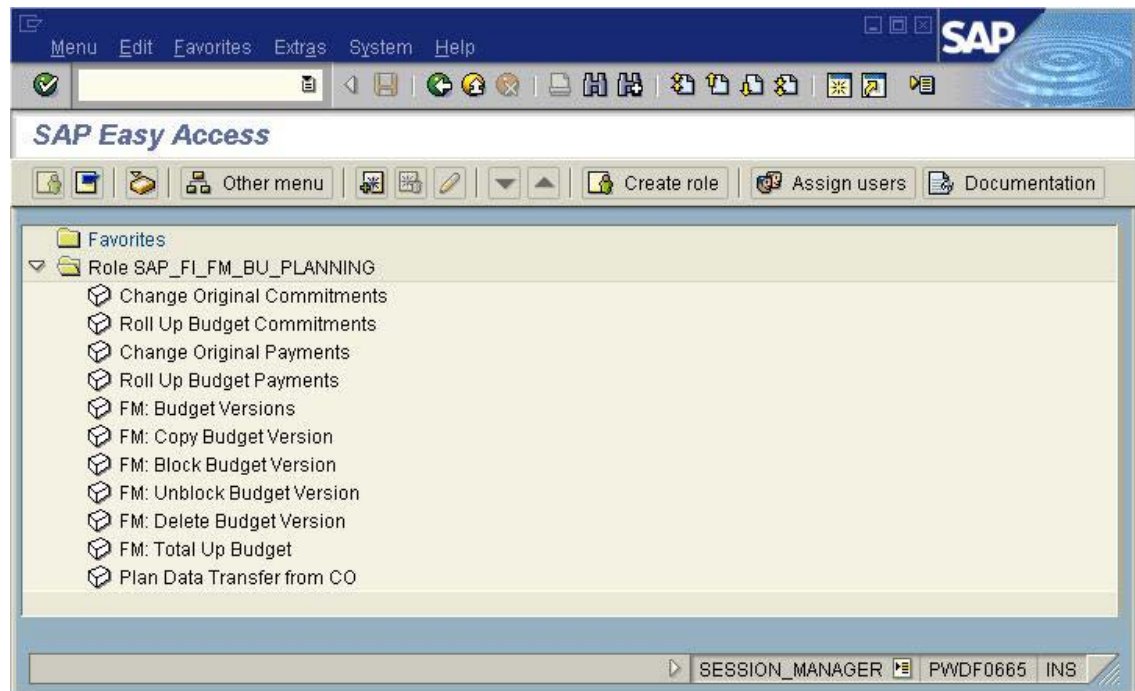
Procedure

To assign user roles unchanged:

The SAP System *SAP Easy Access* initial transaction contains additional functions for administrators. You need the authorizations of a role administrator to be able to use these functions.

1. Choose *Other menu* in the initial transaction *SAP Easy Access*.
2. Choose a role or composite role from the displayed list of standard roles by double-click.

The user menu for the selected role or composite role (such as SAP_FI_FM_BU_PLANNING) is displayed. This does not create an assignment to your user.



3. To assign the currently displayed role directly to one or more users, choose *Assign user*.
4. Enter the name of the user that 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. For more information, see [Create and maintain user master records \[Page 12\]](#).

5. Choose *Copy user*.
6. Confirm that the role profile is to be generated and the user master adjusted. The authorization profile is generated with the Profile generator 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. Unless you have assigned a role with a profile that is already generated to the users.



Revise the authorization data for the standard roles delivered by SAP and adjust this to the requirements of your company. You should at least define the organizational level fields and complete all empty fields.

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 \[Page 99\]](#).

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 \[Page 102\]](#).

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 \[Page 41\]](#)

[Create roles \[Page 42\]](#)

[Create composite roles \[Page 63\]](#)

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

[Compare roles \[Page 65\]](#)

[Transport/assign roles \[Page 67\]](#)

See also:

[Assign standard roles \[Page 34\]](#)

[Role Maintenance \[Page 38\]](#)


















Role Maintenance

Roles contain the following information:

- Role name
- Role description text
- Role menu structure
- Authorization profile data
- Users or organization plan elements to which the role is assigned
- MiniApps
- Personalization data

Functions in the role maintenance initial screen:

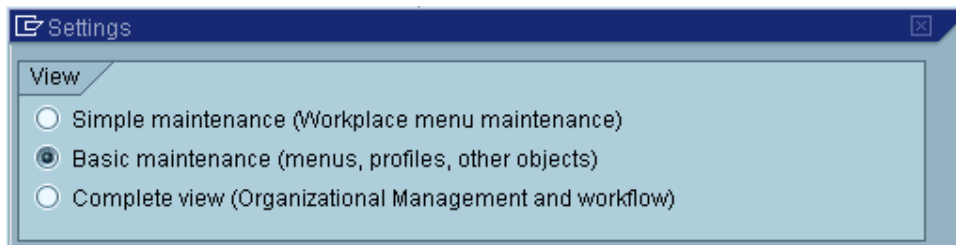
 - <i>Change</i>	Change and assign delivered roles [Page 41] or change customer roles
 - <i>Display</i>	Display single or composite roles
 - <i>Create roles</i>	Create roles [Page 42]  Guidelines for creating roles [Extern] contains an overview of the procedure.
 <i>Create Composite Roles</i>	Create composite roles [Page 63]
 - <i>Add to Favorites</i>	Role is put in the tree display. The Favorites are displayed when you call the role maintenance transaction or choose <i>Views</i> . To delete a role from the Favorites, position the cursor on the role. Choose the right-hand mouse key and choose <i>Delete from Favorites</i> in the context menu.
 - <i>Delete</i>	If the deletion is to be transported, put the role objects in a transport request before deleting. To delete the role in a system linked by RFC (For example, a component system in Workplace), choose <i>Role</i> → <i>Distribute deletion</i> .
 - <i>Copy</i>	Predefined roles are delivered as templates. They begin with the prefix "SAP_". Copy a role to a name in the customer namespace. You can also copy the user assignment and personalization objects.
 - <i>Transport</i>	Transport/assign roles [Page 67]
 <i>Transactions</i>	Where-Used list for transactions in roles
 <i>Views</i>	Select views to display roles. The following views exist:

	<div> <div> Favorites Single roles Comp. roles Roles in comp. roles Inheritance hierarchy Display roles for role owner Roles grouped by country Roles grouped by industry Roles grouped by target system </div> </div> <p><i>Inheritance hierarchy</i> displays all roles from which other roles have been derived. See Derive roles [Page 64].</p>
 <i>Display documentation</i>	<p>Displays the documentation of delivered roles in the bottom right-hand part of the screen.</p> <p>You can link a role to a document in the Knowledge Warehouse with <i>Utilities</i> → <i>Info object</i> → <i>Assign</i> in the role maintenance <i>Change roles</i> screen.</p>
 <i>Set filter</i>  <i>Reset filter</i>	<p>You can further restrict the role display at the bottom of the screen with <i>Set filter</i>.</p> <p></p> <p>The <i>Roles in composite role</i> view also displays the composite roles to which a single role with the filter search string is assigned.</p> <p>You can reset filter values with <i>Reset filter</i>.</p>

Other functions in the *Role* menu:

<i>Print</i>	All role data (activity assignments, organizational levels, authorization data, user assignment, and so on) are printed.
<i>Download/Upload</i>	Download/Upload roles [Page 67]
<i>Read from another system by RFC</i>	Role is imported into the current system via an RFC link. The menu and role description are copied. The authorization data is not imported.

Options under *Goto* → *Settings*:




Choose *Simple maintenance (Workplace menu maintenance)* to create composite or single roles on the Workplace Server.

The *Basic maintenance (menus, profile, other objects)* contains all role maintenance functions. This is the standard setting.

You can display and change role Workflow tasks in an additional tab (*Workflow*) in *Full view (Organization management and Workflow)*. The assignments are only relevant for Workflow,

that is, the users directly or indirectly assigned to the role are potential Workflow task performers.

Environment Menu Functions:

<i>Status overview</i>	Output a list of all or selected roles with user assignment, menu, authorization profile and user master record comparison status information.  If you use organization management, the statuses of the Workflow tasks and the indirect user assignments are also displayed.
<i>Mass generation</i>	Generates the profiles of several roles (Mass generation of profiles [Page 60]) at the same time
<i>Mass comparison</i>	User master comparison for several roles (Compare user master records [Page 32])
<i>Mass transport</i>	You can select several roles to transport in a dialog box (Transport/distribute roles [Page 67]).
<i>Mass download</i>	Save several roles in the PC (Upload/Download roles [Page 67])
<i>User master</i>	Call user maintenance (Create and maintain user master records [Page 12]).
<i>Role comparison tool</i>	(Cross-system) role comparison (Compare roles [Page 65]).
<i>Installation/upgrade</i>	Call the transaction which initially fills the Profile generator customer tables or updates them after an upgrade. The profile generator customer tables contain a copy of the SAP field value and check indicator default values. (Reducing the Scope of Authorization Checks [Page 82]).
<i>Check Indicators</i>	Call the transaction which allows check indicators and field values to be changed for the Profile generator.
<i>Auth. Objects → Display/Deactivate</i>	Display authorization objects with documentation / Deactivate authorization checks [Page 84]

Create Customizing roles

To assign projects or views of projects in the Implementation Guide (IMG) to a role, choose *Utilities → Customizing Auth.* in role maintenance. 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.

Roles with responsibilities

Roles with responsibilities which were created in Releases 4.0A and 4.0B, are migrated in separate roles, which are derived from one another, from Release 4.5A. The result of the migration is roles which contain transactions, and a derived role which contains the authorization data and user assignments for each responsibility.

Authorization checks in the role maintenance transaction

This transaction checks the following authorization objects:

Technical name:	Authorization object:
S_USER_GRP	User master maintenance: User groups
S_USER_PRO	User master maintenance: Authorization profile
S_USER_AUT	User master maintenance: Authorizations
S_USER_AGR	Authorization system: Check for roles
S_USER_TCD	Authorization system: Transactions in roles
S_USER_VAL	Authorization system: Field values in roles

See the authorization object documentation for details of the authorization checks.



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).
5. Choose the *Menu* tab to change the user menu. You can reduce, extend or restructure it. See [Create roles \[Page 42\]](#).
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 \[Page 46\]](#).
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 \[Page 12\]](#).

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 \[Page 34\]](#) and [Change and assign roles \[Page 41\]](#).

Procedure

The creation of a single role is described below. To create a composite role, see [Create composite role \[Page 63\]](#).

To create a single role:

10. Choose the pushbutton *Create role* or the transaction PFCG in the initial transaction SAP Easy Access. You go to the role maintenance.
11. 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.
12. Choose *Create*.
13. Enter a meaningful role description text. You can describe the activities in the role in detail. To assign Knowledge Warehouse documentation to the role, choose *Utilities* → *Info object* → *Assign*. The user of the role can then display the documentation.



You may use an existing role as a reference. See [Derive roles \[Page 64\]](#).

14. 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.

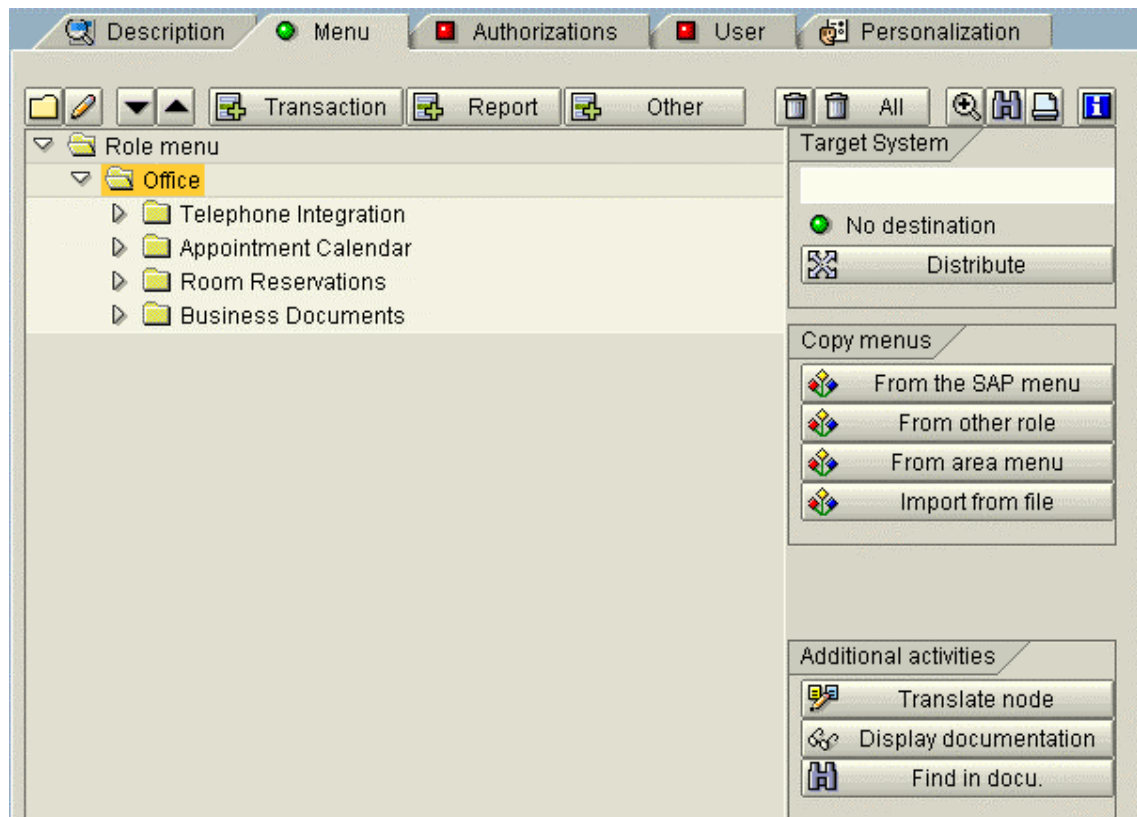
You should only use RFC destinations which were created using the Trusted System concept ([Trusted System: Relationships between R/3 Systems \[Extern\]](#)) to guarantee that the same user is used in the target system. This is only necessary if you want to navigate via the Easy Access Menu in the SAP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

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

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*

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.



You can also copy submenus via an RFC link if you want to use the menu from another Workplace component system for example. Specify a target system and choose *From SAP menu*. You can specify whether you want to copy the menu locally or via an RFC link. If you choose *Remote*, you are offered the SAP menu of the target system.

The procedure is analogous for the *From other role* and *From area menu* pushbuttons.

- *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.

- *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.

Transaction Code for Reports

Report type:

☒ ABAP report ☐ ReportWriter

☐ SAP Query ☐ Drilldown

☐ Transaction with variant ☐ Rep.portfolio

☐ BW Report

ABAP report

Report

Variant

☐ Skip selection screen

GUI-Fähigkeit

☐ SAP GUI für Windows

☐ SAP GUI für Java

☐ SAP GUI für HTML

☒ Generate automatically

Transaction code:

☒ Adopt report description

Description:

☒ ☐

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 \[Extern\]](#).

Transactions with variants

The system administrator can create transaction variants in the SAP System personalization. Transaction variants adjust complex SAP System transactions to customer business processes, by, for example, 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:

URL (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.

Predefined URL from directory

If you want to use some URLs frequently, for example, you can predefine URL objects in the Object Navigator (SE80). Choose a development class and *Create → Other → URL objects* in the context menu in the Object Navigator.

BW WebReport

You can publish queries which were defined in the Business Explorer Analyzer, in the Intranet or Internet with WebReporting. The queries can be put in any HTML pages and presented. You can put various queries in an HTML page and use predefined navigation buttons or graphics to display the data.

See *WebReporting* and *Business Explorer Browser in the Web* in the Business Information Warehouse documentation. See also the Web Reporting function documentation under *Product background → Documentation Enhancements* in BW in the SAP Service Marketplace (<http://service.sap.com/bw>).

WebSource from Drag&Relate Servlet

Enter name and a URL which you have defined in the Web Source Editor of the Drag&Relate servlet which is delivered with the Workplace. URLs which you define in the Web Source Editor allow Drag&Relate between the SAP Workplace and the World Wide Web.

For more information, see the *mySAP Workplace Drag&Relate* documentation.










External Mail System

A call of a mail system can be integrated here.

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.

Function:	Meaning:
 <i>Create folder</i>	Group transactions, programs, and so on, 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.
 <i>Delete all nodes</i>	Delete the complete role menu
 <i>Translate node</i>	Translate a menu entry
 <i>Documentation</i>	Display the documentation of transactions, programs, and so on
 <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.



To assign Implementation Guide (IMG) projects or views of projects to a role, choose *Utilities* → *Customizing auth.* The aim of this assignment is to generate the authorization for specific IMG activities and to assign it to 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.

15. Save your entries.

Result

You have created a role.

The next section [Edit predefined authorizations \[Page 46\]](#) describes how to display and edit predefined authorizations.

See also:

[Create composite roles \[Page 63\]](#)



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).

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.

[illegible]

You can display and maintain existing organizational levels with the transaction SUPO.

Save your entries.

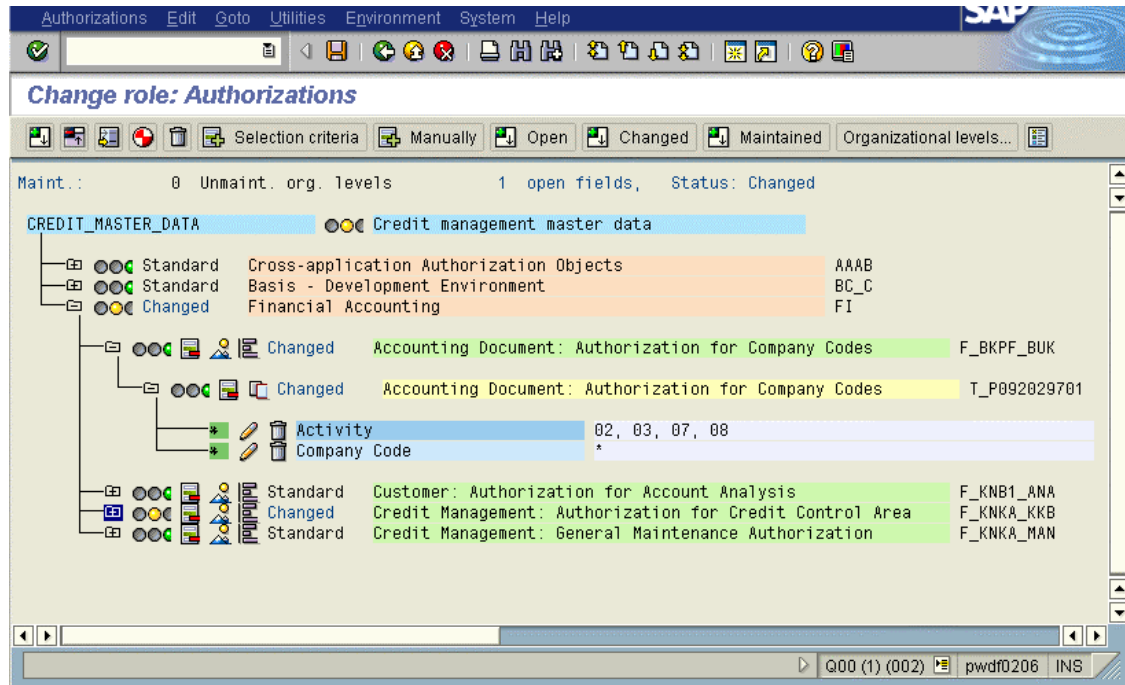


The system only displays the dialog box if the selected authorization data contains organizational levels.

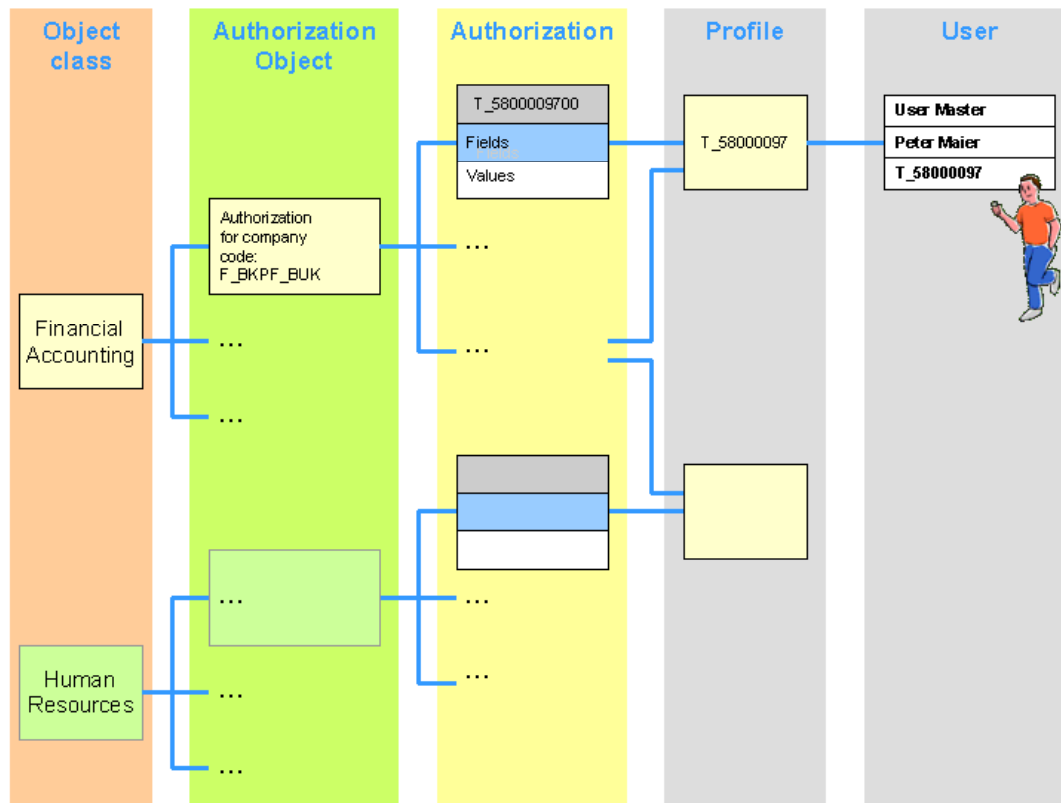
2. Check or change the default authorizations in the hierarchy view displayed. See [SAP authorization concept modules \[Page 49\]](#) and [Authorization maintenance symbols and status texts \[Page 54\]](#).

SAP Authorization Concept Modules

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

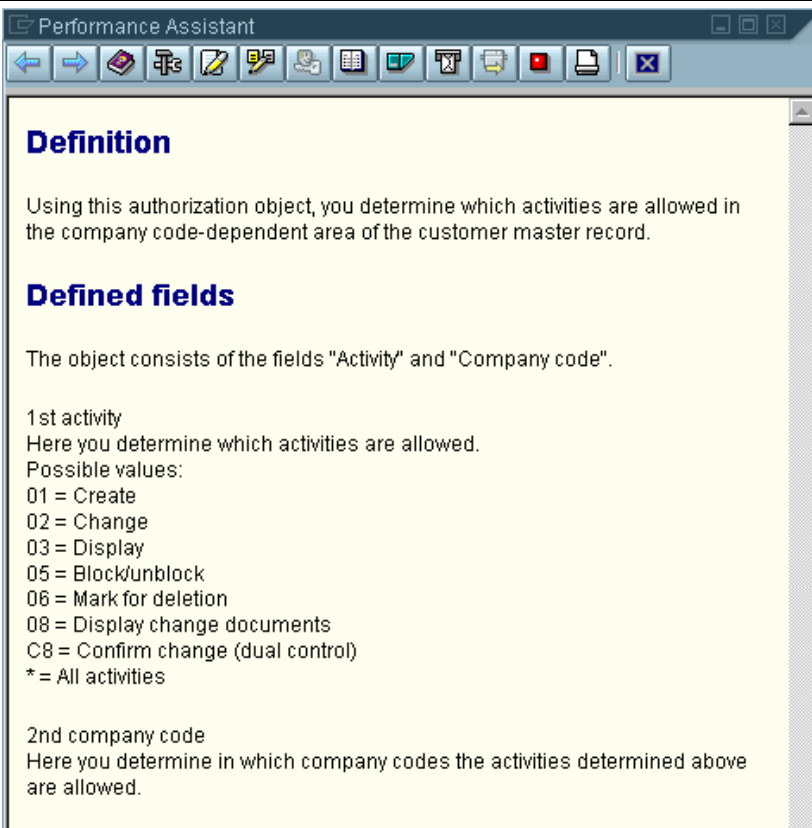



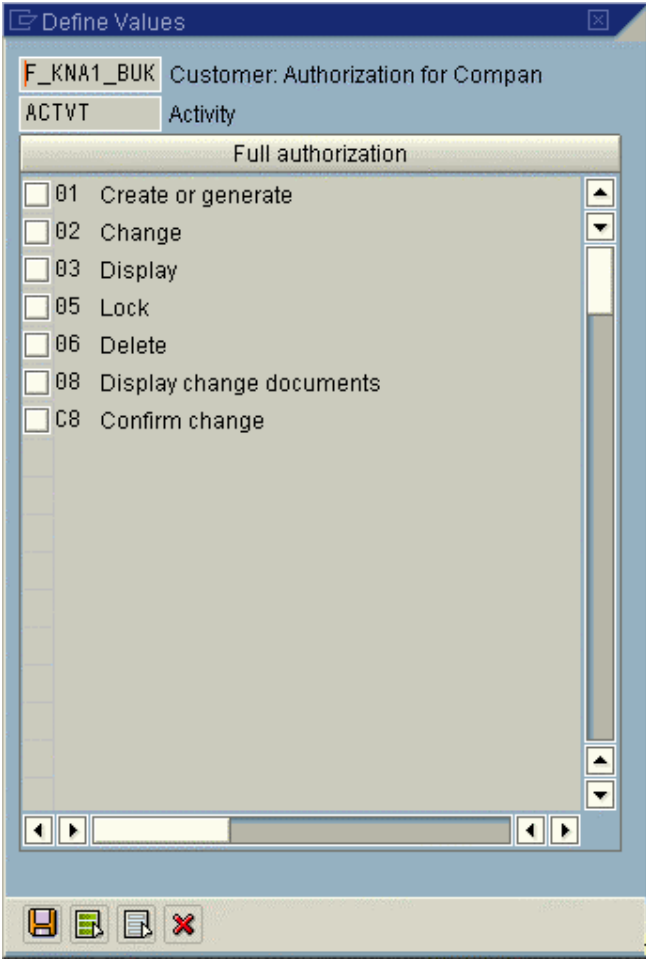
The basic SAP authorization concept terms are displayed below, before you specify the authorization field values. The colors of the SAP authorization concept modules are the standard colors in the following hierarchy display.



Explanation of terms:

Object class	<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, for example, to an application (Financial accounting, and so on).</p>
Authorization objects	<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>Definition</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>Defined fields</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>
<p>Authorizations</p>	<p>Authorizations have a yellow background in the hierarchy display. Authorization fields are light blue and their values are white.</p> <p>An authorization enables you to perform a particular activity in the SAP System, based on a set of authorization object field values.</p> <p>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.</p> <p></p> <p>T_9092029701 is an authorization for the authorization object F_KNA1_BUK with the following values:</p> <p style="padding-left: 40px;">* for company code and</p> <p style="padding-left: 40px;">01,02 activity</p> <p>Use of an authorization: Specifies permissible authorization object field values.</p> <p>Contents: One or more values for each field.</p> <p>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.</p> <p>Changes: All users with this authorization in their authorization profile are affected.</p> <p>You can maintain authorizations manually with reference to the</p>

	<p>authorization object documentation or by double-click on a value field in the following dialog box:</p>  <p>You can select individual field values or choose <i>Full Authorization</i>.</p>
<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>Use: Specifies authorizations in user master records</p> <p>Contents: 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</p>

	<p>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 \[Page 53\]](#) 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 \[Page 91\]](#) (**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 \[Page 92\]](#) (here **S_TRVL_BKS**) and [assign the authorization object to an object class \[Page 92\]](#).

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.

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</p>


	SUPO.
--	-------

If a yellow traffic light is displayed in the status line, you can click on it. You are asked whether you want to assign full authorization "*" to all unmaintained authorizations. You can choose this procedure if you want to create an authorization profile now and perform detailed authorization maintenance later. You can also click on yellow traffic lights at object class, object or authorization level and assign full authorizations. Red lights indicate that organizational levels are not maintained. If you want to assign full authorization, maintain the organizational levels first. You can then assign full authorization.

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:

	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. Maintain the values in the dialog box.
*	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.

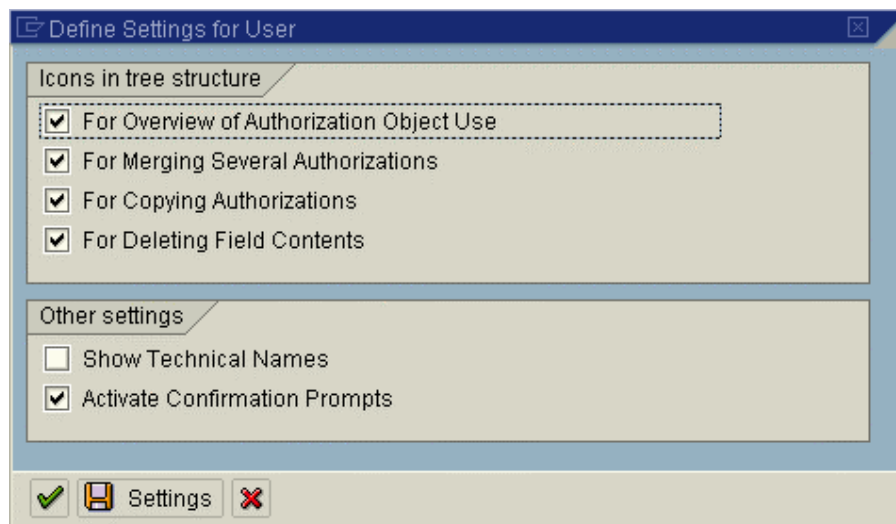






When you maintain authorizations, check the values of the authorization fields with a green light as well.

The following icons are also displayed where appropriate:

	Deactivate an authorization or authorization object. Inactive authorizations are ignored when profiles are generated. You must deactivate an authorization/authorization object before you can delete it.
	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.
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  Manually 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 \[Page 57\]](#)



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: 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:

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).

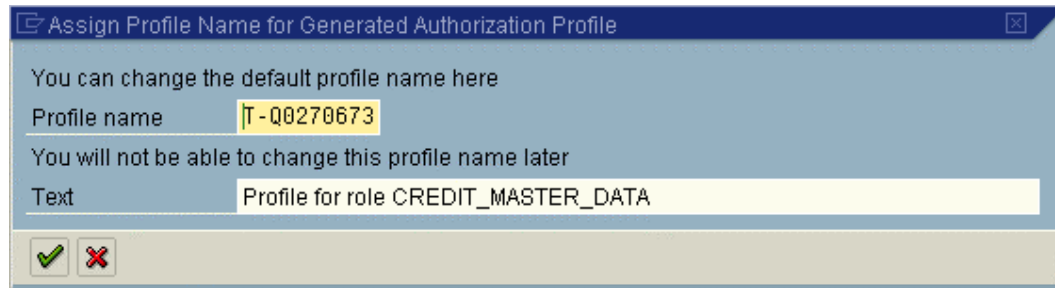
If the changed profile is already assigned to some users:

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:



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).

You can also just save the profile and generate later with transaction SUPC.

Result

Whenever you assign the role to a user, you can also assign the generated authorization profile to that user (see [Assigning Profiles \[Page 18\]](#)).

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

See also:

[Regenerating Authorization Profiles Following Changes \[Page 58\]](#)

[Check roles for existing profiles \[Page 60\]](#)



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.

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 \[Extern\] 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.

Roles: Mass generation of profiles

The screenshot shows the SAP transaction screen for 'Roles: Mass generation of profiles'. The interface is divided into several sections:

- 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: [Yellow highlighted field] to [Field] [Right arrow]
 - Last changed by: [Field] to [Field] [Right arrow]
- 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

Prerequisites

You have created a menu for the new role and setup the authorizations.

Procedure

1. Choose the *User* tab page.

The status display on the tab page tells you whether users have already been assigned to the role.

- Red: No users assigned
- Green: At least one user assigned
- Yellow: Although users are assigned, user master comparison is not current

For composite roles, the status display refers only to the assignment of users.

User ID	User name	From	to
BRODERICK	Chris BRODERICK	08.03.2000	31.12.9999
MILLER	John Miller	08.03.2000	31.12.9999

2. Enter the user names in the list.

Enter the user names either directly or from the possible entries help. You can make a multiple selection with the *Select* pushbutton, such as 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.

You have the following options for performing a user comparison:

- Choose *User comparison* on the *User* tab page. 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* → *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. Set the indicator *HR-OrgComparison* indicator on the selection screen of the report.

You should schedule the report 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.

Display *Org.Management* Pushbutton

The *Org.Management* pushbutton is only displayed if you have defined an active plan variant in the current client, as this is required to use organizational management.

If this is the case, at the start of transaction PFCG, choose *Goto* → *Settings* → *Complete view*. The *Org.Management* pushbutton is then displayed on the *User* tab page.

For more information about indirect role assignment using HR-ORG, see [Indirect Role Assignment Using HR-ORG \[Page 74\]](#).



Assign MiniApps

Use

A MiniApp is an application, information or service that can be displayed in a Web Browser.

MiniApps provide users with basic information and provide frequently used functions.

You can integrate existing MiniApps in your Workplace. MiniApps are simple and intuitive to use. They give the user a quick overview and access to his or her most important data when the mySAP Workplace starts.

The assignment of MiniApps to a role determines which MiniApps the user sees in his or her mySAP Workplace.

Possible MiniApps include Alerts, Reports, Calendar, Search machines, Company and Web News, Share Price Ticker, and so on.

You can find detailed information about using MiniApps on the Workplace CD in the *MiniApps* section.



Personalization

Use


You can make adjustments for a role centrally in the *Personalization* tab. You can further differentiate the activities assigned to a role by assigning values to personalization objects.

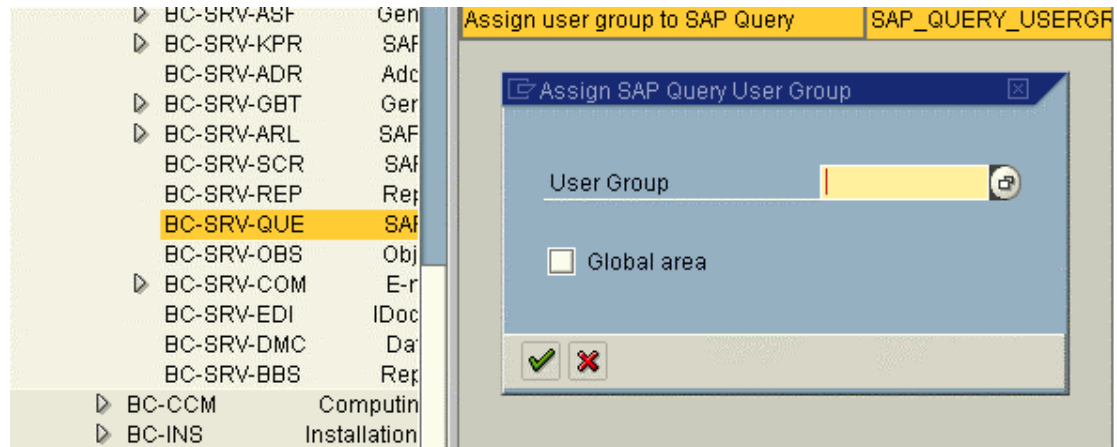
Integration


You can assign values to personalization objects in the user maintenance as well as in the role maintenance. Settings made in the user maintenance are person-specific.

Activities


To assign personalization data to a role:

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



7. Double-click on a personalization object or choose . A dialog box for entering default values appears.

Choose  to reset the values for a personalization object.

You can display the documentation of a personalization object with .

The opportunity to create personalization objects provides a framework for application development with which user-dependent data can be easily saved for an application.

To use the framework, you must simply create a key, under which the user-dependent data is to be saved. The data can then be stored in the application simply by calling an interface direct to a generic data repository. You can specify if changing the data for this key should also be performed with the user administration. To do this, the application must provide a dialog that can be called for the personalization key in user administration.

In addition to the generic storage of personalization data, it is possible to connect your own tables with user-dependent data to user administration using the framework.

For more information about user-dependent data, see under [Central Repository for Personalization Data \[Extern\]](#).



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 \[Page 42\]](#).
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 *Roles in composite roles* with the *View* pushbutton in the role maintenance initial screen.



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

Roles derived from another cannot have any additional menu entries.

Procedure

To set 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 page.

When you save, you have created a role whose menu is derived from another role. If additional transaction codes are added to the menu of the original role, they are copied into the derived role.

To copy the authorizations from the source role 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 data is maintained for the organizational levels in the derived role, and if you have maintained the organizational levels using the dialog box, the data is not overwritten by another conciliation (See SAP Note 314513).

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

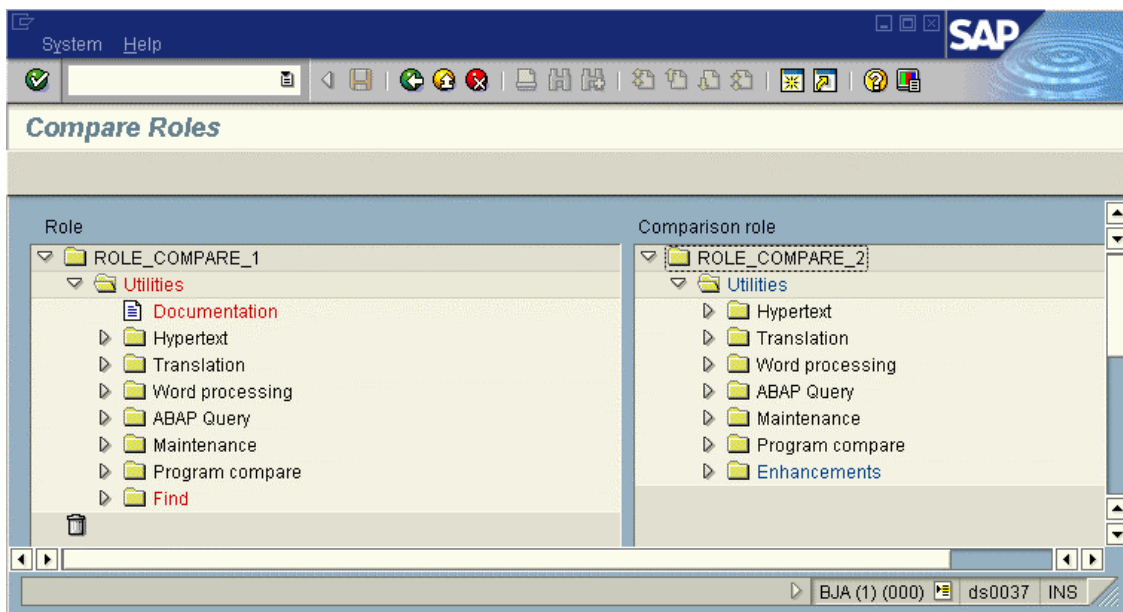
To compare two role menus in different systems, their RFC destinations must be maintained.

Procedure

Role menu 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.

3. Choose *Compare*.



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 at least Release 4.6A.



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* → *Mass 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 'Y'. This is the case for new installations.

Check the setting in your system using report RSPARAM.

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 \[Page 83\]](#).

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*.
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 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 \[Page 17\]](#).

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.
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 \[Extern\]](#) 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.

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 \[Extern\]](#) 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.
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*.



Indirect Role Assignment Using HR-ORG

Use

Indirect role assignment means that you do not assign the role directly in transaction SU01, SU10, or PFCG to one or more users, but link the role with only one organizational unit (work center, job, organizational unit, position) using HR-ORG. The users are then assigned the role linked with this organizational unit indirectly using the evaluation path US_ACTGR (table T77AW). The evaluation of the organizational model with transaction PFUD switches indirect role assignment to direct role assignment.

The evaluation path is delivered with default values; that is, you can modify it to suit your requirements. As soon as a valid evaluation path is available, the roles can be assigned to users.



You can also create direct user assignments using organizational management with the object *User*. These are then identical with the assignments maintained on the *User* tab page.

You can use HR_ORG to assign single and composite roles with and without the use of central user administration in accordance with the rules of the composite roles resolution. However, this is a local assignment; that is, the role must exist in the system in which it is to be assigned.

Prerequisites

- The Customizing switch HR_ORG_ACTIVE in table PRGN_CUST is set to **YES** to activate the HR_ORG management.
- The evaluation path is defined.
- You have shown the *Org.Management* pushbutton.



The *Org.Management* pushbutton is only displayed if you have defined an active plan variant in the current client, as this is required to use organizational management.



Assign Role Indirectly

1. Choose *Tools* → *Administration* → *User Maintenance* → *PFCG – Roles* (transaction PFCG).
2. Choose *Goto* → *Settings* → *Total View (Organizational Management and Workflow)*.
The *Org.Management* pushbutton is then displayed on the *User* tab page.
3. Specify the role that you want to assign indirectly, and choose *Display*.
4. Choose the *Org.Management* button on the *User* tab page.
The *Role: User Assignment* screen appears.
5. Switch to change mode, and choose the *Create Assignment* pushbutton.
The system displays the *Select processor type* dialog box, in which you can select some or all of the following object types, depending on the system settings: work center, job, organizational unit, position, and user.
6. Select the object to which the role is to be assigned.

7. In the following dialog box, select an available object (for example, using the possible entries help) and choose *Continue*.
8. Choose *Compare Indirect User Assignment*.



The assignments created in this way are called indirect user assignments, as they are not made directly between the user and the role.

These indirect user assignments are stored as gray in the user display and highlighted in color.

Status Display and Maintenance

The status display in the *Org.Management* button shows whether you need to update the indirect user assignments:

- Green: User assignments are current
- Red: User assignments are not current, the indirectly assigned users are not completely displayed on the tab page.

You have the following options to update the assignment:

- Choose *Org.Management* and then *Compare indirect user assignment*.
- Perform the manual user master comparison that also automatically updates the indirectly assigned users.
- Schedule the report PFCG_TIME_DEPENDENCY periodically
- Call transaction PFUD and set the indicator *HR-ORG comparison* on the selection screen

This executes the report PFCG_TIME_DEPENDENCY, which inserts all indirectly assigned users for the role, that have become valid due to the assignment period, and removes all indirectly assigned users that have become invalid. It then performs a complete user master comparison for all roles.



Distribution of the HR-ORG Model

Use

You want to distribute the HR-ORG model that you have created in your HR system into another system of your choice (such as the CUA central system) in order to use indirect role assignment in this system, or to copy the role assignment of the HR system without changes.

You should usually only distribute the required objects when distributing the HR-ORG model. In this description, only the objects required for user administration are distributed.

You have the following options for the distribution of the HR_ORG model:

- Distribution with role assignment:



In the receiving system, ensure that no user can change the HR-ORG model, using authorizations.

You want to have the same role assignment in every system. To achieve this, the roles used must exist in all systems.

- Distribution without role assignment:



In the receiving system, ensure that no user can change the objects of the HR-ORG model, using authorizations. Only the role assignments may be changed.

You assign roles individually in every system, or if you have distributed the model to the CUA central system, you can use composite roles.

This differentiation affects the filter setting of the HR-ORG model.

Procedure

1. [Create the HR-ORG distribution model in the HR system \[Page 76\]](#).
2. [Generate Partner Profile in the HR and CUA central systems \[Page 77\]](#).
3. So that you can later distribute only the changed data in the HR-ORG model, [activate the change pointer in the HR system \[Page 78\]](#)
4. [Create an outbound filter with customer exit in the HR system \[Page 79\]](#)
5. [Distribute the HR-ORG structure. \[Page 81\]](#)
6. [Distribute the changes to the HR-ORG structure. \[Page 81\]](#)

See also:

- SAP Note 200343: HR-CA-ALE: Composite SAP Note: Distribution of HR Master Data
- SAP Note 363187: HR-CA-ALE: Initial Distribution with HRMD_A/HRMD_ABA (Tips)



Create HR-ORG Distribution Model

Use

To be able to copy the HR_ORG model to other systems, you must first create a corresponding distribution model. This distribution model is a view of the HR-ORG model that is then distributed instead of the entire HR-ORG model.

Procedure

1. Call the transaction BD64 in the HR system.
2. In change mode, choose *Create Model View* and enter the following data:

Field	Value:
Short text	Description of the distribution model (for example: HR-ORG Distribution Model)
Technical name	Technical name of the distribution model (such as HR_ORG)

3. Choose *Insert Message Type* and enter the following data:



Field	Value
Model view	HR_ORG
Sender	Logical name of the HR system
Receiver	Logical name of the receiving system
Message Type	HRMD_ABA

4. Expand the *HR-ORG Distribution Model* node.
5. Define a filter for the distribution model by double clicking the option *No Filter Set*.

The system displays the *Edit Filter* dialog box.



The filters described below reduce the distribution of the HR-ORG model to the objects that are significant for user administration.

- a. Choose *Create Filter Group* and expand the *Data Filtering* node.
 - b. Call the *Edit Value List* dialog box by double clicking the *Infotype* node.
 - c. Enter the value 1000 (Filter group for objects) by choosing the *Insert Line* button () and choose *Copy*.
 - d. Call the *Edit Value List* dialog box by double clicking the *Object type* node.
 - e. Enter the values c (job), o (organizational unit) and s (position) using the insert line button () and choose *Copy*.
 - f. Create another filter group in the same way, with the infotype 1001 (Filter group for relationships), and the object types C, and S. Define the node *Type of linked object* for these filter groups, with the following values: AG (role), C (job), O (organizational unit), S (position), T (task), TS (standard output), UG (user group), US (user), and WF (workflow task).
6. Distribute the model view by choosing *Edit* → *Model View* → *Distribute to All Receiving Systems*.



Generating Partner Profiles of the HR_ORG Distribution Model

Use

Perform these procedures both in the HR system and in the receiving system of the HR-ORG distribution model.



Choose serial background processing for the incoming processing. In this way, you can avoid two background jobs being run in parallel, as this can easily cause update problems.

If the system displays an error message in transaction WE02, saying that the object was locked, check the background processing of the IDocs.

Procedure

1. Choose *Environment* → *Generate Partner Profile* in transaction BD64.
Sie gelangen auf das Bild *Generierung der Partnervereinbarung*.
2. Specify the model view and the receiving system.
3. Under inbound parameters, choose the option *Trigger by Background Program*.



To be able to use background processing, you must then schedule the report RBDAPP01 for the message type HRMD_ABA in all receiving systems.

4. Check the result log for the partner profile generation in the sending and receiving systems.
 - If message type HRMD_ABA was not generated correctly in the sending system, adjust the outbound processing in transaction WE20.
 - i. On the *Partner Profiles* screen (transaction WE20), choose the partner profile of the sending system under *Partner type LS*.
 - ii. Check whether message type HRMD_ABA is listed under *Outbound parameters*.

If not, add it with *Create Outbound Parameter*. On the *Partner Profiles: Outbound Parameters* screen, you can specify the following data:

- *Outbound Options* tab page: Message type: HRMD_ABA, process code: HRMD, syntax check, triggered by background program
 - *Postprocessing* tab page: Allowed Processor: Type: US, Processor: User name of the administrator, Language: EN
- If message type HRMD_ABA was not generated correctly in the receiving system, adjust the inbound processing in transaction WE20.
 - iii. On the *Partner Profiles* screen (transaction WE20), choose the partner profile of the sending system under *Partner type LS*.
 - iv. Check whether message type HRMD_ABA is listed under *Inbound parameters*.

If not, add it with *Create Inbound Parameter*. On the *Partner Profiles: Inbound Parameters* screen, you can specify the following data:

- *Inbound Options* tab page: Message type: HRMD_ABA, process code: HRMD, syntax check, triggered by background program
- *Postprocessing* tab page: Allowed Processor: Type: US, Processor: User name of the administrator, Language: EN



Activate the Change Pointer

Use

During the first distribution of the HR-ORG model to the receiving system, you distribute all defined data in the filter of the distribution model. If, however, you want to transport only the changed data during later distributions to the receiving system, activate the change pointer in the HR system.

Procedure

1. In the Implementation Guide (IMG, transaction SALE), choose *Modeling and Implementing* → *Master Data Distribution* → *Replication of Modified Data* → *Activate Change Pointers - Generally*.
2. Set the activation status *Activate Change Pointers - Generally*, and save your entry.
3. Choose the activity *Activate Change Pointers for Message Types*.
4. Set the *active* indicator for the message type HRMD_ABA.
5. Save your entries.



Create Outbound Filert with Customer Exit

Use

As the receiving systems only use the object types *User* and not *Employee*, you must map the role assignment of the HR system (O-S-P) that assigns the object type P (employee) and not object type US(user) to the role assignment of the receiving system (O-S-US).

Prerequisites

- The HR-ORG structure is maintained.
- Every employee has a user (infotype 105).
- The used users all exist in all systems (through CUA distribution or client copy).

Procedure

1. Call the transaction CMOD in the HR system.
2. Assign the enhancement RHALE001 to the project using the *Enhancement Assignments*.
3. Insert a filter by choosing the *Components* pushbutton and double clicking EXIT_SAPLRHA0_001.
4. Enter the following coding in include ZXHALU01 of function module EXIT_SAPLRHA0_001.
5. Generate the function group.
6. Activate the include, the function, and the project.

Coding to Be Inserted

```

*-----*
*-----*
*   INCLUDE ZXHALU01
*
*-----*
*-----*
*""-----*
*-----*
*""Local Interface:
*""   IMPORTING
*""       VALUE(F_IDOC_CONTROL) LIKE EDIDC STRUCTURE
EDIDC
*""   TABLES
*""       T_COMM_CONTROL STRUCTURE EDIDC
*""       T_IDOC_DATA STRUCTURE EDIDD
*""   CHANGING
*""       VALUE(FLAG) TYPE C DEFAULT 'X'
*""   EXCEPTIONS
*""       ERROR_IN_IDOC_CONTROL
*""       ERROR_WRITING_IDOC_STATUS
*""       ERROR_IN_IDOC_DATA
*""       SENDING_LOGICAL_SYSTEM_UNKNOWN
*-----*
*-----*
DATA: e1p1001 LIKE e1p1001,
      p0105   LIKE p0105 OCCURS 0 WITH HEADER LINE,
      subrc   LIKE sy-subrc,
      pernr   LIKE prelp-pernr.

```

```

* we are trying to switch 1001 relationships of type P to US.
* In other words, the HR org system has
*   O--S--P relationships
* we want to convert that to
*   O--S--US
* so that the workplace server can handle objects
* it knows about. IE P is not known in a 4.6d basis system.

* This will allow PFUD to be run in Workplace.
* Note, this exit assumes the CUA master is in Workplace
system.
*****
***

CHECK f_idoc_control-mestyp = 'HRMD_ABA'.      "org to WP
message type

LOOP AT t_idoc_data WHERE segnam = 'E1P1001'.
  elp1001 = t_idoc_data-sdata .

  CHECK elp1001-sclas = 'P'.      "personnel
  CHECK elp1001-otype = 'S'.      "position
  CHECK elp1001-relat = '008'.    "holder
  CHECK elp1001-rsign = 'A'.      "bottom up

  MOVE elp1001-sobid TO pernr.

  REFRESH p0105.

  CALL FUNCTION 'HR_READ_INFOTYPE'
    EXPORTING
      pernr      = pernr
      infty      = '0105'
      begda      = elp1001-begda
      endda      = elp1001-endda
    IMPORTING
      subrc      = subrc
    TABLES
      infty_tab  = p0105
    EXCEPTIONS
      infty_not_found = 1
      OTHERS      = 2.

  IF sy-subrc EQ 0 AND subrc EQ 0.
    READ TABLE p0105 WITH KEY pernr = pernr
                                usrty = '0001'.      "SAP Userid

    IF sy-subrc EQ 0.
      elp1001-varyf      = 'US'.      " user
      *   elp1001-varyf+2(8) = p0105-usrid.  " the rest of varyf
      elp1001-sclas      = 'US'.      " object type p to US
      elp1001-sobid      = p0105-usrid.  " object id is the
      USerid now

      t_idoc_data-sdata = elp1001.
      MODIFY t_idoc_data.
    ENDIF.
  ENDIF.
ENDLOOP.

```




Distribute HR-ORG-Model (Initial Distribution)

Use

Perform the following steps in order with report RHALEINI:

1. Make a preselection of the data to be distributed on the selection screen of the report.
2. The report automatically filters the data with the filters defined in the distribution model.
3. The report automatically filters the data with the outbound filter of the Customizing exit.
4. The report distributes the data that has been selected to the receiving system.

Procedure

1. Start the report RHALEINI with transaction SA38.
2. Specify the following data:

Field	Value:
Plan variant	01
Object type	
Object ID	Relevant HR structure
Evaluation period	All
Evaluation value	O-S-P Staff assignments along organizational structure With this path you can choose the data that is relevant for user administration.
Transfer mode	Insert This mode inserts the data to be distributed by overwriting
Receiver Partner Number	Logical name of the receiving system

3. Choose *Execute*.



Distribute Changes to the HR_ORG Model

Use

With this procedure, you can distribute only the delta of changed data for the HR-ORG model to the receiving systems.

Procedure

1. Call transaction BD21.
2. Choose message type HRMD_ABA and then *Execute*.



With the report RHALEPCS, you can evaluate the change pointer.



Infosystem

Use

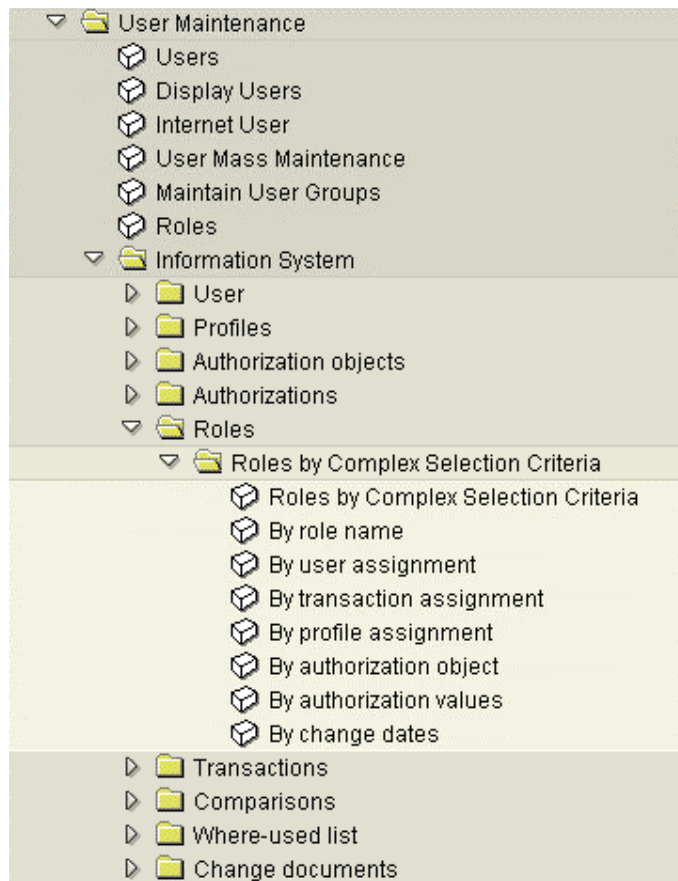
You can gain an overview of user master records, authorizations, profiles, roles, change dates and so on with the Infosystem.

You can output lists to answer various questions. For example:

- What authorizations are assigned to which user?
- What changes have been made to the authorization profile of a user?
- Which roles contain a particular transaction?

You can go to the info system from the SAP menu in SAP Easy Access with *Tools* → *Administration* → *User maintenance* → *Infosystem* or with *Info* → *Infosystem* (transaction SUIM) 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 System transactions are executed, a large number of [Authorization Objects \[Extern\]](#) 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 authorization 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 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 \[Page 83\]](#)

[Globally Deactivating Authorization Checks \[Page 84\]](#)

[Reducing Authorization Checks in Transactions \[Page 85\]](#)

[Editing Templates for General Authorizations \[Page 86\]](#)

[Comparing Check Indicators and Field Values After a Release Upgrade \[Page 87\]](#)



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.

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



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 \[Page 32\]](#).

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 authorization proposals in the Profile generator.



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:

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 \[Extern\]](#).

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 [Development Classes \[Extern\]](#).



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 \[Page 96\]](#)

If you choose *User Maintenance* → *Users*, you can assign the role you have just created to the user. See [Assigning roles \[Page 17\]](#).



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.

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.
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 \[Page 90\]](#).

- 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 **/nSU53** 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*.

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 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 \[Page 91\]](#)
2. [Create an Authorization Object \[Page 92\]](#)
3. [Assign an Authorization Object to an Object Class \[Page 92\]](#)
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 ([check authorization \[Extern\]](#)).



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 a authorization field:

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 [Link to the check table \[Extern\]](#). The link provides possible field values. You can also define a value range by way of the area 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.

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 \[Page 93\]](#)

[Maintaining Authorization Profiles \[Page 93\]](#)

[Maintaining Authorizations \[Page 96\]](#)

[Adding Authorization Checks To Your Own Developments \[Page 90\]](#)

[Analyzing Authorization Checks \[Page 89\]](#)



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 \[Page 102\]](#).



Maintaining Authorization Profiles

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



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

Choose *Tools → Administration → User Maintenance → Manual Maintenance → Edit Profile Manually* to access the profile maintenance functions.

- [Simple and Composite Profiles \[Page 94\]](#)
- [Defining Profiles and Authorizations \[Page 94\]](#)
- [Alternative Authorizations \[Page 95\]](#)

- [Choosing Authorization Objects \[Page 95\]](#)
- [Maintaining Composite Profiles \[Page 95\]](#)
- [Activating Profiles \[Page 96\]](#)
- [Naming Convention for Predefined Profiles \[Page 96\]](#)



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.



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

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 \[Page 97\]](#)

[Entering Values \[Page 97\]](#)

[Activating Authorizations \[Page 98\]](#)

[Naming Conventions for SAP Authorizations \[Page 98\]](#)



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.

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
<i>User groups</i>	<i>User master maintenance: User group</i>	S*
	<i>Administrator action</i>	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 \[Page 96\]](#).



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



First Installation Procedure

To set up user and role administration for your SAP system:

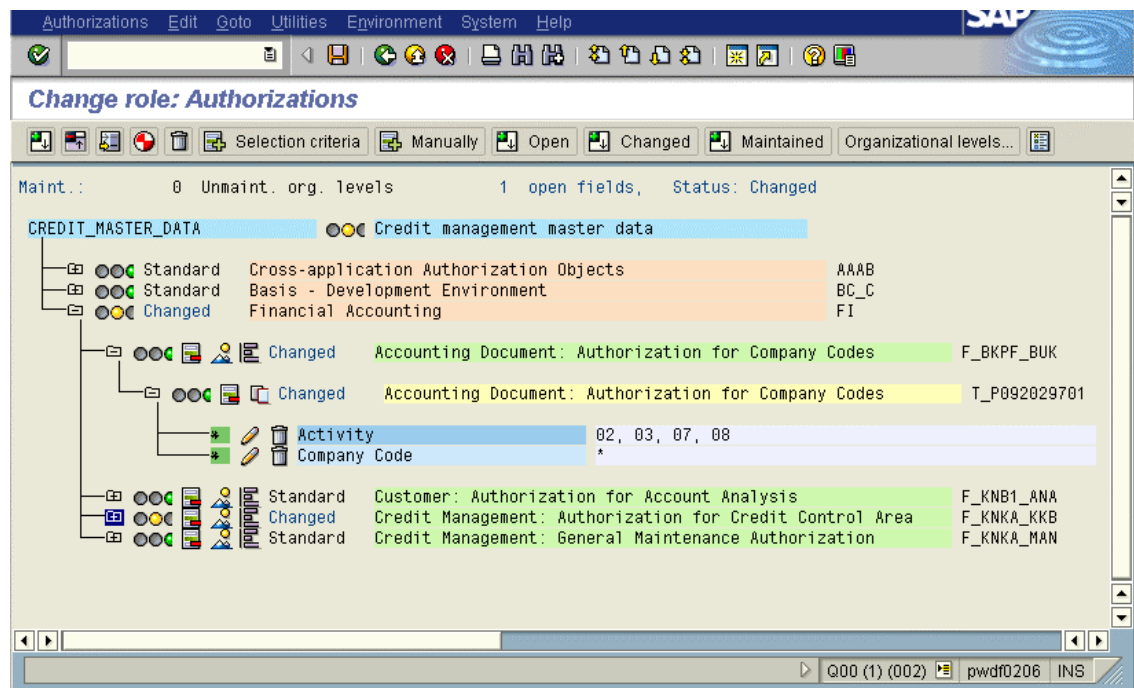
1. See [Security in system networks \[Page 107\]](#).
2. Get an overview of the various tasks of your staff.

If your company uses various applications, you must liaise with the various departments to decide which roles to define in each department, and which authorizations the staff is to be given. Each workplace should be defined (in writing). The authorization administrators need to know which employees can access which data, call which transactions and programs, and so on.

3. In transaction SU25, choose menu entry 1: *Initial Fill of the Customer Tables*.

When initially filling the customer tables, the check indicators and authorization values that are preset by SAP are copied to the appropriate customer tables.



Users and user groups are assigned roles, possibly predefined, that contain typical transactions for their work. On the basis of the transactions contained in a role, the profile generator selects the authorization objects that are checked in the transactions. If a menu has been created for a role, the profile generator searches for the associated authorizations. These can be supplemented and modified by the administrator.



Depending on how exact the default values are, green (complete authorization) or yellow (must be maintained by the authorization administrator) lights appear in the display for the maintenance of the individual roles.

Default values for authorizations are delivered by SAP in the form of the tables USOBX and USOBT. The customer tables USOBX_C and USOBT_C are initially filled with the contents of these tables and can be synchronized at each further upgrade. These tables can be evaluated in the Data Browser (transaction SE16).

USOBX	Defines which authorization checks should occur within a transaction and which authorization checks should be maintained in the profile generator. You determine the authorization checks that can be maintained in the profile generator are using check indicators [Extern] . Only the authorization
-------	--

	<p>checks that are assigned the indicator "PP" can be maintained in the profile generator.</p>  <p>In these tables, "PP", which is used in transaction SU24, corresponds to an X.</p>  <p>Authorization checks can be suppressed despite a programmed authority check command.</p>
USOBT	Defines for each transaction and authorization object which default values should be used in the profile generator for the transaction codes entered in a role menu.

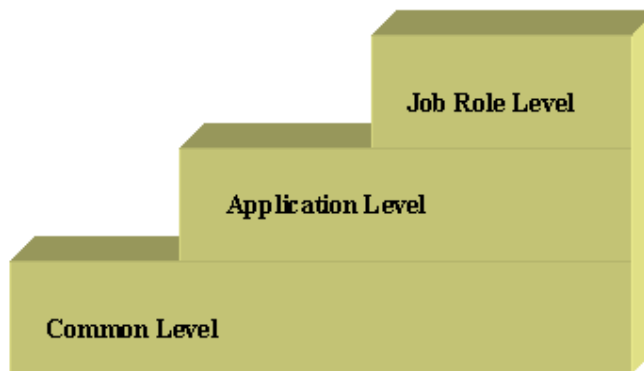
4. If necessary, adjust the extent of authorization checks before using the profile generator.

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.

Adjust the authorization checks to be performed for each transaction according to your wishes. To do this, call transaction SU25 and choose point 4: *Check Indicators in Transactions (SU24)*.

You can also globally deactivate authorization objects in the transaction SU25 (item 5). See [Reduce extent of authorization checks \[Page 82\]](#).

5. To copy the tables to other systems in your system group, choose point 3: *Transport Customer Tables*.
6. Implement your role administration in accordance with the following model:



At the common level, access to commonly used transactions is created for all users of the system. Examples of contained transactions are: Printing, Online Help, SAP office, and so on. Create one (or more) roles for general activities in your company. Changes to these roles affect all employees. If general activities are part of specific job roles, changes in the general authorizations must be adjusted in all roles.

At the application level, all users of a particular application should be assigned general transactions for this application. This procedure leads to a time saving, as these general application-specific roles usually remain stable even after upgrades. If you need to make changes, you can again make "one change for all".

At the job role level, you should assign the transactions and authorizations that are required especially for one (or a few) work centers. If roles are used at different organizational levels (for example, in different company codes), you can [derive roles \[Page 64\]](#) and change the appropriate organizational levels for the derived role in a dialog window.

As both of the lower levels remain largely stable after the authorization administration has been implemented, the work of the authorization administrator will mainly be related to roles at the job role level after the implementation.

See also:

[Organizing User and Authorization Maintenance \[Page 102\]](#)

[Protecting Special Users \[Page 105\]](#)



Organizing User and Authorization Maintenance

This section describes how you organize user and role maintenance in your system.

[Managing users and roles \[Page 103\]](#)

[Distributed Administration \[Page 103\]](#)

[Create administrator \[Page 104\]](#)



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 \[Page 105\]](#).

- 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 \[Page 104\]](#).

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:

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.

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 SAP EarlyWatch experts use this user which 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 \[Page 106\]](#)

[Protecting user DDIC against unauthorized access \[Page 107\]](#)



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 \[Extern\]](#) for system profile parameter details.

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. 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 SAP 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 SAP 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 SAP R/3 tasks, in their user master record. As the SAP 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. Proceed 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, but 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. Using the Profile Generator, generate a new profile and save it under a new name.

You can assign the role you have just created to the user in user maintenance. See [Assigning roles \[Page 17\]](#).

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*.



If you want more information about the Basis system and SAP work area authorizations, choose *Tools* → *AcceleratedSAP* → *Customizing* → *Edit Project* and then choose the pushbutton *SAP Reference IMG*. Then search for "user" or "authorization" to find the relevant sections of the Guide.

The authorization administrator creates the roles for end users in the development system. These roles 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.

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.

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.

You should never make changes to a production SAP system. You should therefore not assign following authorizations to users in a production system:

- Authorizations for the ABAP Workbench (authorization objects *ABAP 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

After an upgrade, you must make adjustments to the user and role administration. What these are depends on whether you were already using the profile generator in the source release.

In the following, it is assumed that you have not yet used the profile generator, and that you are not upgrading from SAP R/3 3.0F.



If you were already using the profile generator in the last release, read [Source Release with the Profile Generator \(> SAP R/3 3.0F\) \[Page 111\]](#).

First of all, choose one of the following options:

1. Convert the profiles that you manually created to roles. To do this, choose step 6 in transaction SU25.

This has the advantage that the administrator can assign all of the existing, thoroughly checked profiles to the corresponding roles. You can, however, only create a user menu for the role if the corresponding authorizations for the authorization object S_TCODE are contained in the profile. Additionally, you cannot use the configuration tables (USOBX_C, USOBT_C) in which the predefined authorization values are contained.

2. Carry out a new implementation of the authorization administration using the profile generator.

This has the following advantages:

- Customers' experiences have made it clear that the time invested in the new implementation of the authorization administration pays off with a large time saving during other maintenance of the user and authorization data.
- Your employees can take advantage of user-friendly user menus.

We recommend the second option. In addition to the advantages already mentioned, you can use the three level model for the implementation of roles, as shown in the section [First Installation Procedure \[Page 99\]](#). A redesign of the authorization administration using the three-level model makes sense in the long term, in that the work time that an authorization administrator must expend for the maintenance of the roles can be significantly reduced.

If you have decided to use the second option (Redesigning the Authorization Administration), read the [First Installation Procedure \[Page 99\]](#), and the following advice:

- Plan the conversion of profiles to roles. Produce a list of transactions and associated profiles for which you want to set up roles. Use the Infosystem (transaction SUIM). You can download the Infosystem lists to a Microsoft Excel sheet and use it as the basis for the migration to be performed. Contact the departments and discuss which roles should be provided for which departments.
- During the conversion to roles, you can decide if the naming conventions that you used have proved to be useful. If necessary, you can define a different naming convention.
- Create the new roles in the development system.

The following procedure may be useful when copying the authorization values from the old profiles:

Open three sessions in the SAP system.

- In the first session, start transaction SU02 and choose a profile that you want to convert to a role
- In the second session, call transaction PFCG and create the new role there.

- In the third session, start the transaction SUIM as a utility for maintaining the authorizations. Choose *Authorization Objects* → *Authorization Objects by Complex Selection Criteria*. Enter the name of an authorization object. You want to know, for example, in which profile the object S_TABU_DIS is used. Choose *Where-Used List*. Choose the profile for which you want to create a role. Select the profile and choose *Expand Subtree*.
You can now search for the desired authorization object (in this case S_TABU_DIS) and enter the authorization values in the role.
- When you have finished the conversion of profiles to roles, call step 2C of transaction SU25. The system produces a list of roles that must be checked after the upgrade. Transaction SU25 would have produced no output for profiles. It makes sense to create the roles beforehand, in order to find out which roles authorization checks have been added for.
- Call step 2D to find out if transaction codes have been changed in the new release. You can also download this list to a Microsoft Excel sheet and then remove the old transaction codes during the test phase once the testers are satisfied with the new transactions.

See also:

[First Installation Procedure \[Page 99\]](#)

[Migrate Report Trees \[Page 113\]](#)

[Source Release with the Profile Generator \(> SAP R/3 3.0F\) \[Page 111\]](#)



Source Release with the Profile Generator (> SAP R/3 3.0F)

You must perform the following steps after an upgrade, if you were already using the profile generator before the upgrade.

- Choose steps 2A to 2C if you made a large number of modifications in transaction SU24 in the last release. Step 1 (*Initial Filling of Customer Tables*) should only be executed in transaction SU25 if you made no changes in transaction SU24 in the previous release. The system overwrites tables USOBT_C and USOBX_C when it executes step 1, and the values that you maintained in the last release are lost. In steps 2A and 2B, a synchronization procedure is performed.
 - Step 2A

The tables USOBT and USOBX, delivered by SAP, are compared with tables USOBT_C and USOBX_C. You can find a description of the meaning of these tables in [Upgrade Procedure \[Page 109\]](#).
 - Step 2B

If you have made changes to check indicators or field values in Transaction SU24 in the source release, you can compare these with the new SAP default values. If you did not make any changes in transaction SU24 in the source release, the system displays a message informing you that a comparison is not necessary.

The status of the transactions is displayed at the right edge of the list of the transactions to be checked. The status is *to be checked* at first.

By selecting the appropriate menu entry in the list of transactions, you can set the status to *checked*, or reset it to *to be checked* without changing check indicators or field values.

If you want to copy the SAP default values for all transaction that you have not yet checked manually, you can choose the menu entry to copy the remaining SAP default values.

To go to the assignment of check indicators and field values, double click the line of the desired transaction. You can perform the maintenance as described in the documentation for transaction SU24.

The system displays the values delivered by SAP and those that you have maintained next to each other, and you can, if necessary, adjust them.
 - Step 2C

The system displays all roles that are affected by newly added authorization checks and that must be correspondingly supplemented. Edit and regenerate their authorization profiles. The system assigns the status *Profile comparisonrequired* to the affected roles.

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. You should only leave the subprofiles that match your release upgrade in the SAP_NEW profile. The system assigns the status *Profile Comparison Required* to the roles and you can adjust them when you make the next required change: for example, when you are changing the menu for the role.

You can go to the authorization data for a role by double clicking on the corresponding line in the output list.

If you have roles in more than one client, you must perform this step separately in each client to determine the affected roles.



If you are upgrading from SAP R/3 Release 4.0B to SAP R/3 Release 4.6B and you used responsibilities in SAP R/3 Release 4.0B, these are automatically converted to derived roles, which replaced responsibilities in SAP R/3 4.5A (See SAP Note 156250).

- [Migrate the report tree \[Page 113\]](#).



Migrate Report Trees

Use

The report tree data structure was changed in SAP R/3 Release 4.6B. Existing report trees must be adjusted to the changed data structures if they are to continue to be used. This also allows you to put reports in the user menu in the role maintenance.

Procedure

1. Call the transaction RTTREE_MIGRATION. The migration is automatically executed.
Transaction codes are assigned to all reports in a tree during the migration.
2. In the SAP Reference IMG, call *Set Namespace for Report Tree Migration* under the node *Basis* → *System Administration*. You can, if you wish, enter a company-specific prefix for the transaction codes here.