BC Users and Authorizations

HELP.BCCCMUSR

Release 4.0B

Copyright

© Copyright 1998 SAP AG. All rights reserved.

No part of this brochure 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.

SAP AG further does not warrant the accuracy or completeness of the information, text, graphics, links, or other items contained within these materials. SAP AG shall not be liable for any special, indirect, incidental, or consequential damages, including without limitation, lost revenues or lost profits, which may result from the use of these materials. The information in this documentation is subject to change without notice and does not represent a commitment on the part of SAP AG for the future.

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

Microsoft®, WINDOWS®, NT®, EXCEL® and SQL-Server® are registered trademarks of Microsoft Corporation.

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

OSF/Motif® is a registered trademark of Open Software Foundation.

ORACLE® is a registered trademark of ORACLE Corporation, California, USA.

INFORMIX®-OnLine *for SAP* is a registered trademark of Informix Software Incorporated.

UNIX® and X/Open® are registered trademarks of SCO Santa Cruz Operation.

ADABAS® is a registered trademark of Software AG.

SAP®, R/2®, R/3®, RIVA®, ABAP/4®, SAP ArchiveLink®, SAPaccess®, SAPmail®, SAPoffice®, SAP-EDI®, R/3 Retail®, SAP EarlyWatch®, SAP Business Workflow®, ALE/WEB™, Team SAP™, BAPI™, Management Cockpit™ are registered or unregistered trademarks of SAP AG.

Icons

Icon	Meaning
	Caution
	Example
	Note

Contents

BC Users and Authorizations

Overview: Creating and Maintaining User Master Records

The user master record contains all master data for a user in the R/3 System. This section describes how to create and maintain user master records.

You can find out about how to organize the maintenance tasks in the section: Organizing User and Authorization Maintenance [Page 128]

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

If you only want to display a user master record, choose *Tools → Administration, User maintenance → Display users*.

Maintaining User Master Records

User master records are client-specific. You therefore need to maintain individual user master records for each client in your R/3 System.

When you maintain user master records, you assign authorization to individual users in the form of profiles. You can create a user master record in two ways.

You can create a user master record by copying an existing one. However, you can also create a completely new record and then enter the data yourself.

Authorization to Create and Maintain User Master Records [Page 9]

Displaying, Creating and Maintaining User Master Records [Page 10]

Copying User Master Records [Page 16]

Displaying Profile Lists [Page 17]

Maintaining User Defaults and Options [Page 18]

User Master Records and Activity Groups

Activity groups come into play if you create authorization profiles using the Profile Generator. An activity group is a collection of activities (tasks, reports and transactions) for which you can then use the Profile Generator to generate an authorization profile automatically. You then assign the activity group to the user master record as a task profile.

For further information, see the following sections:

Generating Authorization Profiles Automatically with the Profile Generator [Page 79]

Assigning Task Profiles [Page 13]

Comparing Profiles in the User Master Record with Activity Groups [Page 20]

Authorization to Create and Maintain User Master Records

If you want to create or maintain user master records, you need the following three authorizations:

- 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 the user (object S_USER_PRO).
- Authorization to create and maintain authorizations (object S_USER_AUTH).

For further details on these authorizations, see Setting Up User Administrators [Page 135].

Displaying, Creating and Maintaining User Master Records

Displaying User Master Records

If you only want to display a user master record, choose *Tools* → *Administration*, *User maintenance* → *Display users* and enter a user name. You can find detailed information on the contents of the tab displayed later in the section below.

Creating and Maintaining User Master Records

You create and maintain user master records as follows:

1. Choose *Tools* → *Administration*, *User maintenance* → *Users*. This brings you to *User maintenance: Initial screen.*

   If you choose *Measurement data* you can enter measurement-relevant details. You can find further details about this in the *System Measurement Guide - Individual Installation* brochure which is available from SAP. This describes the measurement program which enables you to determine the total number of R/3 users and HR master records which have been set up.

2. Enter an existing user name or create one (by choosing *User names* → *Create).*

   The next screen *Maintain users* contains a series of tab pages for the various categories of user data: Address, Logon data, Fixed values, Task profiles, Authorization profiles and Parameters.

   If you are using the SNC interface, the system displays a corresponding tab page.

   The following tab pages contain fields that you may want to complete:
   Fixed values
   Parameters.
   Users can change this data and their address data by choosing *System* → *User profile* → *Own data* (see Maintaining User Defaults and Options [Page 18]).

   The remaining tab pages *Address, Logon data, Task profiles and Authorization profiles* contain fields that you must complete.

   On the *Address* tab page*, y*ou only have to maintain the *Surname* field. If you want to change the company address, choose *Environment* → *Maintain company address.*

   You can find further information on the remaining tab pages in the following sections:

   Maintaining Logon Data [Page 11]

   Assigning Task Profiles [Page 13]

   Assigning Authorization Profiles [Page 14]

Maintaining Logon Data

Procedure

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

Further information is available by choosing F1.

- *Initial password:* The password for the first logon with the user name. You are required to enter the password twice to eliminate the possibility of typing errors.

  Passwords:

  - are not case-sensitive (the R/3 System does not differentiate between upper- and lowercase letters).
  - must be at least three characters long. Maximum length: Eight characters.

    You can change the minimum password length using system profile parameters. See Setting Password Length and Validity [Page 148] for further details.
  - may contain any characters which can be input from the keyboard. This includes digits, spaces and punctuation marks.
  - may not begin with a question mark or exclamation mark.
  - may not contain spaces within the minimum length. This is normally the first three characters.

    You can set this value using a system profile parameter. See Setting Password Length and Validity [Page 148] for further details.
  - may not begin with three identical characters.
  - may not be PASS or SAP*.
  - may not start with a sequence of three characters which appears in the user name.

    When the user logs on for the first time, he or she must enter a new password. When a user changes his or her password, the new password must be different to each of that user's last five passwords.
  - may not be used if its use has been forbidden. See Specifying Impermissible Passwords [Page 149] for further details.

- *User group:* Enter the name of the user group to which this user is to belong.

  If you want to distribute the user maintenance tasks amongst several user administrators, you must assign the user to a group. Only the administrator with authorization for that group may then change the master record.

  A user master record which is not assigned to a group may be changed by any user administrator.

- *User type:* The system proposes *Dialog* for normal dialog users. If this is not the case for the user in question, change the user type.

  You can use the other user types for special processing tasks, for example, for background processing. Further information is available by choosing F1.

- *Valid from*...*Valid to*... These optional fields allow you to specify a start and end date for the user master record. Leave them blank if you do not want to set a limit.
- *Account Number:* 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.

  A recommended account number would be the user's cost center or company code, for example.

  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.

Assigning Task Profiles

You assign a task profile to users in *Task profiles*.

A task profile is generally a list of individual tasks that are assigned to a particular object. The list of tasks defines the purpose, role and/or the activities of an object in the R/3 System.

Procedure

1. Assign a task profile to an object by choosing *Add*.
2. Select one of the three options in the *Selection* dialog box:
   - Activity group
   - Responsibility
   - Position

   You can find details on these terms in the glossary.
3. You can use a search request to create a link with the user master record for a period of validity to be specified.
4. Save the link you have created.

The link is then included as a new object in the table format.

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

You can post-process the period of validity by clicking on the relevant field in the *Valid from* or *Valid to* column and then using the calendar to choose a new date.

Note that you can extend the columns over the separators. For example, you can display the object name in full-length by widening the second column.

Assigning Authorization Profiles

Procedure

Choose *Profiles* to assign authorization profiles to a user.

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

Profiles issue users with various authorizations.

You should maintain your profile using the Profile Generator unless you have to edit profiles that were created manually.

You can manually maintain profiles by choosing *Tools* → *Administration, User maintenance* → *Profiles* (see Creating and Maintaining Authorizations and Profiles Manually [Page 102]). You can also enter composite profiles (a combination of several profiles) in the user master records when manually maintaining profiles.

If you choose automatic maintenance, the Profile Generator [Page 79] generates an authorization profile on the basis of an activity group. For this, the system parameter `auth/no_check_in_some_cases = Y` must be set (see the system documentation).

From the user maintenance, you can select *Environment* → *Maintain act. group* to branch into the functions for maintaining activity groups and generating profiles. Further details on this topic are contained in: Generating Authorization Profiles Automatically with the Profile Generator [Page 79]

You can assign activity groups to a user by choosing *Environment* → *Maintain activity group*. This simultaneously assigns the appropriate authorization profiles to the user. You can find further details in Assigning Task Profiles [Page 13] and Comparing Profiles in the User Master Record With Activity Groups [Page 20].

The R/3 System contains predefined profiles for all components. A few examples of these are listed below:

- **SAP_ALL**: You assign this profile to users who are to have all R/3 authorizations, including superuser authorization.
- **SAP_NEW**: You assign this profile to users who are to have access to all currently unprotected components. Further details are contained below in the section ”The SAP_NEW Profile”.
- Access authorization for the following user types (R/3 Basis authorizations only)

  System administrator: **S_A.SYSTEM**

  System operator: **S_A.ADMIN**

  Customizer: **S_A.CUSTOMIZ**

  Program developer: **S_A.DEVELOP**

  End user: **S_A.USER**

  Further details are contained in the section Basis Authorizations in Standard Profiles [Page 39].

  In the Customizing documentation you can find information about predefined profiles for SAP work areas. If you want to display this information, choose *Tools* → *Business Engineer* → *Customizing*, *Implementation projects* → *SAP Reference IMG.* You can

then search for the work area documentation regarding authorizations. The individual documentation modules all contain the word ‘authorization’.

You can find information about the SAP naming convention for predefined profiles in the section Naming Convention for Pre-Defined Profiles [Page 111].

The SAP_NEW Profile

The SAP_NEW profile is a composite profile which is supplied by SAP in every Release or upgrade level. It contains a single profile, SAP_NEW_<Release> with new authorizations for each new Release or upgrade level, for example, SAP_NEW_30D. SAP_NEW is included in every SAP delivery.

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 which were not previously executed. This ensures upwards compatibility.

For this reason you should assign SAP_NEW to all user master records.

As system administrator, you decide which users should receive the new authorizations following a Release upgrade.

- You need to add the new authorizations to manually generated profiles
- Following a Release or upgrade you need to regenerate all authorization profiles which have been generated using the Profile Generator.

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.

Once you have carried out these tasks, delete the single SAP_NEW_<release> profiles from the SAP_NEW profile.

Copying User Master Records

You can create a user master record by copying an existing one. You can also copy defaults, addresses and parameter settings.

You copy user master records as follows:

1. Choose *User names* → *Copy*. Enter the names of the source and target users.
2. On the following screen you can edit the new user master record as required.

You can also rename user master records if you simply want to replace one record with an identical one of a different name.

Displaying Profile Lists

You can display a list of authorization profiles defined in the system, from which you can select profiles.

Choose *User maintenance* → *Profiles* from the *Maintain users: Profiles* screen.

By choosing *Values* you can display the individual profiles. In the first line of the screen is the profile name, for example, SAP_ALL. The following details are displayed for each authorization in the profile:

- *Object:* The authorization object
- *Authorization:* The authorization assigned to the object
- *Field:* The fields in the authorization object

  A user has authorization for an object if he or she satisfies the authorization check for each field in that object. Otherwise the user cannot execute any action which is protected by that object.
- *Values:* The set of values contained in an authorization. The R/3 System uses these values to check a user's authorization.

The Infosystem provides you with additional information on profile lists according to complex search criteria. See Using the Infosystem [Page 30].

Maintaining User Defaults and Options

Both system administrators and individual users can maintain user data.

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

Users can maintain the following user data: *Defaults*, *Addresses* or *Parameters*

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

Maintaining Own User Data

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

Choose F1 to call Help on the fields. F4 displays the input values that are available.

Defaults

You can set the following defaults:

- Start menu

  A function (menu name) which is automatically started when the user logs on.

- Logon language

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

- Printer
- Spool control
- Personal time zone (different from the company time zone in *Address,* crucial with RFC)
- Date format
- The format for decimals
- CATT check indicators

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

User Address

The user address data fields are self-explanatory.

Company addresses can only be maintained by the system administrator (*Environment → Maintain co. address).*

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

Parameters

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

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

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

Comparing Profiles in the User Master Record with Activity Groups

Activity groups or their assignment to user master records can be delimited. 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.

For the changes in the user master record to be effective, the comparison must take place 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 RHAUTUP1 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.

   Further details on report RHAUTUP1 are contained in the report documentation.

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.

   In Transaction PFUD you are informed if a complete comparison is necessary (if, for example, the last complete comparison - perhaps using RHAUTUP1 - was unsuccessful).

   To ensure that the authorization profiles in the user master records are always current, you should always execute a complete comparison (choose *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 both report RHAUTUP1 and Transaction PFUD:

- *Take organizational plan into account*

  Authorization profiles are included for a user which are ”inherited” due to the user’s place in the organizational structure.

- *Generate flagged activity groups*

  Authorization profiles are generated for planned, but not yet generated, activity groups.

- *Delete expired authorization profiles*

  If the selection dialog is displayed, you select all of the authorization profile assignments you want to delete. If the dialog is not displayed, all expired

authorization profile assignments are automatically removed from the user master record.

- *Create new authorization profiles*

  Assigning Authorization Profiles [Page 14]

In Transaction PFUD you additionally have the following options:

- *Display selection dialog*

  The system displays a selection dialog in which the user can choose for which users changes and generation of profiles should take place.

  The system displays a list which shows the individual actions necessary to compare the authorization profiles with the user master record.

  For each user, the profiles which need to be added to the user master record are displayed first (*Insert*), followed by the profiles to be deleted (*Delete*).

  In the final part of the table, if necessary, the system displays the authorization profiles which need to be regenerated because of changes to the activity groups (*Generate*).

  The system displays a checkbox for each action. When you choose *Compare User Master*, only the actions you have marked are executed.

  If you choose *Insert Lines*, you can select profiles to add to the user master. Similarly, choosing *Delete Lines* allows you to select profiles to be deleted from the user master. There are two additional pushbuttons which you can use to select or deselect all activities for a user. The *Generate all profiles* pushbutton is self-explanatory.

  There are two more pushbuttons which you can use to select or deselect all activities for a user. To do this, the cursor must be positioned on the line containing the appropriate user name.

  The checkboxes are filled in according to your choices for the G*enerate flagged activity groups*, D*elete expired authorization profiles* and A*dd new profiles* checkboxes on the selection screen.

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.

Locking and Unlocking User Master Records

You can grant or deny a user access to the system by selecting *User names* → *Lock / Unlock* from the *User maintenance* initial screen. Locking or unlocking a user master record takes effect the next time a user attempts to log on. Users who are logged on at the time that changes are made are not affected.

The system automatically locks users if twelve successive unsuccessful attempts are made to log on. The lock is recorded in the system log, along with the terminal ID of the machine where the logon attempt took place.

You can set the number of permissible unsuccessful logon attempts in a system profile parameter. See Limiting Logon Attempts and Predefining Clients [Page 146] for further details.

This automatic lock is released by the system at midnight. You can also remove the lock manually before this time. Locks that you specifically set yourself apply indefinitely until you release them.

Changing Passwords

You can set a new password for a user by choosing *User names* → *Change password* from the *User maintenance* initial screen, or by choosing the corresponding pushbutton.

This new password must fulfill the standard conditions regarding permissible passwords. Further details are contained in Displaying, Creating and Maintaining User Master Records [Page 10].

New passwords are immediately effective. If users forget their password, they can use the new one as soon as it has been set.

Users may change their passwords no more than once a day.

System administrators, on the other hand, may change user passwords as often as necessary.

Displaying Change Documents

By choosing *Information* → *Information system*, *Change documents* from the *User maintenance* initial screen, you can display a list of changes to user master records, authorization profiles and authorizations. The system logs the following changes:

- Direct authorization changes in a user record

  These are changes to the profile list in the user master record

  Indirect changes are changes to profiles and authorizations which are contained in the user master record. These changes cannot be seen in the display. You can, however, see them in the change documents for profiles and authorizations.

- Changes to user passwords, user type, user group, validity period and account number

For each change made, the log shows the deleted value in the *Deleted entries* line. The changed or new value is displayed in the *Added entries* line.

Archive Change Documents

User master records and authorizations are saved in USR* tables. You can reduce the amount of space that these take up in the database by using the archiving function. Change documents are saved in USH* tables. The archiving function deletes change documents that are no longer required from the USR* tables.

You can archive the following change documents or change documents relating to user master records and authorizations from the USH* tables:

- Changes to authorizations (archiving object US_AUTH)
- Changes to authorization profiles (archiving object US_PROF)
- Changes to the authorizations assigned to a user (archiving object US_USER)
- Changes to a user's password or to defaults stored in the user master record (archiving object US_PASS)

Each main function involving user and authorization maintenance (users, profiles and authorizations) allows its own access to the archiving system. From the appropriate maintenance function, choose *Utilities* → *Archive and read*. On the subsequent screen, you can archive change documents for users, profiles or authorizations, or re-load already archived documents.

You can find more detailed information about the archiving system in the *System Services* section of the Basis documentation on CD-ROM.

Changing Several User Master Records

There are two possibilities within the R/3 System for changing more than one (or even all) user master records. From the *User maintenance* initial screen, selecting:

- *Environment* → *Mass changes* → *Delete all users*, you can delete all user master records from a client. Before the deletion takes place, the system displays a screen on which you must confirm that you really want to delete all records. At this point, you may cancel the procedure.
- *Environment* → *Mass changes* → *User profile*, you can insert or delete a profile in a selection of user master records or in all user master records.

For further details on the authorizations necessary for this, see Setting Up User Administrators [Page 135].

Where is User and Authorization Data Stored?

The user and authorization data which you maintain using *Tools* → *Administration, User maintenance* is stored in invisible tables (with the exception of table USR40).

The names and contents of these tables are as follows:

Menu option	Table	Contents
Users	USR01	User master record (runtime data)
Users	USR02	Logon data
Users	USR03	User address data
Users	USR04	User master record: Authorizations
Users	USR05	User master record: Parameter ID
Profiles	USR10	User master record: Authorization profiles
Profiles	USR11	User master record: Texts for profiles (USR10)
Authorization	USR12	User master record: Authorizations
Authorization	USR13	Short texts about authorizations
Users	UST04	User master records (transparent table for USR04)
Profiles	UST10 C	User master record: composite profiles (transparent table for USR 10)
Profiles	UST10S	User master record: Single profiles (transparent table for USR 10)
Authorization	UST12	User master record: Authorizations (transparent table for USR 12)
Users	USH02	Change history for logon data
Users	USH04	Change history for users
Profiles	USH10	Change history for authorization profiles
Authorization	USH12	Change history for authorizations
System → Services → *Ext. table maintenance*	USR40	Table of non-permitted passwords

Creating and Maintaining Internet Users

To create an activity group, choose *Tools* → *Administration*, *User maintenance* → *Internet users*.

You should proceed as follows:

1. Enter an ID for the Internet user.

   The Internet user is identified internally by a user ID and a user type. The user type related to the Internet transactions that the user wants to execute. When you create an Internet user, you are prompted to enter a user type. If you make changes to the Internet user, the user type is only requested if it is not unique. Otherwise the system displays a selection of user types for which the user with the specified ID exists.

2. Initialize the user.

   The initial password is assigned automatically.

You can lock, unlock, delete or rename an Internet user at any time. You may also change the user's password.

The associated data is managed centrally in table BAPIUSW01.

Using the Infosystem

You can access the Infosystem by selecting *Tools* → *Administration*, *User maintenance* → *Information* → *Information system*.

You find details on using the report tree by choosing *Help* → *Extended help*, or by choosing *Utilities* → *Online manual*.

In the hierarchy tree you can use a range of selection criteria for the following objects:

- Users
- Profiles
- Authorization objects
- Authorizations
- Activity groups
- Transactions
- Comparisons
- Where-used lists
- Change documents

You can display the node attributes for each node in the report tree by choosing the relevant symbol.

You can display a key for the different levels by choosing *Utilities* → *Color key.*

If you want to find a particular node, choose *Edit* → *Find*.

If you want to find authorizations with the generic value *, you should note the following:

A star (*) is regarded as a formatting character in the input field on the selection screen.

The character # removes the star as a formatting character.

Therefore you should use the character string #* for a generic search.

Expanding the Report Tree

Click on a node in the hierarchy if you want to expand the node underneath it.

If you want to see all levels of a hierarchy assigned to a node, select the node and choose the icon to expand the hierarchy.

You can expand and collapse the tree structure by selecting it and choosing the appropriate icon.

You can also choose a part of the report tree by selecting the appropriate note and choosing *Set focus.* All nodes with the exception of the selected node and its sub-nodes are hidden.

Using Selection Criteria With Objects

To restrict an object according to specific selection criteria, double-click on the selection criteria, or select it and choose *Execute*.

You can also restrict an object according to selection criteria in the background. To do this, choose *Nodes* → *Exec. in background*.

Overview: Authorizations, Profiles and the Profile Generator

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 128].

You can generate authorization profiles either *manually* or *automatically using the Profile Generator*.

If you want to maintain authorizations and profiles manually, you need detailed knowledge of all SAP authorization components.

If, on the other hand, you use the Profile Generator, you do not need such detailed knowledge. As a result, implementing an R/3 System requires considerably less time and effort.

The Profile Generator creates profiles automatically based on selected menu functions. These are then presented for fine-tuning. The Profile Generator can be integrated with HR-Org (Organization management, time dependency).

If you want to use the Profile Generator, you are strongly recommended to read the example scenario and the helpful hints.

If you want to administer users or authorizations centrally for several clients or R/3 Systems, you should execute transports. Further details are contained in the section Transporting User Master Records, Authorizations and Profiles [Page 124].

If you want to include authorization checks in your own developments, see Adding Authorization Checks To Your Own Developments [Page 118].

Basics and concepts

The SAP Authorization Concept [Page 33]

Basis System Authorizations [Page 37]

Automatic maintenance with the Profile Generator

Reducing the Scope of Authorization Checks [Page 71]

Generating Authorization Profiles Automatically with the Profile Generator [Page 79]

The Profile Generator : An Example [Page 93]

The Profile Generator: Helpful Hints [Page 100]

Manual maintenance

Creating and Maintaining Authorizations and Profiles Manually [Page 102]

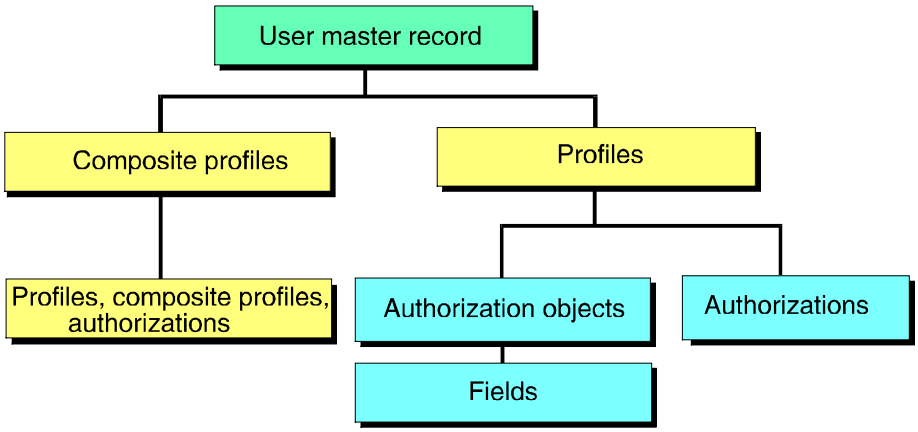
The SAP Authorization Concept

Authorization checks allow you to protect any functions or objects you choose within the R/3 System.

The programmer decides which aspects of a function should be checked, and how.

The system administrator creates authorizations, which are assigned to individual users in collections called profiles. Generally speaking, profiles are created using the Profile Generator, although they can also be generated manually.

The following graphic shows the authorization components and explains their relationship. You can display an explanation by clicking on one of the components. Examples in the explanations relate to the Authorization Check Scenario [Page 36].



For details on the graphic, see the following explanations:

User Master Records [Ext.]

Profiles [Ext.]

Authorizations [Ext.]

Authorization Objects [Ext.]

Fields [Ext.]

For further details, see the following sections:

Assigning Authorizations [Page 34]

Authorization Checks [Page 35]

Authorization Check Scenario [Page 36]

Assigning Authorizations

The R/3 system administrator (or a designated sub-administrator, see Organizing User and Authorization Maintenance [Page 128]) is responsible for assigning authorizations.

By assigning Authorizations [Ext.], the administrator determines (within the range of possibilities defined by the programmer) which functions a user may execute or which objects he or she may access.

As an administrator, you are responsible for the following:

- Maintaining authorizations for each authorization object

  An authorization is the combination of permissible values in each authorization field of an authorization object.

- Generating authorization profiles

  Authorizations are grouped in authorization profiles in such a way that the profiles describe work centers, for example, *flight reservation clerk*.

  The system administrator can create authorization profiles in two ways:

  – Automatically, based on activity group maintenance (*Tools* → *Administration*, *User maintenance* → *Activity groups*), using the Profile Generator.

    Further details on this topic are contained in: Generating Authorization Profiles Automatically with the Profile Generator [Page 79].

  – Manually, by choosing *Tools* → *Administration*, *User maintenance* → *Profiles*

    For more information, see Creating and Maintaining Authorizations and Profiles Manually [Page 102].

    You can combine profiles and single authorizations to form composite profiles using the manual maintenance tool. Composite profiles are not strictly necessary, but they do make system administration easier.

- Assigning authorization profiles to a user master record

  You assign one or more authorization profiles (work centers) to a user master record.

When an authorization check takes place, the system compares the values entered by the system administrator in the authorization profile with those required by the program for the user to execute a certain activity.

Authorization Checks

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

During an authorization check, the system compares the values assigned by the system administrator in an authorization profile with the values specified in the program which are necessary to execute a certain action.

A user may only execute the action if the authorization check is successful for every field in the authorization object.

Authorization checks are triggered by the ABAP `AUTHORITY-CHECK` statement. The programmer then 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.

When R/3 transactions are executed, a large number of Authorization Objects [Ext.] are often checked, since the transaction calls other work areas in the background. In order for these checks to be executed successfully, the user in question must have the appropriate authorizations. This results in some users having more authorization than they strictly need. It also leads to an increased maintenance workload. You can deliberately disable such authorization checks by setting the Check Status [Ext.] in Transaction SU24.

Authorization Check Scenario

Suppose a programmer wants to impose an authorization check before bookings for business customers can be changed.

To do this, the programmer should create an authorization field (**ACTVT** and **CUSTTYPE**) and assign for each field defined the value to be checked (**02, B**), by choosing *Tools* → *ABAP Workbench*, *Development* → *Other Tools* → *Authorization Objs* → *Fields*. For more information, see Creating Authorization Fields [Page 119].

The programmer should also create an authorization object (here **S_TRVL_BKS**) by choosing *Tools* → *ABAP Workbench, Development* → *Other tools* → *Authorization objects* → *Objects*, and then assign the authorization object to an object class. For more information see Creating Authorization Objects [Ext.] and Assigning Authorization Objects to an Object Class [Page 121].

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

```
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 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 (**ACTVT** field).

  Users with this authorization may change all customers' bookings.

- **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 customers' 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 Meyer on the other hand is only authorized to display the records (**S_TRVL_CUS2**) and therefore cannot change bookings.

Basis System Authorizations

This topic reviews authorizations for components of the Basis System.

You can also find information on system authorizations for the Basis System and SAP applications in the Customizing system. From the initial screen, choose *Tools → Business Engineer → Customizing, Implement. projects → SAP Reference IMG.* Then search for ”user” or ”authorization” to find the relevant sections of the Guide.

Authorizations in Production Systems [Page 38]

Basis Authorizations In Standard Profiles [Page 39]

Basis Authorizations Components [Page 41]

You can generate authorizations and profiles automatically on the basis of selected menu functions. see Generating Authorization Profiles Automatically With the Profile Generator [Page 79].

Authorizations in Production Systems

You should not assign the authorizations shown in the following list to users in production systems. No modifications of the R/3 System should be performed in a production system.

- ABAP Workbench development authorizations (*ABAP Workbench* (S_DEVELOP)and *Change and Transport Organizer* authorization objects (S_TRANSPRT))
- Executing operating system commands from within the R/3 System (Transaction SM52) (*System Authorizations* (S_ADMI_FCD) value *UNIX*).

Basis Authorizations In Standard Profiles

You can use predefined profiles to give the Basis authorizations required for standard system administration jobs. These profiles contain the sets of authorizations that are required for executing such jobs as central administrator (superuser) or system administrator.

Using the Profile Generator, you can easily adapt a standard profile to your own requirements. Further details are contained in the section Defining Profiles and Authorizations [Page 106].

See the profile display in the R/3 System for information on which component authorizations are contained in each profile.

The profiles are as follows:

- **SAP_ALL**: For the superuser. Contains unrestricted authorizations for the entire SAP R/3 System, including both the Basis System and applications.
- **S_A.SYSTEM**: For the central system administrator. Contains all authorizations for the SAP Basis System, but no authorizations for the R/3 applications.

  This profile allows full access to users and authorizations.
- **S_A.TMSADM**: For RFC user TMSADM of the Transport Management System.

  This profile is assigned to user TMSADM as the user is generated. This provides authorization to execute the TMS basic functions.
- **S_A.ADMIN**: For an operator or system administrator who is responsible for overseeing the operation of an R/3 System.

  The profile contains all Basis authorizations with the following restrictions:

  – No authorizations for the ABAP Workbench

  – No authorization to modify the superuser (users in group SUPER)

  – No authorization to modify the standard profiles in this list (profile names beginning with "S_A").
- **S_A.CUSTOMIZ**: For users working with the SAP Customizing system (*Tools* → *Customizing*).
- **S_A.DEVELOP**: For developers working with the ABAP Workbench. The profile excludes authorizations for system administration and for user / authorization maintenance.
- **S_A.USER**: For end users. Contains all of the Basis authorizations required by ordinary users of your R/3 System.

  This profile does not contain authorizations for SAP applications. Use the standard profiles that are provided by the applications to give these authorizations.
- **S_A.DOKU**: Contains authorizations to develop and release documentation in the R/3 System.
- **S_A.SHOW**: Contains display authorizations for Basis functions. This profile is especially suitable for auditors.

As of Release 2.1D, the initial set of Basis profiles that was delivered with the R/3 System (profile names beginning with "S_" and not including "S_A.") will no longer be maintained. In a future release, they will be withdrawn in favor of the standard profiles described above.

If you use the "S_" profiles, please replace them with the standard profiles listed above or copy them to private profile names, as described in Naming Convention for Predefined Profiles [Page 111].

Basis Authorization Components

The table below shows the components with their authorization objects. For detailed information, see the following topics or the online authorization object documentation.

ABAP and the ABAP Workbench

Component	Authorization objects
ABAP programming language and Workbench	*ABAP: Program Run Checks* (S_PROGRAM): run programs, schedule background jobs. *ABAP Workbench* (S_DEVELOP): Development authorizations for all Workbench components except the Workbench Organizer: ABAP Workbench Menu Painter Screen Painter ABAP Dictionary Data Modeler Application hierarchy Repository Browser Information System Function Builder Transaction management (table TSTC maintenance) ABAP trace and SQL trace Authorization object maintenance *Correction and Transport Organizer* (S_TRANSPRT): Authorizations for creating development projects and objects **Standard profile** for end users (run programs only): S_A.USER **Standard profile** for developers (all development tasks): S_A.DEVELOP For more information, see ABAP and Workbench Authorizations [Page 49].
ABAP Dictionary	For more information, see ABAP Dictionary Authorizations [Page 51].
ABAP Query	*Authorization for ABAP Query* (S_QUERY): Run and maintain queries. **Standard profile** for end users (run queries): S_A.USER **Standard profile** for maintaining queries: S_A.DEVELOP For more information, see ABAP Query Authorizations [Page 50].

Matchcodes	*ABAP Workbench* (S_DEVELOP): Maintaining matchcodes User-programmable exit routine. Naming convention: MC_<Name of matchcode object>& **Standard profiles**: S_A.USER, S_A.ADMIN For more information, see Matchcode Authorizations [Page 52].
Customizing (IMG)	*IMG: Authorization for Generating the Enterprise IMG* (S_IMG_GENE): Generate the Customizing model to be used for all Customizing projects in the R/3 System. Should be restricted to high-level users. *IMG: New Authorizations for Projects* (S_PRO_AUTH): Authorization to display or make changes to a Customizing project. The authorization is assigned by project number. **Standard profiles**: S_A.CUSTOMIZ (both authorizations) For more information, see SAP Customizing System Authorizations [Page 53].
Table contents	*Table Maintenance (Using Standard Tools)* (S_TABU_DIS): Maintain table entries. *Table Maintenance for Client-Independent Tables* (S_TABU_CLI): Maintain entries in cross-client tables. Applies to table entry maintenance with the standard and extended table maintenance (Transactions SM30, SM31), and the Data Browser, and to table entry maintenance in the Customizing system. **Standard profiles** (no authorization for cross-client tables): S_A.USER, S_A.DEVELOP **Standard profiles** (with authorization for cross-client tables): S_A.ADMIN, S_A.CUSTOMIZ, S_A.SYSTEM For more information, see Authorizations for Table and View Entries [Page 54].
Field selection editor	*Central Field Selection* (S_FIELDSEL): Specify field selection rules. **Standard profiles**: S_A.DEVELOP, S_A.ADMIN For more information, see Field Selection Editor Authorizations [Page 56].

Maintain online documentation with SE61	*Authorization for Document Maintenance* (S_DOKU_AUT): Create and maintain documentation. **Standard profiles**: S_A.ADMIN, S_A.CUSTOMIZ, S_A.SYSTEM For more information, see Online Documentation Authorizations [Page 57].
Transport and correction system, Workbench Organizer	*Correction and Transport Organizer* (S_TRANSPRT): Create corrections and transport requests, perform transports. **Standard profiles**: S_A.DEVELOP, S_A.CUSTOMIZ, S_A.ADMIN, S_A.SYSTEM For more information, see Correction and Transport Authorizations [Page 58].

R/3 System Administration

Component	Authorization objects
User master records	*User Master Maintenance: User Groups* (S_USER_GRP): Maintain user master records. For further information, see Setting Up User Administrators [Page 135]. **Standard profiles**: S_A.ADMIN (restricted), S_A.SYSTEM (unrestricted)
Authorization profiles	*User Master Maintenance: Authorization Profile* (S_USER_PRO): Maintain authorization profiles For further information, see Setting Up Authorization and Activation Administrators [Page 138]. **Standard profiles**: S_A.ADMIN (restricted), S_A.SYSTEM (unrestricted)
Authorizations	*User Master Maintenance: Authorizations* (S_USER_AUT): Maintain authorization profiles. For further information, see Setting Up Authorization and Activation Administrators [Page 138]. **Standard profiles**: S_A.ADMIN (restricted), S_A.SYSTEM (unrestricted)
GUI activities	*Authorization for GUI Activities* (S_GUI): Authorization to download lists to local files (list download)

System monitoring functions	*System Authorizations* (S_ADMI_FCD): Operations on work processes and sessions other than user's own update records. **Standard profiles**: S_A.ADMIN, S_A.SYSTEM For more information, see System Administration Authorizations [Page 59].
Update record management tool	*System Authorizations* (S_ADMI_FCD): Execute operations on entries other than user's own. Users do not need an authorization to display update records or execute operations on their own records. **Standard profiles**: S_A.ADMIN, S_A.SYSTEM For more information, see System Administration Authorizations [Page 59].
System log	*System Authorizations* (S_ADMI_FCD): Start component. **Standard profiles**: S_A.ADMIN, S_A.SYSTEM
System trace	*System Authorizations* (S_ADMI_FCD): Set options, trace authorizations. **Standard profiles**: S_A.ADMIN, S_A.SYSTEM For more information, see System Administration Authorizations [Page 59].
Copy clients	*Table Maintenance for Client-Independent Tables* (S_TABU_CLI): Copy tables from one client to another. *Table Maintenance (Using Standard Tools)* (S_TABU_DIS): Maintain table CCCFLOW. *System Authorizations* (S_ADMI_FCD): Create new client in table T000 with the SAP Customizing system. *User Master Maintenance: User Groups* (S_USER_GRP): Copy user master records from one client to another (optional). **Standard profiles**: S_A.SYSTEM For more information, see Authorizations for Creating and Copying Clients [Page 60].
Transaction locking	*System Authorizations* (S_ADMI_FCD): Lock, unlock transactions. **Standard profiles**: S_A.ADMIN, S_A.SYSTEM For more information, see System Administration Authorizations [Page 59].

Computing center management system	*CCMS: System Administration* (S_RZL_ADM): Use management system display, management functions. **Standard profiles**: S_A.ADMIN, S_A.DEVELOP, S_A.SYSTEM *Tools Performance Monitor* (S_TOOLS_EX): Use the RDBMS-Specifics function in the CCMS and the performance monitor. *Authorization to Execute Logical Operating System Commands* (S_LOG_COM): Use the CCMS planning calendar for database administration. **Standard profiles**: S_A.SYSTEM For more information, see Authorizations for the Computing Center Management System [Page 61].
Operating system commands in R/3	*CCMS: System Administration* (S_RZL_ADM): Define operating system commands in the R/3 System. Commands are saved in the database. **Standard profiles**: S_A.ADMIN, S_A.SYSTEM *Authorization to Execute Logical Operating System Commands* (S_LOG_COM): Use the CCMS planning calendar for database administration. **Standard profiles**: S_A.ADMIN, S_A.SYSTEM
Performance monitor	*Tools Performance Monitor* (S_TOOLS_EX): Access to special functions. **Standard profiles**: S_A.SYSTEM For more information see Performance Monitor Authorizations [Page 62].
Early watch	*Background Processing: Background Administrator* (S_BTCH_ADM): Administrator access. *ABAP Workbench* (S_DEVELOP): Type SYST authorization for using debugging tools. *Computer Center Management System: System Administrator* (S_RZL_ADM): Use management system display, management functions. *Tools Performance Monitor* (S_TOOLS_EX): Use the *RDBMS Specifics* function in the CCMS and the performance monitor. **Standard profiles**: None.

Background processing	*ABAP: Program Runtime Checks*: Submit ABAP programs for background processing. *Background Processing: Operations on Background Jobs* (S_BTCH_JOB): Additional end-user actions in the job monitor (delete your own jobs, for example). *Background Processing: Background User Name* (S_BTCH_NAM): Specify a runtime authorizations user other than your own user. *Background Processing: Background Administrator* (S_BTCH_ADM): Full access to all functions for administrators. *ABAP Workbench* (S_DEVELOP): Use debugging functions on background jobs. **Standard profiles**: All S_A.* profiles contain background processing authorizations. S_A.USER can only schedule jobs. For more information, see Background Processing Authorizations [Page 63].
Batch input	*Batch Input Authorizations* (S_BDC_MONI): Run, manage sessions. **Standard profiles**: All S_A.* profiles. S_A.USER is limited to running and analyzing sessions For more information, see Batch Input System Authorizations [Page 64].
Queue management	*Queue Management Authorizations* (S_QIO_MONI): Use function. **Standard profiles**: S_A.ADMIN, S_A.SYSTEM For more information, see Queue Management Authorizations [Page 65].
Spool system, use output devices	*Spool: Device Authorizations* (S_SPO_DEV): Authorization to use a particular output device (by name in the SAP spool system). **Standard profiles**: All S_A.* profiles For more information, see Queue Management Authorizations [Page 65].
Spool system, manage spool requests; define and manage output devices and associated objects	*System Authorizations* (S_ADMI_FCD): Display requests other than user's own, use management functions. **Standard profiles**: S_A.ADMIN, S_A.SYSTEM For more information, see Spool System and TemSe Database Authorizations [Page 66].

Spool system, manage spool requests that have authorization protection	*Spool: Actions* (S_SPO_ACT): Execute operations on spool requests that are protected by authorization strings. **Standard profiles**: S_A.ADMIN, S_A.SYSTEM For more information, see Spool System and TemSe Database Authorizations [Page 66].
TemSe (temporary sequential object) database	*System Authorizations* (S_ADMI_FCD): Manage TemSe objects (spool request data, job logs from the background processing system. **Standard profiles**: S_A.ADMIN, S_A.SYSTEM For more information, see Spool System and TemSe Database Authorizations [Page 66].
Lock management	*Enqueue: Display/Delete Lock Entries* (S_ENQUE): Display, manage lock entries other than user's own entries, use special management functions. Users do not need an authorization to display their own lock entries. **Standard profiles**: S_A.ADMIN, S_A.SYSTEM For more information, see System Administration Authorizations [Page 59].
SAP communications server	*SAPcomm Server Authorization* (S_SKOM_SRV): Required authorization for the CPI-C user that is used for SAPcomm logons. **Standard profiles**: S_A.SYSTEM
Text processing (SAPscript)	*SAPscript: Standard Text* (S_SCRP_TXT): Edit texts. *SAPscript: Style* (S_SCRP_STY): Edit styles. *SAPscript: Form* (S_SCRP_FRM): Edit forms. **Standard profiles**: All S_A.* profiles For more information, see SAPscript Text Processing Authorizations [Page 67].
Factory calendars	*Public Holiday and Factory Calendar Maintenance* (S_CALENDAR): Display, maintain calendars. **Standard profiles**: S_A.CUSTOMIZ, S_A.SYSTEM, S_A.USER (display only) For more information see Holiday and Factory Calendar Authorizations [Page 68].

Number ranges	*Number Range Maintenance* (S_NUMBER): Display, maintain number ranges. **Standard profiles**: S_A.CUSTOMIZ, S_A.SYSTEM, S_A.USER (display only) For more information, see Number Range Authorizations [Page 69].
Change documents	*Change Documents* (S_SCD0): Display, maintain change documents. **Standard profiles**: All S_A.* profiles (S_A.USER has only restricted access) For more information, see Change Document Authorizations [Page 70].
Central address management	*Central Address Management: Address Type 1 (Organization, Company)*(S_ADDRESS1): Use the central address management facility. **Standard profiles**: S_A.SYSTEM, S_A.USER (display only)
Application log	*Applications Log* (S_APPL_LOG): Use the application logging facility. **Standard profiles**: S_A.SYSTEM, S_A.USER (display only)
System profile	*Tools Performance Monitor* (S_TOOLS_EX): Display and maintain system profile parameters from within the R/3 System. **Standard profiles**: S_A.SYSTEM
Language installation	*Language Administration* (S_LANG_ADM): Import additional R/3 System languages. **Standard profiles**: S_A.ADMIN, S_A.CUSTOMIZ, S_A.SYSTEM

For information on defining authorizations for other Basis components and for R/3 applications, see the documentation of the components.

ABAP and Workbench Authorizations

The system tests access to the ABAP programming language with the following authorization objects:

- S_PROGRAM, ABAP: *Program Run Checks*:
  Run ABAP programs and maintain variants, attributes, and texts.
- *S_DEVELOP, ABAP Workbench*:
  Create or edit programs and use the tools of the ABAP Workbench.
- *S_TRANSPRT, Change and Transport Organizer*:
  Create corrections and transport requests and move system objects from one system to another.
- S_DATASET, *Authorization for File Access*
  Accessing operating system files and executing operating system files.
- S_CPIC, *CPI-C Calls from ABAP Programs*
  Calling CPI-C functions from ABAP programs (COMMUNICATION statement).
- S_C_FUNCT, *C Calls in ABAP Programs*
  Calling C-kernel functions directly.
- S_OLE_CALL, *OLE Calls from ABAP Programs*
  Calling OLE applications from the SAP frontend.

Running Programs

Use the *ABAP: Program Run Checks* authorization object to allow users to run programs and perform such runtime tasks as maintaining variants.

Editing Programs and Using the ABAP Workbench

Use the *ABAP Workbench* object to authorize users to create and modify programs and use the ABAP Workbench tools.

An authorization for *Change and Transport Organizer* is also required to create programs, screens, and other objects. A typical developer should have authorization only to create corrections (tasks). Only project leaders should have the authority to create transport requests or execute transports.

ABAP Query Authorizations

The system uses user group assignments and the authorization object *Authorization for ABAP Query* to test access to the ABAP Query facility.

You can define the following types of authorizations:

- Run queries. A user must be assigned to the appropriate user group to run a query. No authorization for the *Query* object is needed.
- Run and maintain queries. A user must have the "02" *Query* authorization and belong to the required user group.
- Run and maintain queries, maintain user groups and functional areas. An administrator must have the "23" *Query* authorization. To run or maintain a query, an administrator must also belong to the appropriate group.

ABAP Dictionary Authorizations

The system uses the authorization object *ABAP Development Workbench* to test whether a user may:

- display or maintain objects by type, development class, and name in the ABAP Dictionary
- use the database utility of the ABAP Dictionary.

  Menu path: *Utilities* → *Database utility* in the *ABAP Dictionary: Initial screen*.

There is no authorization test for the ABAP Dictionary information system (Transaction SE15).

Matchcode Authorizations

The system uses the authorization object *ABAP Workbench* to test whether a user may create or maintain matchcodes.

For end-user access testing, you can define matchcodes to require an authorization check before records can be displayed. This check takes place in an exit routine and can use any authorization object.

The matchcode exit routine must obey the following naming convention: MC_<Name of matchcode object>&

For more information on matchcode authorizations, see the *ABAP Dictionary* guide.

SAP Customizing System

Access to projects in the Customizing system (*Tools → Business Engineer → Customizing*) is protected by the following three authorization objects:

- IMG: Authorization for Generating the Enterprise IMG (S_IMG_GENE): A user with this authorization can generate the Customizing model that is used for all Customizing projects in the R/3 System. The assortment of SAP components that is to be customized is determined when the enterprise IMG is generated, for example.

  Authorization to this object should be restricted to only a few higher-level users.

- IMG: New Authorization for Projects (S_PRO_AUTH): With this authorization, a user can either display or also work in a particular Customizing project. The authorization is assigned by Customizing project number.

- Table maintenance authorizations: A user must be authorized for the tables that he or she wants to change in a Customizing function. For more information, see Authorizations for Table and View Entries [Page 54].

Authorizations for Table and View Entries

The contents of most system and Customizing tables and views -- the tables which govern the operation of the R/3 System -- are protected by the authorization objects *Table maintenance (Using Standard tools)* (S_TABU_DIS) and *Maintenance of Client-Independent Tables* (S_TABU_CLI). The system tables and views are included in delivery classes S and E, the Customizing tables and views are in delivery classes C and G. These tables control the R/3 System.

Table maintenance authorizations apply to maintenance of table and view contents with the standard table tools:

- System → Services → Table maintenance
- *Extended table maintenance* (Transaction SM30 or table maintenance functions in application programs)
- *ABAP Data Browser* (Transaction SE16).

You must have table maintenance authorizations to maintain tables in the Customizing system (IMG).

Authorization Structure

A user who wants to maintain a table must have:

- an authorization for the table's authorization class and the activity "maintain" (*Table Maintenance (Standard tools)*
- if the table is client independent, the user must also have the global authorization for such tables (*Table Maintenance of Client-Independent Tables*). The authorization test applies only to tables in delivery classes C (customer), G (customer table with SAP entries), and E (system table, modifiable by customers)

  You should restrict access to client-independent tables to those users who understand the possible effects of changes to these tables.

Table Application Classes

SAP has defined a default set of application classes for tables and views and has assigned all standard tables and views to the application classes.

The name of an application class may be up to four characters long. For the default application classes, SAP has defined two-character names that conform to the naming convention shown below:

- First character: The code letter for each SAP application
- Second character: One of the following three code letters, indicating the class of table:
  - **S**: System table (includes tables of delivery classes S and E).

    System tables are control tables (tables used by programs in the course of their execution) which are of an internal nature and which usually are maintained only by SAP.

    Example: the TSTC transaction table.
  - **C**: Customer table (includes tables of delivery classes C and G).

Customer tables are control tables which you must customize in the course of setting up and operating your system. Most of them are accessible through the Customizing system and/or special maintenance transactions.

Example: Currency exchange tables.

- **A**: Application table (delivery class A).

  Application tables are data tables that are maintained with transactions of SAP applications. They are generally delivered to you empty and are filled as you set up and use the system.

  Example: Master record tables.

Sample table application classes include: FC, FI Customizing tables; VS, SD system tables.

Maintaining and Transporting Table Authorization Classes

You can edit the list of permissible application classes in table TBRG. You can change the default assignments of tables to classes in table TDDAT. You can edit both of these tables using the Data Browser of the ABAP Workbench, and transport their entries (choose *Overview → Data Browser*).

As of Release 2.1A, there is view support for maintaining table TBRG.

To transport TDDAT entries, you must still manually add **R3TR TABU TDDAT/<generic entry specification>** to your transport requests. Transport support for TDDAT entries will be offered in an upcoming release.

Field Selection Editor Authorizations

The system uses the authorization object *Central Field Selection* (S_FIELDSEL) to test user access to the field attributes editor (Transaction SFAW or SFAC). With this editor, you can dynamically change such attributes of fields according to rules. For example, you can mask fields that do not apply under certain conditions.

The system tests user authorization to start the transaction and to conduct certain operations within the transaction.

Online Documentation Authorizations

The system restricts maintenance access to online documentation with the authorization object *Authorization for Maintaining Documentation with SE61*.

All types of SAP documentation, such as report, data element (field) and hypertext documentation, are protected with this authorization object. The authorization also restricts access to "final version" mode for writing documentation.

Exception: Authors or creators of system objects such as ABAP programs or ABAP Dictionary objects can create their own technical documentation for these objects without an authorization. This documentation can only be maintained in draft or "raw" mode.

Correction and Transport Authorizations

The system uses the *Correction and TransportOrganizer* object to test authorization to create or modify transport requests and tasks (corrections) and to use the correction and transport management functions (Transactions SE01 and SE09).

Developers must be authorized to create and modify tasks. Otherwise, they cannot create or modify programs and associated objects. Authorization to create transport requests and to execute transport requests should be restricted to leaders of development projects.

System Administration Authorizations

The system uses the *System Administration* authorization object to test access to many of the SAP system administration utilities.

- System trace: *Tools* → *Administration, Monitor* → *Traces* → *System trace*.

  Users may call up the trace function but cannot execute any operations without authorizations.

- Transaction locking: *Tools* → *Administration, Administration* → *Tcode administration*.

- System monitoring functions: *Tools* → *Administration, Monitor* → *System monitoring*.

  Authorizations are required to execute any operations other than display. Exception: Users can execute operations on their own programs in the *Process overview*.

  Additional restriction: In the user display, users who do not have *System Administration* authorizations can display detailed reports only on their own sessions.

- Spool system and the Temporary Sequential Object database (TemSe database). For more information, see Spool System and TemSe Database Authorizations [Page 66].

- Client copy: Permission to create a client in table T000.

- Memory management: Access to report RSMEMORY. You can use this report to display and set the limits for the SAP extended memory and local private memory that may be allocated to a work process.

- X.25 connection. Allow SAP to establish a connection to your system for purposes of Early Watch analysis or remote problem support and problem analysis.

Authorizations for Creating and Copying Clients

Normally, you use the superuser (SAP* or equivalent) to create or copy a client. The superuser has all of the authorizations necessary for these operations.

Should you want to use another user, the user must have authorizations for three objects:

- *System Authorizations* (S_ADMI_FCD): Define a new client in table T000 with the SAP Customizing system. Defining a client is the necessary first step in copying a client.
- *Maintenance of Client-Independent Tables* (S_TABU_CLI): Authorization to copy table contents from the source client to the target client.
- *Table Maintenance (Using Standard Tools)* (S_TABU_DIS): Authorization to maintain table CCCFLOW, the log table for the client-copy report.

If you want to copy user master records from the source client to the target client, you must also have a global authorization for this object:

- *User Master Maintenance: User Groups* (S_USER_GRP)

You must copy user master records and authorizations to the target client if you want to execute the copy with a user other than the superuser. The target client must contain a user master record and the required authorization for the user with which you perform the client copy.

Authorizations for the Computing Center Management System

The system uses the following objects to control access to the Computer Center Management System of the R/3 System (*Tools* → *CCMS*):

- *The CCMS: System Administration* (S_RZL_ADM) authorization object to control access to the Computing Center Management System
- *Tools Performance Monitor* (S_TOOLS_EX): Use the RDBMS-Specifics function in the CCMS and the performance monitor.
- *Authorization to Execute Logical Operating System Commands* (S_LOG_COM): Use the CCMS planning calendar for database administration.

To access the backup scheduling functions in the Computing Center Management System, you must also have complete (*) access to both fields in the *Background Processing: Operations on Batch Jobs* authorization object.

You can find more details about background processing in the Computing Center Management System documentation. To access this choose *Help* → *Extended help* from the CCMS initial screen.

You can find additional information in the online description of *CCMS*: *System Administration* (S_RZL_ADMIN), *Tools Performance Monitor* (S_TOOLS_EX) and *Authorizations to Execute Logical Database Commands* (S_LOG_COM).

Performance Monitor Authorizations

The system uses authorization object *Tools Performance Monitor* (S_TOOLS_EX) to test access to the performance monitor.

Unauthorized users can use some functions of the performance monitor. User and terminal names, however, are blanked out. An authorization is required to use sensitive functions, such as administrative functions.

Background Processing Authorizations

The system uses three authorization objects to test access to background processing services and administration.

You can find more details about background processing in the Computing Center Management System documentation. To access this choose *Help* → *Extended help* from the CCMS initial screen.

Background processing tasks and the authorization object used to test access are as follows:

- Authorize a user to schedule ABAP programs for background execution.

  Authorization object: *ABAP: Program Run Checks* (S_PROGRAM)

- Specify the "authorization users" that a user can select for a background processing job. The background processing system uses the authorization user to test system authorizations when a job is run.

  Authorization object: *Background Processing:* `NBackground`*Background User Name* (S_BTCH_NAM).

- Perform additional end-user actions in the job monitor (delete your own jobs, for example).

  Authorization object: *Background Processing: Operations on Background Jobs* (S_BTCH_JOB)

- Give full authorizations for administering the background processing system.

  Authorization object: *Background Processing: Background Administrator* (S_BTCH_ADM)

- Use the background debugging transaction (Transaction SM61) for technical analysis of the background processing system.

  Authorization object: *System Authorizations* (S_ADMI_FCD, field value PADM)

- Create and maintain background processing events for starting jobs (Transaction SM62).

  Authorization object: *Background Processing: Background Administrator* (S_BTCH_ADM, required for both user and system events).

Background Processing: Administration

A user with background processing administrator privileges has the following special capabilities:

- Access to background jobs in all of the clients of an R/3 System. In the background processing queue display, the system lists all background jobs system-wide for the user.

  A user without the authorization object *Background Processing: Background Administrator* can only work with background jobs in the client in which he or she is logged on.

- Execute any operation on any background processing job.

Batch Input Authorizations

The system uses authorization object *Batch Input Authorizations* (S_BDC_MONI) to test access to the batch input system.

Suggested profiles for users of batch input services: Activities ABTC, AONL, DELE, and ANAL; generic name specification.

Queue Management Authorizations

The system uses authorization object *Queue Management Authorizations* to test user access to the queue management tool.

This tool, which you can access by selecting *System* → *Services* → *Queue*, lets you display and manage the queues which the R/3 System uses to send and receive data from outside sources. Queues are used, for example, by the batch input facility and by applications that send data through the CPI-C gateway. To call the tool, choose *System* → *Services* → *Queue.*

Queue management is only for use in trouble-shooting or problem analysis. Queues are generally managed through the management functions of the components that use queues. You can manage batch input queues, for example, with the batch input function.

Spool System and TemSe Database Authorizations

The system uses three authorization objects to test access to the spool system and the TemSe (temporary sequential object) database.

- System Authorizations (S_ADMI_FCD): Administrator access to the output controller, the spool system and the TemSe database, user access to spool requests other than the user's own.
- Spool: Actions (S_SPO_ACT): Authorization check for operations on those spool requests that are protected with an authorization string.

  If the authorizations field is blank, any user with the required *System Administration* authorization can execute any operation on the spool request.

  If a user or the generating program enters a string, such as department name in the field, then the *Spool: Actions* check applies. Only users who have the string in their *Spool: Actions* authorization can access the spool request. They can also only execute the actions defined in this authorization.

  Example: Value **FIPAYROLL*** in a *Spool: Actions* authorization allows access to all spool requests with the string FIPAYROLL in the authorization field.

  By convention, authorization strings begin with the two-letter code of an SAP component. You can choose the rest of the string. In the example, "FI" is the code for the R/3 Finance application, payroll is a freely-selected extension.
- Spool: Device Authorizations (S_SPO_DEV): Authorization to use a printer or other output device defined by name.

An administrator requires authorization for all three authorization objects.

End users require authorizations only for *Spool: Device Authorizations* for the printers that they are to use. Optionally, you can give end users the *System Authorizations* authorization to access spool requests other than their own in the output controller. Furthermore, with *Spool: Actions*, you can authorize them to access spool requests that are protected with an authorization string.

SAPscript Text Processing Authorizations

The system tests access to SAP*script* text processing with the following authorization objects:

- *Standard Text*: Create or edit texts.
- *Style*: Create or modify styles.
- *Form*: Create or modify forms.

To maintain SAP*script* fonts, a user must also have the FONT authorization for the *System Authorizations* (S_ADMI_FCD) object.

For more information, see the authorization object documentation for the SAP*script* objects in the R/3 System.

Holiday and Factory Calendar Authorizations

The system uses authorization object *Public Holiday and Factory Calendar Maintenance* (S_CALENDAR) to test access to the functions for displaying and maintaining holiday definitions, holiday calendars, and factory calendars.

Number Range Authorizations

The system uses the *Number Range Maintenance* (S_NUMBER) authorization object to test access to the functions for managing number ranges. You can authorize users to maintain number ranges by specifying the number range object.

You can display the number range objects defined in the Customizing system or in table TNRO.

Change Document Authorizations

With the *Change Documents* authorization object, you can authorize users to access change documents.

Reducing the Scope of Authorization Checks

When R/3 transactions are executed, a large number of Authorization Objects [Ext.] are often checked, since the transaction calls other work areas in the background. In order for these checks to be executed successfully, the user in question must have the appropriate authorizations. This results in some users having more 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 [Page 79] 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.

Preparatory Steps [Page 72]

Suppressing Authorization Checks Globally for an Authorization Object [Page 73]

Reducing Authorization Checks in Transactions [Page 75]

Editing Templates for General Authorizations [Page 77]

Comparing Check Indicators and Field Values After a Release Upgrade [Page 78]

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

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

Preparatory Steps

The first thing you need to do is to activate the Profile Generator and permit specified authorization checks to be deactivated.

You can maintain the following system profile parameter by choosing *Tools* → *CCMS*, *Configuration* → *Profile maintenance* or by using Transaction RZ10:
`auth/no_check_in_some_cases = Y`.

This parameter 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.
- This activates the authorization Profile Generator. The system displays *Authorizations* on the initial screen for Transaction PFCG (*Edit activity group*).

Execute the following steps in the SAP Reference Implementation Guide (IMG):

1. **Copy SAP Default Settings for Check Indicators and Authorization Field Values**

   Using Transaction SU25, *Copy initial defaults into customer tables*, 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.

   Entries with transaction codes Y* or Z* (customer name ranges) are never deleted.

   To import an upgrade, choose *Adjust with new SAP defaults after upgrade*.

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

2. **Generate the company menu**

   Execute all steps of Transaction SSM1 to generate the company menu. This selects from the SAP menu those transactions that are implemented by the company.

   On the basis of this you can then later specify the functions and transactions for an activity group, create an authorization profile for this and assign a user.

3. **Schedule Background Job for Time Dependency (if Necessary)**

   You can maintain time-dependent activity groups. 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.

You can find further details in Comparing Profiles in the User Master Record with Activity Groups [Page 20].

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

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

Suppressing Authorization Checks Globally for an Authorization Object

You can also suppress authorization checks for an authorization object globally in all transactions where the object occurs. You should have a thorough knowledge of this application and its connections before you start.

You can also expressly exclude individual transactions from it.

On the initial screen of Transaction SU24, choose *Global changes for an authorization object*.

The system displays a list of all transactions in which the authorization object occurs. By choosing *Execute* next to the transaction code, you can call the transaction itself to check its function.

The Check Indicator [Ext.] of the authorization object is displayed for each transaction.

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

  Leave the corresponding authorizations or organizational levels open. Do not set the check indicator in Transaction SU24 to *No check*.

You can change the check indicator either for selected transactions, or globally for all transactions:

1. Select the transactions whose object check indicator you want to change.

   You can select all transactions at once and then deselect individual transactions as necessary. The system only changes the check indicators for the transactions you have selected.

2. Change the check indicator for the selected transactions in the first line that contains the name of the authorization object.

   The system only changes the check indicators for the transactions you have selected.

   You can also change the check indicator for individual transactions by changing it in the appropriate lines. As soon as at least one entry is set to CM (check / maintain), the system displays *Change field values*. By choosing this you can maintain the field values for all transaction whose check indicator has been set to CM. You can also restore the selected transactions to their original delivery status as set by SAP. You do this by choosing *Copy SAP defaults*. This restores the check indicators and field values to the default values delivered by SAP.

   When you compare the current settings with the SAP defaults, the system displays any changes in color.

   If you want, you can also display any transactions that have changed in color. To do this, choose *Display changes*.

   Transactions whose check indicator cannot be changed because of a local lock (ENQUEUE) or a lock in the correction and transport system (for R3TR SUSK

<Tcode>, are also displayed in color. There is also a short error message in the *Description* field.

You cannot set the check indicator of a parameter transaction to N.

The authorization check is only disabled if you set the check indicator to **N** (no check).

3. 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).

Reducing Authorization Checks in Transactions

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

Proceed as follows:

1. From the initial screen of Transaction SU24, choose M*aintain check indicators for transaction codes*.
2. Enter either a single transaction code (for example Transaction 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 *Tcod*.
3. Select the required transaction and then choose the appropriate pushbutton.

   The system displays a list of the authorization objects involved with their Check Indicators [Ext.].

   Using the pushbuttons, you can display field values for individual objects and the SAP default values for check indicators. Values which you have changed from the SAP defaults are displayed in color.

   You can 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 configured 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 maintain the check indicators.

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

If you want to set the check indicator of 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 on the transaction code, the system branches directly to the 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 as defaults in the Profile Generator. If the authorization object is also set to *CM* in XYZP, the field values maintained for XYZP will be proposed as defaults in the Profile Generator, and the entries for XYZE will be overridden.

You can only maintain and or overwrite the field values of the target transaction for parameter transactions in Transaction SU24.

Editing Templates for General Authorizations

It does not makes 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 activity groups (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. To do this you require the *User Master Maintenance: User groups* authorization (S_USR_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 carry out activity group comparisons.

If you want to transport your template, you need to specify an appropriate development class when you create it (not $TMP, local objects). You can find details on this in the **BC - Workbench Organizer** documentation in Maintaining Development Classes [Ext.].

Suppose you want to create a Basis user in your test system with authorization to do ”almost everything”. Typically, users with this level of authorization may not create user master records or change authorization profiles.

Proceed as follows:

- Create an activity group by choosing *User maintenance* → *Activity groups*
- Do not select any transactions. Instead go to the authorizations directly.
- In the dialog box, choose the SAP_ALL template.
  All authorizations for all objects are generated with the default value *.
- 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 (see Naming Convention for Pre-Defined Profiles [Page 111]).
- Activate the profile (see Activating Profiles [Page 110]).

If you choose *User Maintenance* → *Users,* you can assign the activity group you have just created to the user. For further information, see Assigning Task Profiles [Page 13].

Comparing Check Indicators and Field Values at Release Upgrade

After a Release upgrade you can compare the default check indicators and the field values of the previous and new Releases.

Use Transaction SU26 to do this.

If SAP's default settings change, the previous and new settings are displayed as a list.

Either way, you can decide whether you want to use the new settings or retain the previous ones.

If you adopt the new settings, you should use the Profile Generator to regenerate the authorization profiles.

If you have used Transaction SU24 to make changes to the previous settings, you can compare the changed settings with the new SAP settings.

Otherwise you can use Transaction SU26 to create a list of activity groups to be regenerated, as well as a list of new transactions in the company menu.

Generating Authorization Profiles Automatically With the Profile Generator

You can use the SAP Profile Generator to generate authorization profiles automatically.

To generate an Authorization Profile [Ext.] automatically, you first need to create an activity group.

Once you have an activity group, you can generate authorizations automatically. The fields of these authorizations are predominantly supplied with SAP default values. You can then review and change these values, as well as filling in any empty fields. Finally, you can generate an authorization profile automatically using the Profile Generator.

Authorization profiles can be assigned to individual users.

Further details on this are contained in the following sections:

Creating an Activity Group [Page 80]

Creating and Altering Authorizations [Page 81]

Generating Authorizations [Page 86]

Flagging an Authorization for Later Generation [Page 87]

Regenerating Authorization Profiles Following Changes [Page 88]

Displaying the Authorization Profile Overview [Page 91]

Checking Activity Groups for Existing Authorization Profiles [Page 92]

For details of how to assign profiles to users, see Assigning Authorization Profiles [Page 14].

The Infosystem provides you with additional information on profile lists according to complex search criteria. See Using the Infosystem [Page 30].

Creating an Activity Group

An activity group is a collection of related activities such as tasks, reports and transactions.

To create an activity group, choose *Tools* → *Administration*, *User Maintenance* → *Activity groups*, or Transaction PFCG.

For the following steps, it is assumed that you do not want to define any responsibilities. Answer the query with *No.*

In the activity group maintenance, proceed as follows:

1. Under *Activities, choose Menu.*

   The system displays the *Change menu* screen. This screen displays the main menu entries in the R/3 System as a tree structure.

   You can change the way in which the tree structure is displayed by changing the display settings.

2. To choose a menu area, double click on the appropriate main entry or select the appropriate checkbox.

   Selected areas are highlighted in color and assigned a green stoplight icon.

3. To deselect a menu area, double click on the appropriate main entry.

4. When you have finished making your selection, save it.

   The system saves your selection.

5. Exit the menu tree window and return to the activity group maintenance screen.

Displaying and Editing Predefined Authorizations

Suppose you have created an activity group based on a selection of menu functions.

You can generate authorizations for this activity group automatically, whose fields are predefined to a great extent by SAP.

You can then add missing values afterwards, change predefined values and also add additional authorizations from SAP templates or profiles.

Generating Authorization Profiles

You generate authorizations by choosing *Authorizations* on the activity group maintenance screen.

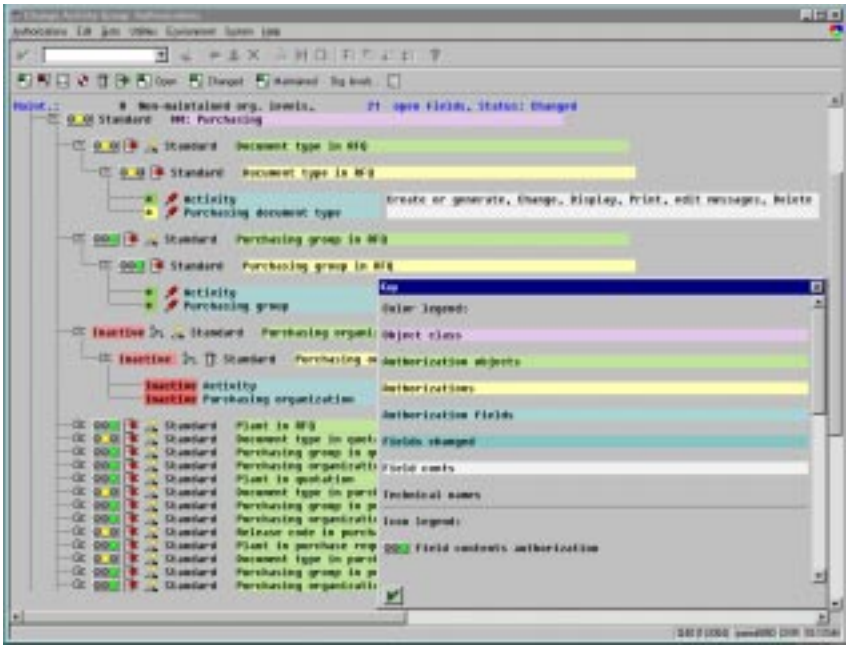
1. You can maintain missing values for organizational levels by choosing *Org. levels*.

   Organization levels are plants, company codes and business areas, for example. For each field that displays an organization level, you determine the global values for these activity groups.

   Save these entries.

2. The system displays a browser view.

   The following example of a browser view contains the various levels and their processing status.



   The key explains the various hierarchy levels and the symbols used (*Utilities* → *Key*).

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

Choose *Org. levels* to maintain the organization levels. Organization levels are plants, company codes and business areas, for example.

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

The highest levels of the hierarchy represent the authorization object classes. Underneath are the associated authorization objects, authorizations and authorization fields. Their field contents are largely predefined by the system.

If you click on the plus sign next to a hierarchy level, the subordinate levels are displayed and the plus sign changes to a minus sign. If you then click on the minus sign, the browser view is compressed.

You can edit the display elements using icons in the hierarchy level and icons in the toolbar. The stoplights display the maintenance status of authorizations.

The Status Text for Authorizations [Ext.] displays their maintenance status.

You can choose any of the following display functions by choosing the *Utilities* menu:

- Display keys
- Show or hide technical names of authorizations
- Reorganize technical names (see below for explanation)
- Redraw (update) the browser view
- Display transactions assigned to an authorization object
- Change settings:
  - Show or hide icons in the browser view
  - Show or hide technical names
  - Activate / deactivate confirmation prompts

Editing Authorizations

You can edit the predefined authorization values from the browser view. You can edit the display elements using icons in the hierarchy level and icons in the toolbar.

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

You should also check the values of the authorization fields that are marked with a green stoplight.

You should maintain the organizational levels before editing field values.

1. Maintaining Organizational Levels

Missing organizational levels are indicated by a red stoplight. Each authorization field that represents an organizational level is filled with a maintained organizational level. Organization levels are plants, company codes and business areas, for example.

You can maintain missing values for organizational levels by choosing *Org. levels*.

Determine the global value for each field that displays an organization level. If, for example, the organizational level *PLANT* appears in several authorizations, you only need to maintain the value for the plant once on the organizational levels screen.

You can display a list of all existing organizational levels using Transaction SUPO.

2. Editing Authorizations and Organizational Levels

Authorization objects and authorizations have associated texts. As a rule, the authorization text is the same as the object text. It is possible that changes to texts can be lost if you delete, recreate or compare them.

If you double click on an authorization object or an authorization field, the system displays a help text.

If you double-click on the contents of an authorization field, you can change the authorization text (*Edit* → *Authorization text*).

Maintaining Authorization Field Values

You maintain authorization field values by double-clicking on the contents of an authorization field, by clicking on an empty field, or by choosing *Maintain*.

Maintain the values in the input window.

You can assign full authorization (*) as follows:

– By choosing the relevant pushbutton in the dialog box

– By selecting the asterisk next to an authorization field name (this also applies to fields where values have already been entered)

Check the browser view for errors in the authorization assignment, and correct these. You should enter a value in the Authorization Groups [Page 90] field that is appropriate to the context, for example. If you are unsure as to the correct value, assign full authorization (*) for the fields where no value has been entered. You can change this value later.

Adding Authorizations

You can add the following authorizations by choosing *Edit* → *Add authorization.* This gives you the option to:

– add a single authorization (also by choosing *Insert*)

– add full authorization (add all authorizations to an authorization object)

– add authorizations from a profile

Copy Authorizations for SAP Templates [Page 85]

Authorizations from composite profiles cannot be added.

Deactivating Authorization Objects

To deactivate an authorization object, choose: 
Deactivated authorizations are ignored when profiles are generated.

Deactivating and Deleting Authorizations

To deactivate an authorization object, choose: 
Deactivated authorizations are ignored when profiles are generated.

To delete an authorization object, choose: 

This deletes the authorization and it is no longer displayed. To enable / disable the security prompt, choose *Utilities* → *Confirmation prompt on / off*.

You can reactivate the inactive authorization by double-clicking on *Inactive*.

Summarizing Authorization Field Contents

You can summarize any identical field contents in the authorization fields of an authorization object by choosing *Utilities* → *Summarize auths.*

Reorganizing Technical Names of Authorizations

The technical names of authorizations within each object are made up of the name of the activity profile plus two final digits in the number range 00...99: T_<Activity_group>**nn**, example: T_5002995**604**.

You can display the technical names by choosing *Utilities* → *Technical names on*.

To avoid problems with number assignment, from time to time you should reorganize the numbers **nn**.

Choose *Utilities* → *Reorganize*.

This starts the number assignment again from 00.

Whenever you generate a new authorization profile, this reorganization is automatically taken into account.

Copying Authorizations From SAP Templates

You will notice that the generated profile does not assign any general rights to the user, such as those required for printing. These authorizations are so general that it is not worth including them in each individual transaction.

Instead, you can do either of the following:

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

   Generate an authorization profile and assign it to the user.

2. Use a template to import the required objects into the activity group and then maintain the missing field contents. This is best, for example, when each user to whom the activity group is assigned may only use certain printers.

   From the Change Activity Group: Authorizations screen, choose *Edit* → *Insert* → *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 the *Edit templates* option 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 execute a comparison.

   In order to edit templates in Transaction SU24 you need the User Master Maintenance and User Group (S_USER_GRP) authorizations, with value * in the CLASS and ACTVT fields.

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

   Regenerate the authorization profile.

Generating Authorization Profiles

When you have maintained all fields and organizational levels, you can generate the authorizations for the activity group (by choosing *Authorizations* → *Generate,* or by choosing *Generate*).

An authorization is generated for each authorization level in the browser view, and an authorization profile for the whole activity group as represented in the browser view.

Before generating an authorization profile, the system checks that you are authorized to execute this action (object *Maintain User Masters: Authorization Profile*, S_USER_PRO).

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

Activate the profile (see Activating Profiles [Page 110]).

Whenever you assign the activity group to a user, you can also assign the generated authorization profile to that user (see Assigning Authorization Profiles [Page 14]).

Flagging an Authorization Profile for Later Generation

You do not have to generate your authorization profile immediately. You can instead create an authorization group with the intention of generating the profile at a later date.

To do this, choose the corresponding option in the *Exit authorization maintenance* dialog box.

You can see which activity groups already have associated authorization profiles by using Transaction SUPC.

Regenerating the Authorization Profile Following the Changes (Optional)

When you change an activity group, you must regenerate its authorization profile using Transaction PFCG (choose *User maintenance* → *Activity groups*). Following changes to the activity group, the *Authorizations* pushbutton is marked in red, with the advice *Comparison necessary* underneath.

If you choose *Authorizations*, you must choose one of the following three options:

- *Delete and recreate profile and authorizations*

  All authorizations are recreated. Values that 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 with its old values. It is not worth doing this if the activity group has changed.

- *Read old status and merge with new data*

  The Profile Generator compares the old and the current data from the activity group. This is the best choice if the activity group has changed. Old 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 within an authorization object have changed, you always need to execute the comparison manually. You must decide whether to keep the old data or to use the current data. Delete or maintain the authorizations you no longer require.

  – Maintained authorizations are, as far as possible, filled automatically with the values you have maintained.

  The activity group transactions require the following authorizations: *Add, Change, Display* Authorization Group [Page 90] (you maintain this yourself).

  This is the old, maintained status. Change the activity group so that the following activities occur: *Change*, *Display* and *Delete*. The value 0001 is then copied for the authorization group for the *Change* and *Display* activities. These were already maintained. *Insert* is no longer displayed on the screen. For the *Delete* activity you need to maintain the authorization group once again, 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 transaction from the activity group, but have the attribute *Old*.

When you choose one of the three options, the system displays the hierarchy.

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

Authorization Group

Field of the authorization objects S_PROGRAM and S_DEVELOP

The field *Authorization group* contains the name of the program groups for which the following operations are permissible as user actions.

- Execute programs
- Schedule programs for background programming
- Maintain programs
- Maintain variants

You can specify the name of a program group when creating a program.

Displaying the Authorization Profile Overview

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

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

Checking Activity Groups for Existing Authorization Profiles

You can see which activity groups already have associated authorization profiles by using Transaction SUPC.

You can limit the choice of activity groups.

You can also generate missing authorization profiles for activity groups as a background task.

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)
- PD: Personnel Planning and Development (P_PLAN_ALL)

The Profile Generator: An Example

Scenario

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. There is a separate employee responsible for each plant. He or she 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 need a basic knowledge of the R/3 authorization concept, authorization objects, authorizations and authorization profiles.

Procedure

Preparation

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

Proceed as follows:

1. Set the following system parameter: `auth/no_check_in_some_cases = Y`.
   Note that value `Y` is capitalized.
2. Restart the system.
3. Use report RSPARAM to check that the setting has been successfully made.

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 72].

Generate the company menu

You should generate the company menu as well as the SAP menu after each upgrade and after every change you make to the area menu.

First of all, reset the menus you have already generated.

1. Start the IMG Transaction SSM1 to generate the SAP menu and the company menu.

   Select the language in which the menus are to be generated.

   Reset the menus that were already generated by choosing *Generation* → *Reset*.

   Execute the steps sequentially to generate the menus.

   The first step generates the SAP menu for the Session Manager. This is then automatically active.

The second step generates the company menu.

- If you want to use a menu other than S000 as the initial menu, enter this in the appropriate field.
- You should deselect the *Without Enterprise IMG filtering* option. This ensures that only the transactions in your chosen components are copied into the company menu. The application components active in the company are specified when generating the Enterprise IMG (Implementation Guide).
- You can make further changes to the company menu after it has been generated if you need to.

2. Activate your company menu.
3. If you want to abandon your company menu and regenerate it, choose *Generation* → *Reset*.

It can take several minutes to generate the menus, especially if you have selected more than one language.

Creating and Maintaining an Authorization Profile for a User

You can create a user-specific menu with appropriate authorizations based on the company menu you have generated.

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.

Execute the following steps to create an authorization profile for a user:

1. Create an activity group and generate an authorization profile
2. Assign the activity group to a user
3. Change the activity group (optional)
4. Change the check indicator defaults (optional)
5. Copy the general authorizations from SAP defaults (optional)
6. Regenerate the authorization profile following the changes (optional)
7. Check the authorization profile

These steps are described in detail below.

1. Create an activity group and generate an authorization profile

The functions (transactions) for a user are put together in an activity group.

1. On the *User maintenance: Initial screen* (Transaction SU01), choose *Environment* → *Maintain act. group*.

2. Create an activity group. To do this, choose *Create*. On the following screen, enter MATST_0001 as the identification code and an appropriate description.
3. Save these entries. If you are using automatic transport recording, enter a suitable request.
4. Choose *Menu.* The company menu that you generated previously is loaded and displayed as a hierarchical structure.
5. Expand the *Logistics*, *Materials management* and *Material master* levels.
6. Flag the checkbox next to *Material*. Some of the stoplights will change to green. If you now expand the node further, you will see the transactions you have just selected. Amongst others you will see *Create* / *Display* / *Change material*.
7. Save your selection.
8. Choose *Authorization profile*. The system now prepares the appropriate authorization data using the transactions you have selected.
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 company structure. These fields occur in many authorizations. You only need to maintain them once, and this occurs in the *Maintain organizational levels* dialog box.

   Following 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. On the following screen, the authorization data is displayed as a hierarchy. At the highest level is the activity group. Underneath are the object classes of the authorization objects relevant to this activity group.

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

    For example, at the lowest level you can see the field values of the authorizations. Most of the fields already contain entries. These are either the default values set by SAP for functions, or the values that you have set for the organizational levels.

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

    Red: You have not maintained the organizational levels.

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

11. Expand the levels that have a red stoplight. One of these is an authorization for the *Material master: Warehouse number* object. 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 later come to generate authorization profiles, this authorization is not copied into the profile.

    There are now no more red stoplights, since no active authorizations remain with unmaintained organizational levels.
13. There are, however, still a lot of yellow stoplights. 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 on the text of an authorization object

    By double-clicking on 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 stoplight. Once you have confirmed the operation, full authorization (*) is assigned for all empty fields in the subordinate levels of the hierarchy. Note how the stoplight reacts.

    Help → *Extended help* offers you detailed information about the individual icons.
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 activity groups and authorization profiles to a user

You assign an activity group to a user by choosing *Assign activity group,* and enter a new object in the form of activity group MATST_0001.

The user is also assigned the authorization profile.

For further information, see Assigning Task Profiles [Page 13].

Log on again as this user. 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 activity group (optional)

You change an activity group as follows:

1. In the activity group maintenance screen, choose *Menu*.
2. Activate the *Stock overview*, *Period closing* and *Allow posting to previous period* menu functions.

3. Save the settings and return to the authorization maintenance.

   In the following dialog box you need to specify which action you want to execute. In this case, you need to compare the data as you have enhanced the functions.

4. Two new levels have now appeared in the dialog box containing the organizational levels: *Purchasing group* and *Purchasing organization*. Maintain these (enter * for example) and choose *Continue*.

Some new authorizations have come into 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 stoplight). 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 authorization 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 has changed.

   If, on the other hand, you maintain an organizational level by clicking on its 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 stoplights to green. You can avoid this by changing the transaction defaults.

1. To do this, call Transaction SU24.
2. Choose *Global changes to authorization objects* and enter M_MATE_LGN as the object. Choose *Execute*.
3. On the next screen, the system displays all the transactions that check this authorization object. In the first line you can assign the Check Indicators [Ext.] globally for the object. In this case it is a good idea to check this object in all transactions, but not to copy the defaults into the Profile Generator.

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

4. Go back to maintaining activity group MATST_0001 again. Go to the authorizations, and choose *Compare* in the dialog box again. 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 to copy the default value of 51 *Initialize* for object M_MATE_PER *Material master: Allow posting to previous period* into the activity group, change the default 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 activity groups are affected, whether these are groups which already exist (and must as such then be compared) or groups which you know 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 for such widespread authorizations to be copied to each transaction with CM as their check indicator.

Instead, you can do either of the following:

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

   Generate an authorization profile and assign it to the user.

2. Use a template to import the required objects into the activity group and then maintain the missing field contents. This is the best thing to do if each user assigned to an activity group 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 should 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 require the S_USER_GRP authorization *User Master Maintenance: User Groups* to do this. 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 activity groups. Your own templates may not begin with S.

6. Regenerate the authorization profile following the changes (optional)

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 activity group: Change activities, insert authorizations manually, and deactivate authorizations.
2. Change the defaults using Transaction SU24 as described above and compare the activity groups.

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

In this example, repeat the test until you are satisfied with its results. The user may execute exactly the right actions in plant / company code 0001. Next, copy the activity group to another name (MATST_0002, for example). Change the organizational level to plant 0002 and company code 0002 and generate the authorization profile. You can then assign this activity group to the users who are to execute material master maintenance for plant 0002.

In a later Release it will be possible to assign user-specific authorization values (plant, for example) with user variables. These will allow you to assign these values directly to each user. The advantage of this is that you do not need to create several activity groups whose contents are the same but differ only in the values assigned by organizational levels or other authorization fields.

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 can see the changes you have executed by choosing *Utilities* → *Change documents* in Transaction SU24.

You should then check whether the functions in your activity group are still correct. Is the menu selection still current, for example? In either case, you should always compare your authorization data.

The Profile Generator: Helpful Hints

1. Limiting activities by time

Even if you are not using HR-Org. you can still take advantage of the option to assign activity groups 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* → *Activity groups*.

Choose *View* → *Overall view*. The system displays details of the assignment period.

Change the processing period and save your data.

So that a time delimited assignment of an activity group to a user master record can take effect, you should first execute a comparison.

The authorization profile is only entered or deleted in the user master record automatically if you have scheduled the comparison report `RHAUTUP1` to run periodically.

2. Managing time-dependent activity groups and assignments

Activity groups or assignments can be time-delimited. This means that the current data will become invalid on a particular day, whilst other data will become valid. Authorization profiles and their entry in user master records are however not time-dependent. You need to execute a comparison to ensure that, on a given day, the user master only contains valid authorization profiles.

How is the comparison executed?

There are two ways to execute the comparison.

1. As a background job, scheduled daily before the start of business.

   If report RHAUTUP1 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.

2. Using Transaction PFUD, *Compare User Master Data*.

   You can call this transaction to correct manually any errors that may have occurred in the background job.

So that changes in the user master record are effective, you should execute the comparison before the user logs on. The system administrator should call Transaction PFUD regularly to check that errors are not occurring in the background job.

3. Do not assign any authorizations for modules you have not yet installed

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

Leave the corresponding authorizations or organizational levels open. Do not set the Check Indicators [Ext.] in Transaction SU24 to *No check.*

4. Initial authorization assignment

Suppose you want to create a user in your test system with authorization to do 'almost anything'. Typically, users with this level of authorization may not create user master records or change authorization profiles.

The quickest way of setting up this user is as follows:

– Create an activity group.

– Do not choose any transactions, instead go directly to the authorization data (by choosing *Authorizations*).
The system displays a dialog box from which you can choose a template.

– Choose SAP_ALL *Full Authorization with all Authorization Objects*.
All authorizations for all objects are marked with '*'.

– Expand the *Basis administration* object class.
This contains the authorization objects that are generally regarded as critical.

– Deactivate all authorizations which begin with *User Master Maintenance*, as well as any others which you regard as critical. Note that authorization S_USER_GRP, *User Master Maintenance: User Groups* (S_USER_GRP) with value * in fields CLASS and ACTVT is required to execute Transaction SU24.

– Generate the profile.

– By choosing *User Maintenance* → *Users,* you can enter the activity group in the task profile, thereby assigning the activity group you have just created to the user.

For further information, see Assigning Task Profiles [Page 13].

5. Transport

Details of the transport system are contained in the following documentation:
BC - Workbench Organizer, Setting Up the Workbench Organizer and the Transport System [Ext.].

Note that following a transport, the authorization profiles in the target system are not automatically updated.

You can use Transaction SUPC to identify activity groups with missing profiles and generate the profiles themselves.

Creating and Maintaining Authorizations and 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 Generating Authorization Profiles Automatically With the Profile Generator. [Page 79]

An authorization is a permission to execute a particular action in the R/3 System. Each authorization refers to exactly one Authorization Object [Ext.] and defines the permitted value range for each authorization field of this authorization object.

By entering such authorizations in user master records in the form of authorization profiles, you enable users to use the system productively.

Administration Tasks

If you want to create and maintain authorizations in the R/3 System, you should create and activate two types of authorization components.

- These components are authorizations to allow specific system authorizations.

  You maintain authorizations by choosing *Tools* → *Administration*, *User maintenance* → *Authorization*.

- Authorization profiles, to enter authorizations in user master records.

  You maintain authorization profiles by choosing *Tools* → *Administration*, *User maintenance* → *Profiles*.

The R/3 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.

Maintaining Authorization Profiles

This topic describes how you create, edit, activate, and delete Authorization Profiles [Ext.]. To access the profile maintenance, choose *Tools → Administration, User maintenance → Profiles*.

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.

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 add new authorizations by selecting them with *Add authorization*. This function displays authorizations that have already been created according to object class and object.

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 *Tools* → *Administration*, *User maintenance* → *Profiles, Profile* → *Create* and then flag *Composite profile*.

In activity group maintenance, proceed as follows:

1. Generate a work area (profile list) by choosing *Generate work area,* or enter the name of the composite profile that 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 that is to be included in the composite profile using *Add profile*. You can list a virtually unlimited number of profiles in 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 a composite profile.

Activating 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

The R/3 System contains several predefined authorization profiles. These are named according to the convention shown in the table below.

You can display the authorization profiles predefined in the R/3 System by using the naming convention and the profile information system.

Naming Convention for Predefined Authorization Profiles, Authorization Objects, and Authorizations

Character	Explanation
1	Index letter of SAP application:
	A: Asset Management
	C: CIM
	F: Financial Accounting
	G: General Ledger
	K: Cost accounting
	L: Warehouse Management
	M: Materials Management
	P: Human Resource Management
	S: Basis System
	V: Sales and distribution
2	Underscore character
3-10	Freely-selectable descriptive string.

Example: S_A.ADMIN: all authorizations for the Basis components of the R/3 System.

Standard profiles: SAP does not guarantee that standard authorizations delivered with the R/3 System will not be changed by 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. SAP places no other restrictions on naming profiles.

For convenience, you may want to use the naming convention shown above, substituting a different character for the underscore character in the second position.

Maintaining Authorizations

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

For information on the authorizations needed to maintain authorizations, see Setting Up Authorization and Activation Administrators [Page 138].

Creating and Maintaining Authorizations [Page 113]

Entering Values [Page 114]

Activating Authorizations [Page 116]

Naming Convention for SAP Authorizations [Page 117]

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.

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 actions.

The fields for which values must be defined are displayed automatically. The system displays a description of each field so that you can easily identify its functions.

You can display the documentation or possible values for a field by positioning the cursor on the field and choosing the appropriate function.

Rules for Entering Values

- Enter single values in *From* fields only. Do not enter any value in the accompanying *To* field.
- Enter value ranges in 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 give 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 the following sequence: **'<space-key>'** (a space enclosed in single quotation marks, or **'<space-key>** or **'**, in shorter fields).
- For many fields, you can display the values that may be entered by choosing *Permissible entries*.

System-independent 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 that users belonging to a user group may execute:

Sample Authorization

Object	Fields	Values
User groups	*User Master Maintenance: User group*	S*
	Administrator actions	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 includes a set of predefined authorizations that are named according to the convention described in Naming Convention for Predefined Profiles [Page 111].

You can display the predefined authorizations by using the naming convention and the user and authorization information system.

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

Naming Your Authorizations

To avoid conflicts between authorizations that you define and those supplied by SAP, you should not use any authorization name that has an _ (underscore) character in the second position. SAP places no other restrictions on naming authorizations.

For convenience, you may want to use the naming convention shown above, substituting a different character for the underscore character in the second position.

Adding Authorization Checks to Your Own Developments

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

If you use the Profile Generator [Page 79] to generate your authorization profiles automatically, the authorization object S_TCODE is contained in the profiles.

Furthermore, you can use 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. Authorizations are also not checked for parameter transactions.

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 119]
2. Create an Authorization Object [Ext.]
3. Assign an Authorization Object to an Object Class [Page 121]
4. Program authority checks
   Use the ABAP AUTHORITY-CHECK statement. Be sure to specify alphabetic values in uppercase letters: ABC. Test values from user master records are converted to uppercase before being passed to AUTHORITY-CHECK.

   See the ABAP programming documentation for more information.

Creating Authorization Fields

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

Prerequisite: Define Structure ZAUTHCUST

Before you define a field, check that you have defined the ABAP Dictionary structure ZAUTHCUST. This structure is required for customer-specific authorization fields. If you have upgraded to Release 3.0 from an earlier release, then you should have already defined this structure in accordance with the release note *New ZAUTHCUST Table for Customer Authorization Fields* for Release 2.1.

If you have not defined ZAUTHCUST, proceed as follows:

1. Start the ABAP Dictionary. Choose *Tools* → *ABAP Workbench, Development* → *Dictionary.*
2. Define the structure by entering the object name **ZAUTHCUST**, flagging *Structures*, and choosing *Create*.

   Be sure to use the name ZAUTHCUST. Otherwise, the *Customer* function for defining fields will not work.

   You do not need to define any fields for the structure.
3. Enter a brief description of the table, such as "Customer authorization fields". Then save the structure by choosing *Save*.

   Be sure to assign the structure to one of your own development classes (class name starting with Y or Z).

   You do not need to activate the structure.

Creating Fields

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

Enter the name of the field and assign it to an ABAP Dictionary data element. Field names must be unique and must begin with the letter **Y** or **Z**, in accordance with the naming convention for customer-specific objects.

You can define a foreign key for an authorization field. To do so, position the cursor on a field and choose *Goto* → *Foreign keys.* You can also define a value range by way of the area with which a field is associated. Users can display both types of value ranges when they maintain authorizations.

So that your fields are not deleted when you install a new release, you should define your fields only with the *Customer* function in the field maintenance. The *Customer* function automatically saves your fields in the ZAUTHCUST structure.

For more information, choose F1 to display the online information available, or see the ABAP documentation for the AUTHORITY-CHECK statement.

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 Authorization Objects 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*.

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 documentation for it.

Ensure that the object definition matches the ABAP 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.

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 123].

- Authorization error analysis

  By entering Transaction **SU53** in the command field, you can analyze an authorization-denied error that has just occurred in your session.

  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: When you choose a function, the system responds with the message "No authorization for this function". If you enter Transaction **SU53** or **/nSU53** in the command field, the system displays the authorization object that was just tested and the value of the object that you have in your user master record.

  However this function is active only if you have set the system profile parameter *auth/check_value_write_on* to a value that is greater than 0. By default, the function is inactive, and the parameter value is 0. For information on setting the parameter, see the *System Profile Parameters* manual.

Tracing Authorizations with the System Trace

To start tracing authorizations, proceed as follows:

1. Choose *Tools* → *Administration, Monitor* → *Traces* → *System trace.*
2. On the system trace initial screen, choose *Trace switch* → *Switch, edit.*
3. In the trace switches screen, flag *Authorization check* and select the value *Trace: Write to disk* in the *Write options* field.

   You can restrict the trace to your own sessions by entering your name in the *General filters* field. Choose the arrow next to the field and enter your user ID in the *User* field in the dialog box.
4. Activate the trace by choosing *Trace switch* → *Editor save in* → *In active system*. You can now trace authorization checks in any of your own sessions.
5. When you have finished the analysis, stop the trace by choosing *Trace switch* → *Immediate switch* → *Stop.*
6. To display the results of the trace, choose *Trace files* → *List of traces.* Position the cursor on the file that you want to display and choose *Display file*.

   The system displays the authorization tests entries in the format <Authorization object>:<Field>=<Value tested>.

   You can display a formatted view of an authorization check by clicking on 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 files* → *Standard options* and ensure that *Trace for authorization checks* is selected.

   You can also restrict the display to trace records from your own sessions. To do this, enter your user ID in the *User* field in the options display.

Transporting User Master Records, Authorizations and Profiles

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

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

The procedures for both kinds of transport are detailed below.

Transports 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.

You can transport user master records, profiles and authorizations between clients in the R/3 System using report RSCLACOP.

- Note that any user master records, profiles and authorizations in the target system with the same name as items in the transport are overwritten.

  Accordingly, you must not use report RSCLACOP if your target client contains authorizations and user master records that you want to keep.
- RSCLACOP must be run from the target client; that is, the client into which you want to copy the user master records and authorizations.

Further details, particularly concerning the necessary authorizations, are contained in the report documentation.

Transports Between R/3 Systems

You can transport authorization components, activity groups and user master records from one R/3 System to another. You may either transport components independently, or you can transport profiles with all their associated authorizations.

For details on the transport, see BC - Workbench Organizer [Ext.].

Transporting Authorization Components

Transporting Profiles:

1. Choose *Tools* → *Administration, User maintenance* → *Profiles*. Create a profile list and then select *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 accompanying the profiles and authorizations.

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

Transporting Authorizations

To transport **authorizations**, first start the authorization maintenance function. Do this by selecting *Maintain users* → *Authorizations*. Choose an object class and then *Authorization* → *Transport*.

Transporting Authorization Objects and Authorization Object Classes

Whenever you create or change **authorization objects** or **authorization object classes**, the system displays a dialog box in which you can create a change request.

Transporting User Master Records

To transport user master records, you use the development environment object type R3TR TABU in a transport request. You can then select and transport entries from the following tables:

- USR01: User master records (runtime data)
- USR02: Logon data
- USR03: User address data
- USR04: User master record: Authorizations
- USR05: User master record: Parameter IDs
- USR06, USR14: License data
- USR08, USR09 and USR30: User menu definitions

Transporting Check Indicators and Field Values

If you want to copy the SAP defaults to your own check indicators and field values, or you want to maintain them, your changes are recorded in the correction and transport systems. By executing the corresponding transport request, you distribute your check indicators in the system. Objects in it have the following syntax:

```
R3TR SUSK <Transaction name>
```

<Transaction name> corresponds to the normal SAP transaction names. The check indicators and field values are included in the transport. Check indicators are saved in table USOBX_C, field values for the Profile Generator in table USOBT_C.

Transporting the Company Menu

Using IMG Transaction SSM1 you can generate, edit and activate your company menu.

For further information on this, see the help screens for Transaction SSM1 (*I* or *?).*

The first screen in Transaction SSM1 allows you to choose the type of transport for the company menu:

- Transport the active company menu

  You cannot edit the active company menu in the target system.

- Transport all menus

  This involves the following objects:

  – SAP menu
  – Inactive version of the company menu
  – Active version of the company menu
  – Change and generation history

  You can edit and activate the inactive company menu in the target system.

Transporting Templates

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

The correction and transport systems record changes to your own templates. Transport the request. The objects in it have the following syntax:

```
R3TR SUSV <Model Name>
```

The template name and the data maintained is transported into all languages.

Transporting Activity Groups

All activity group data is stored in the following infotypes:

1000: Name and short description for the activity group

1201: Indicator: The object is an activity group (to differentiate from Workflow tasks)

1001 Link type/ link A007, B007: Assignment of a user to an activity group

1221: Transactions selected

1250: Authorization (data) for activity group

1251: Field values for authorization data

1252: Maintained organizational levels for activity group

1253: (not used)

1254: (not used)

1016: Name of authorization profile assigned or generated

Additionally, if Workflow tasks have been maintained (no effect on authorizations):

1220: Workflow tasks (activity profile)

1001: Various entries

For further information on infotypes, see PPD - Organization Management [Ext.].

Recording for activity groups is active as a standard setting. If you want to deactivate this, you must call Transaction OOCR and set the value of entry TRSP CORR to X (IMG activity: Set switch for automatic recording of PD data, SIMGSIMG_CFMENUOHP0OOCR).

If the automatic recording is deactivated, you can enter activity group data in a transport request using *Transport* in Transaction PFCG.

Note that activity groups can only be transported (or, at least, exported) complete, with all constituent infotypes and time periods. However, a transport plan variant is also always imported automatically. Only relevant data is activated (for example, if you transport an assignment to a user that does not exist in the target system, the assignment is not activated).

Blocking Imports to the Target System

In the target system you can determine which data should not be imported:

1. In the target system, open a maintenance view for table view T77TR.
2. Make an entry for each infotype you want to block. The object type is always ‘T’. You can find out the infotype from the above table (IMG activity: Determine import lock IMG: SIMGSIMG_CFMENUOHP0OTR).

Authorization Data

To block the import of authorization data, you need to make the following entries in the target system (in each case, leave subtypes):

T,1250

T,1251

T,1252

T,1253

T,1254

Assignment of Activity Groups to Users

If you do not want to import assignments of activity groups to users, you need to make the following entries:

T,1001, A007

US, 1001, B007

Regenerating Authorization Profiles in the Target System

Generated profiles are not included in the transport.

The reason for this is that the source system does not know which, if any, import locks have been set in the target system. For example, if you set an import lock on the authorization data, this will not be activated following the import. In this case, the authorization profile should not have been imported either. As a result, you cannot include authorization profiles in the transport.

Consequently you should regenerate the profiles once the data has been imported into the target system. To do this, call Transaction SUPC in the target client or system. This transaction allows you to identify easily which profiles for activity groups are missing and to start generating them.

Organizing User and Authorization Maintenance

This section describes how you organize user and authorization maintenance in your R/3 System.

Overview: Managing Users, Authorizations and Profiles

The authorization system allows you great flexibility in organizing and authorizing the maintenance of user master records, profiles and authorizations:

- 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 142].
- As you can precisely restrict authorizations for user and authorization maintenance, the administrators do not have to be privileged users. 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.

  In maintenance, these administrators need not be high-level users in your data processing organization. You can assign user and authorization maintenance to ordinary users.

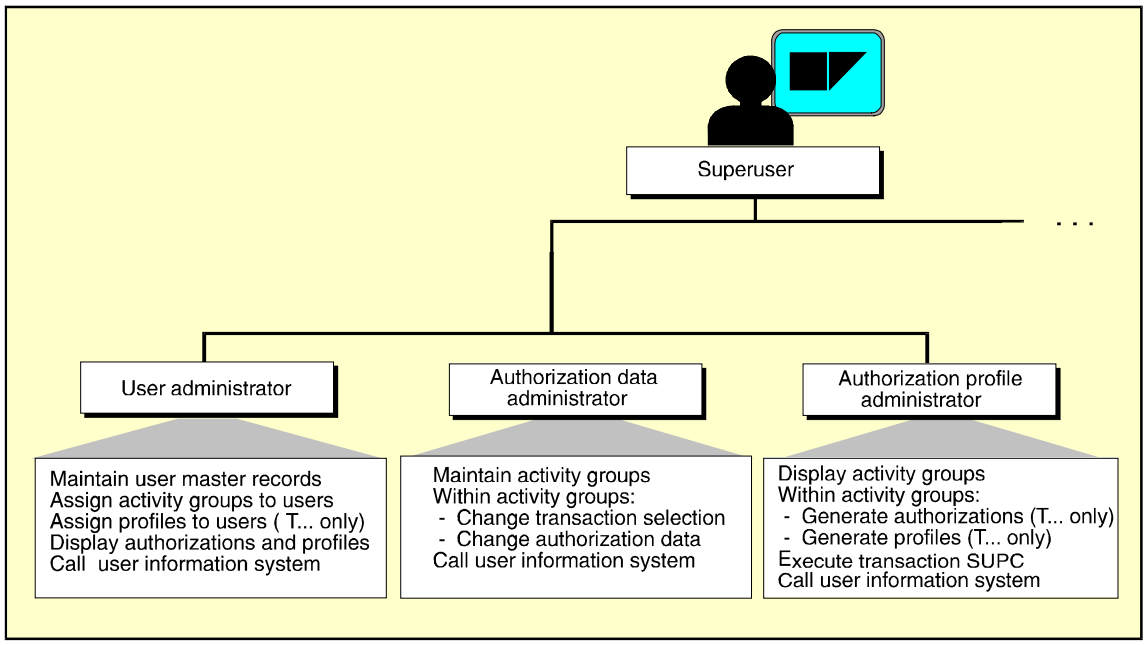
This topic explains:

- 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, profiles and authorizations.

Administration Using the Profile Generator

If you are using the Profile Generator, you can automatically generate authorization profiles based on selectable R/3 transactions. You can generate this type of profile based on templates for administrators.

For reasons of system security, you should divide up system administration tasks between different administrators as displayed 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 entity.

Within an area, administration tasks are divided among three administrators.

- User administrator

  User administrators have the following tasks and authorizations:

  – Creating and changing users
  – Assigning profiles beginning with T to users
  – Displaying authorizations and profiles
  – Using the user information system (Transaction SUIM)

  The following tasks are *not* permitted:

  - Displaying or changing activity group data
  - Changing or generating profiles

- Authorization data administrator

Authorization data administrators have the following tasks and authorizations:

- Creating and changing activity groups
- Changing the transaction selection and authorization data in activity groups
- Using the user information system (Transaction SUIM)

The following tasks are *not* permitted:

Changing users

Generating profiles

- Authorization profile administrator

  Authorization profile managers have the following tasks and authorizations:

  - Displaying activity groups and their data
  - Generating authorizations and authorization profiles based on existing activity groups beginning with T
  - Executing Transaction SUPC
  - Using the user information system (Transaction SUIM)

The following tasks are *not* permitted:

Changing users

Changing activity group data

Generating authorization profiles containing authorization objects beginning with S_USER.

To assign administration tasks to the various users see Setting up Administrators [Page 132].

Setting up Administrators

You should proceed as follows:

1. Create an activity group for each administrator.
2. Do not choose any transactions, but go directly to the authorization data (choose *Authorizations*). The system displays a dialog box asking you to choose a template.
3. Choose one of the following templates:
   - for authorization profile administrators SAP_ADM_PR
   - for authorization data administrators SAP_ADM_AU
   - for user administrators SAP_ADM_US
4. Generate an authorization profile for each.

   Use a profile name which DOES NOT begin with T.
5. Assign the activity groups to the appropriate users.

You can restrict the authorization of user administrators to particular groups of users.

You can exclude further authorization objects from the profiles using the Profile Generator, for example, HR data. If you want your generated authorization profiles to begin with a letter other than T, you should inform the profile administrator.

How the Three Administrators Work Together

The **Authorization data administrator** creates an activity group, chooses transactions and maintains the authorization data. In the Profile Generator, the authorization data administrator merely saves the data since he or she is not authorized to generate the profile, and accepts the default profile name T_....

The **Authorization profile administrator** calls Transaction SUPC and sets the following parameters on the next screen: The administrator flags *All activity groups* and restricts the selection by entering the identifier of the activity group 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 activity group 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*) authorization objects.

Administration Without Using the Profile Generator

For maximum system security, you can divide up maintenance among three types of users:

- Creating and maintaining user master records

  A **user administrator** can perform tasks such as creating user master records, maintaining the list of profiles in a user master record, and setting user parameters.

  A user administrator cannot maintain or activate profiles or authorizations.

- Creating and maintaining authorization profiles and authorizations

  An **authorization administrator** can work only with the maintenance versions of profiles and authorizations. The administrator cannot activate profiles nor authorizations, that is, make them effective in the system.

- Activating authorization profiles and authorizations

  An **activation administrator** cannot change the authorizations defined in profiles and authorizations. The administrator can only activate existing maintenance versions of profiles and authorizations.

Reasons for Dividing Maintenance

Maintenance responsibilities are divided up for the following reasons:

- Increase security against misuse of authorizations and user accounts

  If a single user can execute all user and authorization maintenance activities, then the user can single-handedly define authorizations and put them into effect in the system.

  Similarly, if users can maintain and activate profiles and / or authorizations, they can make changes to a profile or authorization and put them into effect in the system. When the user activates a profile or authorization that he or she has modified, these changes take effect for all users who already have the profiles or authorizations.

- Decentralize user and authorization administration

  The system lets you further subdivide the administrative workload. You can organize user and authorization maintenance by department, cost center, or any other organizational criteria.

  Specifically:

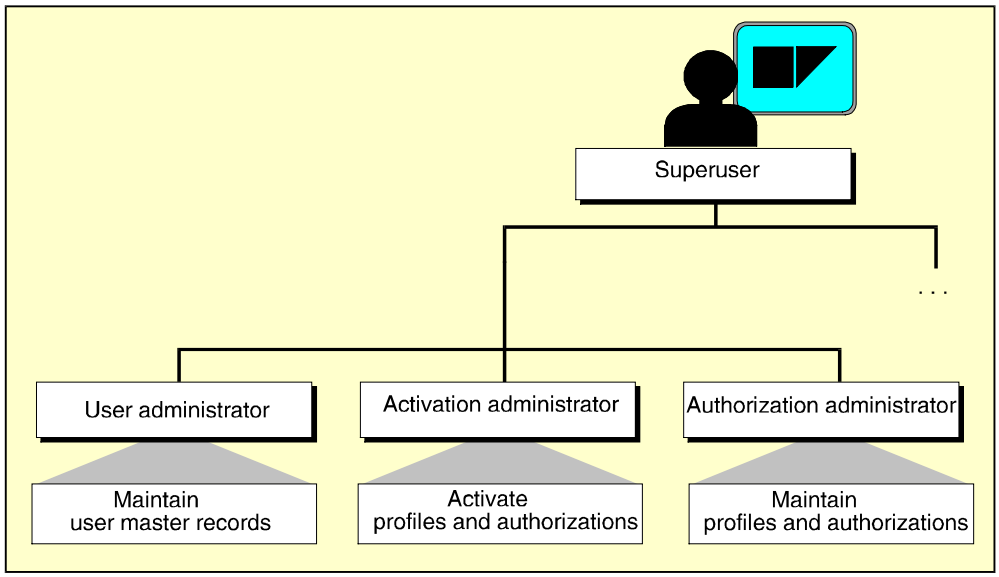
  – You can limit a user administrator to maintain users only in particular user groups.

  – You can limit the number of profiles and authorizations with which an authorization or activation administrator can work by explicitly specifying the names of the corresponding profile and authorizations.

    The users who execute these functions can therefore be ordinary users in your organization. The superuser is required only for setting up the lower-level administrators.

Organizing Maintenance: Example

The graphic below shows how the three types of administrator work together.



In the graphic, the superuser maintains user master records, profiles, and authorizations for administrators in one or more organizational areas.

An area may be a department, a cost center or any other organizational entity.

Within an area, administration responsibilities are divided among three users. One user is responsible for creating and maintaining user master records. Another is responsible for creating and maintaining profiles and authorizations. A third user activates profiles and authorizations.

The following sections describe how to assign administration tasks to the various users:

Setting Up User Administrators [Page 135]

Setting Up Authorization and Activation Administrators [Page 138]

Setting Up Authorization Administrators [Page 139]

Setting Up Activation Administrators [Page 140]

Setting Up User Administrators

You can set up a user administrator by assigning a user with a profile that contains the following authorization objects:

- *User Master Maintenance:* User Groups (S_USER_GRP)
- *User Master Maintenance:* Authorization Profile (S_USER_PRO)

For details of how to assign profiles to users, see Assigning Authorization Profiles [Page 14].

You can use the authorization objects to specify:

- The user groups that an administrator may maintain

  An administrator may edit user master records that

  - belong to the groups for which he or she is authorized.
  - have not been assigned to any group.
- Which activities a user administrator may execute.
- Which profiles an administrator can assign.

User administrator authorizations

Object	Fields	Values	Sample Profile
User Groups (S_USR_GRP)	*User group*	Name(s) of permissible user groups	**S.A_ADMIN**: All user and authorizations except for S_USER* objects and user group SUPER
	Administrator actions	**01**: Create user master records	
		02: Change user master records	
		03: Display user records	
		06: Delete user master records	
Authorization Profile (S_USR_PRO)	*Profile name*	Name(s) of permissible profiles.	
	Administrator actions	**22**: Display profiles and enter them in user master records	

If you want to separate user and authorization maintenance tasks, copy and edit profile S.A_ADMIN. The default version of the profile authorizes a user for all user and authorization maintenance tasks.

User group SUPER: Assign all user and authorization administrator user IDs to the group SUPER. If you use the predefined user maintenance authorizations, this group assignment ensures that user administrators cannot modify their own user master records or those of other administrators. Users in group SUPER can be maintained only by administrators that have the predefined profiles S_A.SYSTEM or SAP_ALL.

Users not assigned to groups: If you organize user maintenance by user group, ensure that every user master record is assigned to a group. Users that are not assigned to a group can be maintained by any user administrator.

Authorizations Reserved for the Superuser

To prevent misuse, you should reserve the following *User Groups* authorizations for the superuser:

- Authorization for users in group SUPER
- **05**: Lock and unlock users (prevent or allow logons); change passwords
- **08**: Display change documents.

Authorizations for Changes to Multiple Users

The R/3 System offers two ways to execute mass changes to user master records. These are described in Changing Several User Master Records [Page 27].

Deleting All Users: Authorization

To use *Delete all Users,* an administrator must have the following authorization for the *User Groups* object:

- * authorization (authorization for all user groups) for the *User group* field
- **06** (Delete profiles): Authorization for the *Action* field.

Adding / Deleting Profiles: Authorization

To add or delete profiles, an administrator must have the following authorizations for the *User Groups* and *Authorization Profile* objects.

For *User Groups*:

- * authorization (authorization for all user groups) for the *User group* field
- **02** (Change) Authorization for the *Action* field.

For authorization profiles:

- Authorization by name for the profile to be added or deleted in the *Profile name* field
- **22** (Display): Authorization for the *Action* field.

Using the *User Groups* Authorization Object

The table below shows the complete set of values for the *User Groups* authorization object.

Using the *User Groups* Authorization Object

Authorization object	Fields	Values
User groups	*User group*	Name(s) of the permissible user groups
	Administrator actions	**01**: Create user master records, add profiles to new or existing records, and set user defaults for the Basis System and applications
		02: Change user master records
		03: Display a user master record with the information system
		05: Lock or unlock a user (prevent or allow logons); change passwords
		06: Delete user master records
		08: Display change documents
		24: Archive change documents

Setting Up Authorization and Activation Administrators

You can set up an authorization administrator with the *Authorization Profile* (S_USER_PRO) and *Authorizations* (S_USER_AUT) authorization objects.

With these authorization objects, you can do the following:

- Limit access to profiles and authorizations by name
- Specify which maintenance activities an administrator may perform.

For maximum security, you should set up separate administrators for maintaining and activating profiles and authorizations.

Setting Up Authorization Administrators [Page 139]

Setting Up Activation Administrators [Page 140]

S_USER_ Authorizations: Do not give administrators other than the superuser authorization to create or maintain authorizations for the *Authorization Profile* (S_USER_PRO) and *Authorizations* (S_USER_AUT) authorization objects. With such authorizations, a user could define, activate, and assign unauthorized privileges.

To exclude these privileges, exclude the string "S_USER" from any authorization that you define for the Authorizations object.

Setting Up Authorization Administrators

An authorization administrator needs the authorizations shown in the table below.

Authorization administrator authorizations

Object	Fields	Values	Sample Profile
Authorization Profile [Ext.]	*Profile name*	Name(s) of permissible profiles	**S_A.ADMIN**: All user and authorizations except for S_USER objects and SUPER user group
	Administrator actions	**01**: Create profiles	
		02: Change profiles	
		03: Display profiles	
		06: Delete profiles	
		08: Display change documents for profiles	
Authorizations [Ext.]	*Object name*	Name(s) of permissible objects	
	Authorization name	Name(s) of permissible authorizations	
	Administrator actions	**01**: Create authorizations	
		02: Change authorizations	
		03: Display authorizations	
		06: Delete authorizations	
		08: Display change documents for authorizations	

An authorization administrator can execute all maintenance operations (apart from activation) on maintenance versions of profiles and authorizations. He or she cannot delete active versions of profiles and authorizations.

If you want to separate user and authorization maintenance tasks, copy and edit profile S.A_ADMIN. The default version of the profile authorizes a user to execute all user and authorization maintenance tasks.

Setting up Activation Administrators

The following example shows how to set up an activation administrator.

Sample profile values for an activation administrator

Object	Fields	Values	Sample Profile
Authorization Profile [Ext.]	*Profile name*	Name(s) of permissible profiles	**S_A.ADMIN**: All authorizations except for S_USER objects and SUPER user group
	Administrator actions	**06**: Delete profiles	
		07: Activate profiles	
Authorizations [Ext.]	*Object name*	Name(s) of permissible objects	
	Authorization name	Name(s) of permissible authorizations	
	Administrator actions	**06**: Delete authorizations	
		07: Activate authorizations	

The administrator can only activate the profiles and authorizations named in the authorization profile.

If you want to separate user and authorization maintenance tasks, copy and edit profile S.A_ADMIN. The default version of the profile authorizes a user to execute all user and authorization maintenance tasks.

Access Security: Logon Customizing and Protecting Special Users

This section explains how to protect your R/3 System.

Protecting Special Users

Clients 000, 001 and 066 are created when your R/3 System is installed. Two special users are defined in clients 000 and 001. Since these users have standard names and 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 R/3 System are as follows:

- The R/3 System superuser, SAP*

  SAP* is the only user in the R/3 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 R/3 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 R/3 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 R/3 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.

For more details, see the following topics:

Securing User SAP* Against Misuse [Page 143]

Securing User DDIC Against Misuse [Page 145]

Securing User SAP* Against Misuse

The R/3 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 R/3 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.

You can find information on this in the Computing Center Management System [Ext.] documentation under *R/3 System Administration*.

If a user master record exists for SAP*, it behaves like a normal user. It is subject to authorization checks and its password can be changed.

Deactivating User SAP*

As SAP* is a known superuser, SAP recommends that you deactivate it and replace it with your own superuser. In the SAP* user master record, you should proceed as follows:

- Create a user master record for SAP* in all new clients and in client 066.
- Assign a new password to SAP* in clients 000 and 001.
- Delete all profiles from the SAP* profile list so that it has no authorizations.
- Ensure that SAP* is assigned to the user group SUPER to prevent accidental deletion or modification of the user master record.

The SUPER user group has a special status in the predefined user profiles. (They are described later in this topic.)

The users that are assigned to group SUPER can be maintained or deleted **only** by the new superuser that you define, provided that:

- you use the predefined profiles, and
- you follow SAP's other user and authorization maintenance recommendations.

Defining a New Superuser

To define a superuser to replace SAP*, you need only give a user the SAP_ALL profile. SAP_ALL contains all R/3 authorizations, including new authorizations released in the SAP_NEW profile.

SAP_NEW assures upward compatibility of authorizations. The profile ensures that users are not inconvenienced when a release or update includes new authorization checks for functions that were previously unprotected.

Securing User DDIC Against Misuse

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.

Limiting Logon Attempts and Predefining 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: 3. You can set it to any value between 1 and 99.

- *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: 12. You can set it to any value between 1 and 99.

- *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.

You maintain the system profile parameters by choosing *Tools* → *CCMS*, *Configuration* → *Profile maintenance*.

To make the parameters globally effective in an R/3 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 R/3 System.

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 [Page 148]

Specifying Impermissible Passwords [Page 149]

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 length of a password.

  Default: Three characters. You can set it to any value between 3 and 8.

- *login/password_expiration_time*: Number of days after which a password must be changed.

  To allow users to keep their passwords without limit, leave the value set to the default 0.

Specifying Impermissible Passwords

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

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

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

123* in table USR40 prohibits any password that begins with the sequence “123.”

123 prohibits any password that contains the sequence “123.”

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

Logging Off Idle Users

You can set up your R/3 System to log off idle users automatically 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 log off is not activated in the R/3 System. A user remains logged on no matter how long he or she may be inactive. You activate automatic log off by setting the system profile parameter *rdisp/gui_auto_logout* to the number of seconds of idleness that 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.

If you have activated this function, inactive users are logged off when the idle-time limit has elapsed. The system does not save data before logging off the user. Any unsaved data in the user's session is lost. The system does not display a dialog box requesting log-off confirmation in the event of an automatic logoff.

A user is considered to be idle after choosing ENTER, or after other actions that transfer control to the application server to which a user is logged on.

Procedure

To activate automatic log off, proceed as follows:

1. Start the system profile maintenance function by choosing *Tools* → *CCMS, Configuration* → *Profile maintenance*.
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.

   Set the parameter in the default profile (DEFAULT.PFL) to activate automatic logoff throughout the system. However, if you want to activate automatic logoff only in the SAP application servers that use the profile(s), 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 only work for long periods of time with 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 R/3 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 on logon groups, see the Computing Center Management System documentation.

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

Logon and Password Security in the R/3 System

This section provides a general overview of logon and password security in the R/3 System.

The Initial Password

When you create a user, you are required to enter a password for the user. The password must meet all of the internal requirements set by the R/3 System as well as any Customizing changes that you have made. For more information, see Setting Password Controls [Page 147].

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

Password Requirements

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

Password Requirement	Type
Minimum length: 3 characters	Can be customized. Minimum length can be increased
Expiration	Can be customized. Number of days after which a password must be changed can be set. Default: password must not be changed
Password may not be set to a value that is contained in a "lock-out list"	Can be customized. Default: all passwords, except PASS and SAP*
First character may not be ! or ?	Fixed in R/3 System
First three characters may not appear in the same sequence in the user ID	Fixed in R/3 System
First three characters may not be identical	Fixed in R/3 System
Space character not allowed within first three characters	Fixed in R/3 System
Password may not be PASS or SAP*	Fixed in R/3 System
Any character which may be typed on the keyboard is allowed in a password. Password is not case-sensitive. No distinction is made between upper- and lowercase letters	Fixed in R/3 System
A user can change his or her password no more than once a day. Restriction does not apply to user administrators	Fixed in R/3 System
Password may not be changed to any of a user's last five passwords	Fixed in R/3 System

For help in setting the customizable password requirements, see Customer-Defined Password Protection [Page 147]

Logging On

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

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

- The user has been locked. If this is the case, the user is not permitted to log on.

  As user administrator, you can lock a user to prevent logons. You can find further details in Locking and Unlocking User Master Records [Page 23].

- The user's current password is not longer valid. If so, the user must enter a new password before proceeding.

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

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

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

Logon Errors

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

If a user enters an incorrect password, then the system allows the user two retries before terminating the logon attempt. Should the user continue to enter an incorrect password in subsequent logon attempts, then the system automatically locks the user against further logon attempts. The default maximum number of consecutive incorrect password entries is set to 12. You can set both of these incorrect logon limits to any value between 1 and 99. For more information, see Setting Password Controls [Page 147].

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.