Chapter 42: Overviewing User Administration

Contents

Introduction

The R/3 System lets you define and maintain users and user authorizations. The user and authorization system gives you precise control over user access to the R/3 System. The definition and validation of authorizations technology is integrated into the SAP development environment and can therefore be easily added to customer modules.

User administration in a productive environment is an ongoing process of creating, deleting, changing, and monitoring users and authorization objects. Administrators' roles in this process differ depending on the level of delegation regarding user administration tasks.

System Users

Users are client-specific. That is, they must be separately defined for each client in your system. A user definition has many components, including the following:

Basic User Data:

- name
- password
- address
- company information

User Defaults:

- logon language
- default printer
- date and decimal formats

User Profile Information:

- authorization profiles which determine which parts of the system a user can access
- user groups
- dates when the user's account is active and when it expires

Discussed in this section are two ways to create a new user:

1. Starting from scratch by defining the various user components, or
2. Making a copy of an existing user. Copying a user will create a new user that has the same authorizations as the original. You also have the option to copy a user's defaults, address, and memory parameter settings.

External and Internal Users

We can differentiate users into two main environments:

External

External users includes those created for:

- Windows NT activities
  - <SAPSID>adm, Administrator, SAPService <SAPSID>
- database connections
  - SAPR3, DB Administrator, SQL users

R/3 or Internal

R/3 or Internal users are those created and maintained in the R/3 System. In the R/3 System, each user is assigned with one user type. This *User Type* controls how the user interacts with the R/3 system.

The different user types are:

1. Dialog

User Type *Dialog* is used for on-line transaction handling. This will be the majority of your user population. This type of user is able to interactively logon and use the R/3 system. These users require:

- the *Authorization Profiles* required to perform their system and/or business tasks
- a *Password*

Although not required, they should be assigned to a user group .

2. Background

Background user types are used to run background jobs. These users **cannot logon and work** interactively.

The administrator can create background users with all the authorizations required to perform a series of tasks. When defining the background jobs, you change the user field to the background user name you created, and all authorization checks will go against the background user as opposed to the user creating the job.

Background users are not affected by password control parameters. That is, password expirations, length, and other profile parameters used to control passwords do not apply to background users.

3. CPIC

The SAPCPIC user is delivered in client **000** with no authorizations. The CPIC user performs logons using the CPI-C interface. The interface does not work interactively with the R/3 system. This is the user that receives return codes from External programs and the *Statistic Collectors* (see note 3310). SAPCPIC is no longer required for the SM51 transaction.

This user, as with all types of users, requires authorization to perform its necessary activities in the SAP System. That is, like a dialog user, CPIC, Background and BDC users are subject to the same authorization checks as a normal Dialog user.

Special R/3 Users

SAP*

The super user SAP* is pre-defined in the clients 000 and 001 in the R/3 System. Although a user master-record for SAP* is created during installation, this record is not strictly necessary since SAP* is programmed in the *system code*.

If you delete the user master record for SAP*, then SAP* has the following properties:

- the user possesses **all authorizations** because no checks are performed.
- the standard password "PASS" cannot be changed.

DDIC

The DDIC user is responsible for the maintenance of the ABAP/4 Dictionary and the software logistics.

A user master record for the DDIC user is automatically created in the clients 000 and 001 when the R/3 System is installed. This user has a standard the password *19920706*. The system code pre-defines certain

authorizations for the DDIC user. For example the only user that can log into the R/3 System while a new release is being installed.

You should protect the DDIC user against unauthorized access by changing its initial password in the clients **000** and **001**. User DDIC is required for certain installation and setup tasks in the system, so you should not delete DDIC.

EarlyWatch

The EarlyWatch user is delivered in client 066 of every SAP system. The initial password for this user is *SUPPORT*. This user is used by SAP's EarlyWatch experts. It has access to monitoring and performance data only. This user should not be deleted, but the password should be changed. This user is delivered in client 066 only. This client should not be used or deleted.

Creating Users

There are 3 methods for creating users.

- *Creating* - Using transaction **SU01**
- *Copying* - Using **SU01**, creating a template user, and copying it to other similar users (manually entering each password)
- *Writing a Batch Input*- Creating a user list (legacy download, manually, etc.)

The hierarchical security effect of User Groups enables the administrator to distribute user maintenance tasks while still maintaining a high level of security. Within a specific group, security tasks can be distributed such that three different people are required to create users and manage authorizations. This series of checks and balances ensures the administrator that no single person is able to circumvent the R/3 authorization scheme.

User and authorization administrators within a specific group can only complete certain parts of the tasks required to add users and change authorities.

Creating and using an authorization involves three basic steps:

- Creating or maintaining Authorizations and/or Profiles
- Activating Authorizations and/or Profiles
- Creating and Maintaining User Master Records

If a company has a centralized organizational structure, it may be necessary for all maintenance tasks to be performed by a single user, the so-called Super User.

For the sake of security, however, the responsibility for the following maintenance tasks should be distributed to three different administrators:

Creating and Maintaining User Master Records

A user administrator creates user master records, maintains the list of profiles held in a user master record and sets user defaults. A user administrator cannot maintain or activate either profiles or authorizations..

When utilizing groups to control user administration, an administrator can enable User, Authorization and Activation Administrators to work with a specific subset of users and authorizations. See the **R/3 System On-Line Help** to see details on creating profiles to segregate and delegate these tasks.

User Groups

User Groups are used to enable the administrator to provide application managers with the rights they need to control their own users. In turn, these application managers can then control all users in their groups, as well as all users not yet assigned to a group. However, they cannot alter users in other groups.

Although a group affiliation is not required when creating users, it is necessary if you intend to delegate user maintenance tasks to the application managers and staff. We will show later how to use these groups to distribute user administration tasks to the appropriate application people.

Groups are normally based on requirements dictated by the different application groups and will be influenced by the number of users in each group. Since user groups are used for distributing user administrative tasks, your groups will be based on the organizational support structure that is made available. This structure will be typically based on business areas.

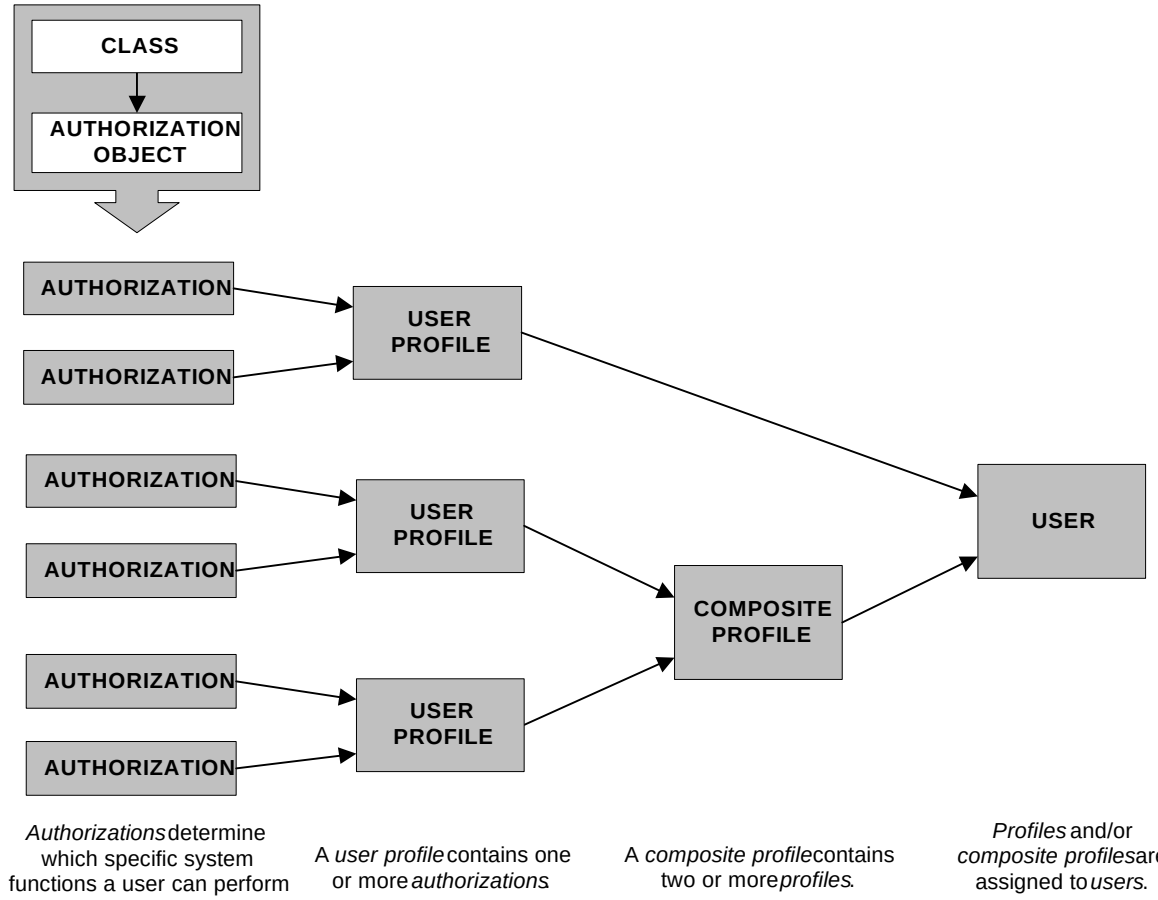
- Transaction **SU01** is used to create groups.
- Creating groups controls nothing until you set up your group administrators.
- A user can belong only to one group.
- Groups do not need to be created before assigning them to a user.

User Authorizations and User Profiles

User profiles allow you to organize access privileges by task or job function. Specifically, a user profile can contain all of the access privileges needed to perform a particular job, such as data entry or maintenance of an application. To authorize a user for a job, you need only give the user the corresponding user profile.

To simplify the task of setting up user profiles, the system provides a comprehensive set of default user profiles for the Basis System and R/3 applications. You can copy and customize these user profiles to provide the access privileges that you need.

The following components are defined in order to determine which system functions a particular user will be able to access:



- ***Authorizations***: Authorizations determine which specific system functions a user can perform. An authorization is created by selecting an *authorization object* from a *class* list (Basis, FI, HR). *Authorization objects* allow for complex tests of multiple conditions by grouping up to 10 *fields* that are tested with AND-logic. When the *authorization object* is named and its fields are defined, it becomes an *authorization*.
- ***User profiles***: A user profile contains one or more authorizations. For example, you can create a user profile containing the *SAPscript: Layout set* (S_SCRP_FRM) authorization and the *SAPscript: Style* (S_SCRP_STY) authorization. The user profile containing both of theses authorizations will control access to both layout sets and styles.
- ***Composite Profiles***: For users with multiple responsibilities in the system, you can define composite profiles. A composite profile assigns a list of simple and / or composite profiles to a user. A composite profile can contain all of the user profiles needed for the jobs performed by a user.
- ***Users***: One or more user profiles or composite profiles are assigned to a user. Entering user profiles (rather than individual authorizations) in user master records simplifies maintenance.

Mass Operations

The SAP System provides two utilities for performing operations on all or on selected sets of users:

- With *Utilities Mass changes Delete all users*, you can delete all users from a designated client. The utility presents a confirmation screen before carrying out the deletion.
- With *Utilities → Mass changes →User profile*, you can add or delete a profile from all or a selection of the user master records in a client.

Creating and Maintaining Authorization Profiles and Authorizations

An authorizations administrator can work with the maintenance versions of the profiles and authorizations only. The administrator cannot activate either profiles or authorizations. That is, he or she cannot make them take effect in the system.

See the On-Line help for detailed instructions and examples on how to setup this user's profiles and authorizations.

Activating Authorization Profiles and Authorizations

An activation administrator cannot change the access rights defined in profiles and authorizations. This administrator can only activate already existing maintenance versions of the profiles and authorizations.

See the On-Line help for detailed instructions and examples on how to setup this user's profiles and authorizations.

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

You can transport user master records, profiles, authorizations, and authorization objects from one SAP System to another. You can transport all three components independently, or transport profiles together with all of the authorizations that they contain.

To transport user master records, use the R3TR TABU development environment object in a transport request to select and transport entries from these tables:

- usr01: user master records (runtime data)
- usr02: logon data
- usr03: user address data
- usr04: user master record authorizations
- usr05: user SPA/GPA parameter values
- usr06, usr14: license data
- usr08, usr09, and usr30: user menu definition

Copying User Master Records

Use transaction */nSCC2* transport user master records, profiles, and authorizations between clients in an SAP System.

You must start */nSCC2* from the target client, (the client to which users and authorizations should be copied).

Do not use */nSCC2* if the target client contains authorizations and users that you wish to preserve. The report deletes all profiles and authorizations in the target client before it copies in the new profiles and authorizations. If you transport users, the existing user master records are also deleted.

Policies and Procedures

User Administration

Policies

Super Users SAP and DDIC*

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

User Naming Convention

- All users are assigned names identical to their employee ID numbers.

Maintaining Users

- The system administration department has to receive via e-mail the *User Modification Request Form* signed by the manager of the users application department.
- All profiles required by the user must be specifically listed on the request form. The form must indicate whether the user is temporary or permanent.
- For temporary employees, an account expiration date must be included.

Users leaving the Company

- First, the User Modification Request Form must be filled out and signed by the application department manager. A copy of this form must be sent to Human Resources department. The HR department must sign the request for deletion and mail the signed copy back to the system administration department.
- All employee master record information including internal post office must be deleted.

Procedures

Super Users SAP and DDIC*

- SAP* is used only for client copies.
- Pseudo super users are created in each client with SAP_ALL profile.
- Password is changed every month.

User Naming Convention

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

Maintaining Users

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

Users leaving the Company

– The User Modification Request Form must be completed and mailed to the system administration department and to the HR department manager. The HR department manager must confirm with signature and send the signed copy back to the system administration department.

Roles and Responsibilities

Task	Role
Maintaining Super Users	System Administrator
Maintaining Naming Conventions	Application Department Manager/HR Department
Maintaining Users	Application Department Manager/System Administrator
Maintaining Users leaving company	Application Dep. Manager/System Administrator/HR Dep.

System Security

Policies

IT-Manager

– The IT-Manager is responsible for all security aspects of the system. The Manager have to review and check the security strategy every two months.

Super Users

– For revision and security purposes the super-user SAP* will not be used for system maintenance. All maintenance has to be performed with newly defined super-users.

System Passwords

– The system passwords (DB user sapr3, O.S. user <SID>ADM, DDIC) must be changed every 4 weeks. Access to the passwords in case of emergencies must be ensured.

User Passwords

– To protect the system from unauthorized access, users will be forced to change their password every 4 weeks.
– A minimum password length of 6 characters is required.
– After 3 unsuccessful logon attempts the account will be locked.

SAP Connection

– The connection to SAP is only opened for a service session. These connections are: *OSS, Early Watch* and *Remote Consulting*.
– Connection to SAP can only be opened from the customer site.
– Connections have to be monitored with an appropriate tool.

SAPRouter

– SAPRouter is an SAP supplied tool is used for securing access to the R/3 system. SAPRouter is also necessary for connecting to SAP systems.

Remote connections

– For external connections (Mobile end-users) fixed IP addresses are assigned.
– One explicit entry per external connection is maintained in the permission list for SAPRouter.

Procedures

IT-Manager

- The IT-Manager together with the system administrator, will have a review meeting every two months to discuss and check the security aspects of the system.

Super Users

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

System Passwords

- The system passwords will be changed every 4 weeks by the system administrator. The system administrator must write down the current passwords and place them in a sealed envelope. This envelope must be stored in the data safe, and must be accessible in case of emergency.

User Passwords

- Users are forced to change their passwords every 4 weeks by setting the appropriate parameters in the DEFAULT profile. This ensures that these settings are valid within the whole system. The minimum password length is set to 6 characters. The intruder lockout count us set to 3.

SAP Connection

- A SAP connection is established by starting SAPRouter in the customer network and starting e.g. SAPGUI for an OSS connection

SAPRouter

SAPRouter is started and stopped once a day to make sure that there will be no open connections left

Remote connections

- For remote users, dedicated IP addresses are maintained. These addresses must also be maintained in the saprouttab to make sure no unauthorized user is allowed to logon to the R/3 system.

Roles and Responsibilities

Task	Role
Defining and Maintaining SAPROUTTAB	System Administrator
Monitoring Open Connections	Operator
Shutdown/Restart SAPRouter daily	Operator
Review Security Strategy	IT-Manager
Changing System Passwords	System Administrator

For further details refer to…

R/3 System Administration Made Easy

Introducing R/3 System Architecture

R/3 Basis Knowledge Products

System Management CD Reference → Implementation → User Administration

R/3 System Online Help

Basis Components → System Administration → Users and Authorizations

Basis Courses

Technical Core Competence—Windows NT/Oracle (BC 310)