



SAP AG
Neuottstr. 16
D-69190 Walldorf

R/3 Security

R/3 Security Guide : VOLUME II

R/3 Security Services in Detail

Version 2.0a : English

July 31, 1998

Copyright

©Copyright 1997 SAP AG. All rights reserved.

No part of this documentation may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG.

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 in the future.

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

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

IBM®, OS/2®, DB2/6000®, AIX®, OS/400® and AS/400® are a registered trademark 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.

SECUDE® is a registered trademark of GMD-German National Research Center for Information Technology.

SAP®, R/2®, R/3®, RIVA®, ABAP®, SAPoffice®, SAPmail®, SAPaccess®, SAP-EDI®, SAP ArchiveLink®, SAP EarlyWatch®, SAP Business Workflow®, R/3 Retail® are registered trademarks of SAP AG.

SAP AG assumes no responsibility for errors or omissions in these materials.

All rights reserved.

Table of Contents

CHAPTER 1 : INTRODUCTION	1-1
Chapter 1-1 : Security with R/3	1-1
Chapter 1-2 : How to Use the <i>R/3 Security Guide</i>	1-3
The R/3 Security Guide VOLUME II : R/3 Security Services in Detail	1-4
Chapter 1-3 : What is new in this guide?	1-6
Chapter 1-4 : Support and Feedback	1-7
Technical Consulting Services	1-7
Feedback	1-7
CHAPTER 2 : THE R/3 SECURITY TOOLBOX	2-1
Chapter 2-1 : User Authentication.....	2-3
Passwords	2-3
Protecting Standard Users	2-5
Preventing Unauthorized Logons	2-7
Security Measures When Using the Session Manager	2-8
Security Measures When Using SAP Shortcuts	2-8
Useful Procedures in User Authentication	2-9
Additional Information on User Authentication.....	2-10
Chapter 2-2 : R/3 Authorization Concept.....	2-11
Maintaining Authorizations and Profiles with the Profile Generator (PFCG)	2-12
Manually Maintaining Authorizations and Profiles	2-14
The Authorization Infosystem	2-15
Organizing Maintenance Tasks	2-16
Authority Checks	2-20
Reducing the Scope of Authority Checks in R/3.....	2-21
Additional Information on the R/3 Authorization Concept.....	2-22
Chapter 2-3 : Network Infrastructure.....	2-23
Network topology	2-23
Network Services.....	2-25
Routers and packet filters	2-27
The Firewall and SAProuter	2-28
Security Concept for an R/3 Network	2-31
Secure Network Communications (SNC).....	2-32
Additional Information on Network Security	2-36
Chapter 2-4 : Operating System Protection.....	2-37
R/3 Security under UNIX	2-37
R/3 Security under Windows NT	2-43
Logical Operating System Commands in R/3	2-53

Table of Contents

Chapter 2-5 : Database Access Protection	2-55
Access Using Database Tools.....	2-56
ORACLE under UNIX	2-57
ORACLE under Windows NT	2-64
INFORMIX under UNIX	2-70
ADABAS.....	2-73
DB2 Common Server under UNIX	2-81
DB2 Common Server under Windows NT.....	2-87
DB2/400	2-94
Chapter 2-6 : Protecting Your Productive System (Change & Transport System)	2-99
The R/3 System Landscape	2-99
Configuring the System Landscape for Changes.....	2-101
Defining the Transport Process	2-103
Responsibilities and their Corresponding Authorizations in R/3	2-104
Emergency Changes in the Productive System	2-105
Additional Information for Change & Transport System.....	2-106
Chapter 2-7 : Remote Communications (RFC & CPI-C).....	2-107
General Security Measures	2-107
RFC Authorizations.....	2-109
Trusted System Networks (RFC)	2-109
Authorizations for External Server Programs (RFC and CPI-C).....	2-110
Secure Network Communications for Remote Communications.....	2-111
Additional Information on Remote Communications	2-111
Chapter 2-8 : Secure Store & Forward Mechanisms (SSF) and Digital Signatures	2-112
Protecting Private Keys	2-113
Protecting Public Keys	2-113
SAP Security Library (SAPSECULIB).....	2-114
Additional Information on SSF and Digital Signatures.....	2-115
Chapter 2-9 : Logging and Auditing.....	2-116
The Audit Info System (AIS)	2-116
The Security Audit Log	2-117
System Log.....	2-118
Statistic Records in CCMS	2-120
Logging of Specific Activities.....	2-120
Additional Information for Logging and Auditing	2-123
Chapter 2-10 : Special Topics.....	2-124
R/3 Internet Application Components (IAC).....	2-124
Protecting Application Link Enabling (ALE) Applications	2-137
R/3 Online Services	2-140
Virus Protection and Integrity Checks.....	2-142
Protecting Specific Tables, Authorizations Objects, etc.....	2-142

CHAPTER 3 : SUMMARY	3-1
Chapter 3-1 : Tools, Transactions, and Reports.....	3-1
Chapter 3-2 : Profile Parameters.....	3-3
Chapter 3-3 : Authorization Objects	3-9

Table of Figures

Figure 2-2-1 : Authorization Maintenance in R/3 / Profile Generator	2-12
Figure 2-2-2 : Organization of User Maintenance Tasks	2-16
Figure 2-3-1 : Separating Frontend LANs from the Server LAN	2-24
Figure 2-3-2 : Firewall.....	2-28
Figure 2-3-3 : Recommended R/3 Network Topology	2-31
Figure 2-3-4 : Two-way Connection Using the SAProuter and a Router/Packet Filter	2-32
Figure 2-3-5 : Application Level Protection Provided by SNC	2-33
Figure 2-3-6 : Network Area Protected with SNC	2-34
Figure 2-3-7 : SNC Protection between SAProuters	2-35
Figure 2-4-1 : R/3 Directory Structure under UNIX	2-40
Figure 2-4-2 : NT Domains MASTER and SAP	2-48
Figure 2-4-3 : Windows NT and R/3 Administration Users and Groups	2-49
Figure 2-5-1 : DB2/400 User Security Concept	2-95
Figure 2-6-1 : Recommended Three-Tier System Landscape.....	2-100
Figure 2-10-1 : The Internet Transaction Server	2-124
Figure 2-10-2 : The Internet Transaction Server Architecture	2-126
Figure 2-10-3 : Providing ITS Security.....	2-128
Figure 2-10-4 : Example ITS Network Topology.....	2-132

Table of Tables

Table 1-2-1	: Typographical Information Used in this Guide	1-5
Table 1-2-2	: Standard Notations used in this Guide.....	1-5
Table 2-0-1	: The Security Toolbox	2-1
Table 2-0-2	: Sources for Information for Additional Areas of Interest.....	2-2
Table 2-1-1	: Profile Parameters Applying to Passwords	2-4
Table 2-1-2	: Default Passwords for Standard Users	2-5
Table 2-1-3	: Loss of Functions when Locking the User SAPCPIC.....	2-6
Table 2-1-4	: Profile Parameters Applying to Preventing Unauthorized Logons.....	2-8
Table 2-2-1	: Organization of the User Administrators when using the Profile Generator	2-17
Table 2-2-2	: Organization of the User Administrators When Maintaining Profiles Manually.....	2-19
Table 2-3-1	: Ports used by R/3	2-27
Table 2-3-2	: SNC-Protected Communication Paths.....	2-34
Table 2-4-1	: Setting Access Privileges for R/3 Directories and Files under Unix	2-41
Table 2-4-2	: Users and their Functions under Windows NT.....	2-45
Table 2-4-3	: Database Users	2-47
Table 2-5-1	: Changing the Passwords for ORACLE Standard Users (ORACLE / UNIX)	2-57
Table 2-5-2	: Setting Access Privileges for ORACLE Directories and Files (ORACLE / UNIX).....	2-60
Table 2-5-3	: Changing the Passwords for ORACLE Standard Users (ORACLE / Windows NT)	2-64
Table 2-5-4	: Setting Access Privileges for DB2/CS Directories and Files (ORACLE / Windows NT).....	2-65
Table 2-5-5	: Changing the Passwords for INFORMIX Standard Users (INFORMIX / UNIX)	2-70
Table 2-5-6	: Setting Access Privileges for INFORMIX Directories and Files (INFORMIX / UNIX)	2-71
Table 2-5-7	: Changing the Passwords for ADABAS Standard Users (ADABAS / All).....	2-73
Table 2-5-8	: Changing the Passwords for ADABAS Standard Users (ADABAS / UNIX)	2-75
Table 2-5-9	: Setting Access Privileges for ADABAS Directories and Files (ADABAS / UNIX)	2-75
Table 2-5-10	: Changing the Passwords for DB2/CS Standard Users (DB2/CS / UNIX).....	2-82
Table 2-5-11	: Setting Access Privileges for DB2/CS Directories and Files (DB2/CS / UNIX)	2-84
Table 2-5-12	: DB2/CS Standard Users under Windows NT (DB2/CS / Windows NT)	2-88
Table 2-5-13	: DB2/CS Standard Groups under Windows NT (DB2/CS / Windows NT).....	2-88
Table 2-5-14	: Managing the Passwords for DB2/CS Standard Users (DB2/CS / Windows NT)	2-90
Table 2-5-15	: Environment Variables for DB2/CS under Windows NT (DB2/CS / Windows NT)	2-90
Table 2-5-16	: Setting Access Privileges for DB2/CS Directories and Files (DB2/CS / Windows NT).....	2-91
Table 2-5-17	: Changing the Passwords for DB2/400 Standard Users (DB2/400)	2-97
Table 2-6-1	: Authorization Profiles for Change and Transport Roles	2-105
Table 2-6-2	: Authorizations for Development and Transport.....	2-105
Table 2-9-1	: Profile Parameters for the Security Audit Log	2-117
Table 2-9-2	: Profile Parameters and File Locations for the System Log	2-119
Table 2-9-3	: Profile Parameters for Statistic Records in CCMS	2-120
Table 3-1-1	: Tools, Transactions, and Reports in R/3.....	3-1
Table 3-2-1	: Profile Parameters	3-3
Table 3-3-1	: Authorization Objects.....	3-9

Table of Useful Procedures

UP 2-1-1	: Specifying Impermissible Passwords.....	2-9
UP 2-1-2	: Defining a new Super User and Deactivating SAP*	2-9
UP 2-1-3	: Changing the Passwords for Standard Users	2-9
UP 2-5-1	: Changing the Passwords for <sid>adm and ora<sid> (ORACLE / UNIX)	2-61
UP 2-5-2	: Changing the Passwords for SYS, SYSTEM, and SAPR3 using chdbpass (ORACLE / UNIX)	2-62
UP 2-5-3	: Setting Access Privileges for Files and Directories (ORACLE / UNIX)	2-63
UP 2-5-4	: Specifying the Name of the User that Starts R/3 - SAPService<SID> (ORACLE / Windows NT)...	2-67
UP 2-5-5	: Creating an OPS\$ User for <SID>ADM (ORACLE / Windows NT).....	2-67
UP 2-5-6	: Creating an OPS\$ User for SAPService<SID> (ORACLE / Windows NT).....	2-68
UP 2-5-7	: Changing the Password of SAPR3 (ORACLE / Windows NT).....	2-68
UP 2-5-8	: Changing the passwords for <sid>adm, sapr3, and informix (INFORMIX / UNIX).....	2-71
UP 2-5-9	: Setting Access Privileges for Files and Directories (INFORMIX / UNIX).....	2-72
UP 2-5-10	: Changing the Passwords for the Users CONTROL, SUPERDBA, and OPERATOR (ADABAS / All)	2-77
UP 2-5-11	: Updating the XUSER File for the Users CONTROL and SUPERDBA. (ADABAS / All).....	2-77
UP 2-5-12	: Changing the Password of SAPR3 As User SAPR3 (ADABAS / All).....	2-78
UP 2-5-13	: Changing the Password of SAPR3 As User SUPERDBA (ADABAS / All)	2-78
UP 2-5-14	: Updating the XUSER File for the User SAPR3 (ADABAS / All).....	2-79
UP 2-5-15	: Changing the Passwords for <sid>adm and sqd<sid> (ADABAS / UNIX)	2-79
UP 2-5-16	: Setting Access Privileges for Files and Directories (ADABAS / UNIX)	2-80
UP 2-5-17	: Changing the password for db2<sid> (DB2/CS / UNIX)	2-85
UP 2-5-18	: Setting Access Privileges for Files and Directories (ADABAS / UNIX)	2-85
UP 2-5-19	: Recreating the File dscdb6.conf (DB2/CS / Windows NT).....	2-92
UP 2-5-20	: Changing the Environment Variable DB2DB6EKEY (DB2/CS / Windows NT)	2-93
UP 2-5-21	: Changing the passwords for <SID>OFR and <SID>OPR Using CHGPWD (DB2/400)	2-98
UP 2-10-1	: Verifying Required Authorizations using Trace	2-139



Table of Useful Procedures

Chapter 1 : Introduction

Chapter 1-1 : Security with R/3

The most important aspect involved when establishing and implementing a security policy for R/3 security is your own demands and priorities on security for your system. Before beginning, you need to ask yourself "What is it that you want to achieve", and "What does security mean to you?" The following list provides a sample of questions to ask yourself:

- Does security mean that unauthorized persons do not have access to certain data?
- Does it mean that no-one can retrieve information over unauthorized means (for example, eavesdropping)?
- Does it mean that activities are recorded so that they can be reconstructed?
- Does it mean that individuals can be held responsible for actions that they perform using the R/3 System?

Do all of these questions mean "security" for your system, or only some of them? Which apply to your needs, and which do not? What else does "security" mean to you and where else is protection important for your system?

Once you have determined what security means to you and your system, you can proceed with the task of deciding where and from what you need protection (protecting your system from threats).

Threats to your system

Security strives to protect your system from known or unknown threats. Therefore, to determine where you want to take security measures, you need to determine which threats are potential hazards for your system. Threats may include:

- Annoyed or frustrated employees
- Eavesdroppers or "hackers" who want to gain sensitive information (for example, a competitor looking for useful statistics)
- User errors or carelessness
- Software errors

You need to decide which threats are relevant and how much it is worth to provide protection.

Chapter 1 : Introduction

R/3 Security

In addition, you need to consider the R/3 System itself. R/3 is a sophisticated system with many areas that are relevant to security. Within R/3, you need to consider some or all of the following areas:

- User Authentication Methods
- The R/3 Authorization Concept
- Your Network Infrastructure
- The Operating System that you use
- Database Access
- The R/3 Change and Transport System
- Logging and Auditing
- Remote Communications (RFC & CPI-C)
- Secure Store & Forward Mechanisms and Digital Signatures
- Internet Application Components (IAC)
- Application Link Enabling Applications (ALE)
- R/3 Online Services

In this volume of the *R/3 Security Guide*, we include details on how these areas in R/3 deal with security. Depending on your policy and your priorities, you may need to handle some or all of these areas. When implementing your security policy, you can refer to this guide for a collection of the measures, tools, and guidelines available in R/3.

Chapter 1-2 : How to Use the *R/3 Security Guide*

The *R/3 Security Guide* consists of three separate volumes, with different levels of detail:

R/3 Security Guide VOLUME I : An Overview of R/3 Security Services

R/3 Security Guide VOLUME II : R/3 Security Services in Detail

R/3 Security Guide VOLUME III : Checklists

R/3 Security Guide VOLUME I : An Overview of R/3 Security Services

The *R/3 Security Guide VOLUME I* provides a general overview of the security services that we offer in R/3. With *VOLUME I*, you can familiarize yourself with these services, for example, before establishing a security policy or before installing an R/3 System.

R/3 Security Guide VOLUME II : R/3 Security Services in Detail

This part of the *R/3 Security Guide* concentrates on the technical measures involved with R/3 System security. It contains descriptions of the tasks involved, as well as our recommendations for the various components of the R/3 System. Use *VOLUME II* once you have established a security policy and are ready to implement it for your R/3 System.

R/3 Security Guide VOLUME III : Checklists

The third part of the *R/3 Security Guide* complements *VOLUME II* with checklists. You can use these checklists to record those measures that you have taken and for assistance when reviewing and monitoring them.

Updates

We will also publish updates to the guide as necessary. These updates will also be available over SAPNet in regular intervals.

The R/3 Security Guide VOLUME II : R/3 Security Services in Detail

You are currently working with the *R/3 Security Guide VOLUME II : R/3 Security Services in Detail*. The prerequisites for using this volume are:

- An existing security policy
- Technical knowledge of R/3, as well as the database, operating, and networking systems.
- Time and resources

Security is an aspect of quality; it is an investment - of both time and resources. We recommend you dedicate sufficient time and allocate ample resources to implement your security policy and to maintain the level of security that you desire.

Finding Your Way in *Volume II*

To find information in *VOLUME II* of the *R/3 Security Guide*, refer to the following contents:

- **Chapter 1 : Introduction**

This chapter provides:

- Introductory Material on R/3 security and how to use the R/3 Security Guide
- The R/3 Releases for which the guide is valid
- Typographical Information and Standard Notations
- What is new in this version of the guide
- Where to obtain support and how to provide us with feedback

- **Chapter 2 : The R/3 Security Toolbox**

This chapter provides the **R/3 security toolbox**. This is a collection of the various tools, mechanisms, and guidelines for providing security for your R/3 System. You can find the exact contents of the R/3 security toolbox on Page 2-1.

- **Chapter 3 : Summary**

This chapter summarizes the guidelines and measures from Chapter 2, to include the following :

- R/3 Security-Relevant Tools and Transactions
- R/3 Security-Relevant Profile Parameters
- R/3 Security-Relevant Authorization Objects and Profiles

- **Appendix A : List of References**

This appendix includes a list of the sources of additional information.

- **Feedback Reply Form**

We are interested in knowing how well the R/3 Security Guide meets your needs. Give us your feedback using the Feedback Reply Form provided at the end of the guide.

Valid Releases

This version of the *R/3 Security Guide* applies to R/3 Releases 3.0, 3.1, and 4.0. Where applicable, references to other releases are explicitly indicated.

Typographical Information and Standard Notations

The following tables explain the meanings of the various formats, symbols, and standard notations used in the guide.

Table 1-2-1 : Typographical Information Used in this Guide




This text format	helps you identify
<i>Screen Text</i>	words or characters you see on the screen (this includes system messages, field names, screen titles, menu names, and menu items).
User Entry	exact user input. These are words and characters you type on the keyboard exactly as they are in the documentation.
<Variable User Entry>	variable user input. Pointed brackets indicate that you replace these variables with appropriate keyboard entries.
ALL CAPITALS	report names, program names, transaction codes, table names, ABAP language elements, file names, and directories.
<i>Book Title</i>	cross-references to other books or references.
KEY name	keys on your keyboard. Most often, function keys (for example, F2 and the ENTER key) are represented this way.
Technical Object Name	names of technical objects outside of the R/3 System (for example, UNIX or Windows NT filenames or environment variables).
This icon	helps you identify
 Example	an Example. Examples help clarify complicated concepts or activities.
 Note	a Note. Notes can contain important information like special considerations or exceptions.
 Caution	a Caution. Cautions help you avoid errors such as those that could lead to data loss.

Table 1-2-2 : Standard Notations used in this Guide

This Notation	helps you identify
<sid>, <SID>	the three character System ID; lower and upper case respectively.
<SYS>	the R/3 system number
<sid>adm, <SID>ADM	the R/3 system administrator at the operating system level; lower and upper case respectively. Exception: Under AS/400, the system administrator is the user <SID>OFR.

Chapter 1-3 : What is new in this guide?

If you are familiar with the older version of the *R/3 Security Guide*, you may want to take note of the following new topics contained in the guide.

New Topics

New topics include:

- **The Profile Generator**
(see *Chapter 2-2 : R/3 Authorization Concept*)
- **Protecting Database Access - DB2 Common Server and DB2/400**
(see *Chapter 2-5 : Database Access Protection*)
- **Secure Store and Forward Mechanisms and Digital Signatures**
(see *Chapter 2-8 : Secure Store & Forward Mechanisms (SSF) and Digital Signatures*)
- **The Security Audit Log and the Audit Info System**
(see *Chapter 2-9 : Logging and Auditing*)
- **Protecting R/3 Internet Application Components**
(see *Chapter 2-10 : Special Topics*)
- **Protecting ALE Applications**
(see *Chapter 2-10 : Special Topics*)

Additionally, sections that were already included in the former version have been updated to include any changes that may apply.

Chapter 1-4 : Support and Feedback

Technical Consulting Services

If the *R/3 Security Guide* does not satisfactorily answer all of your questions, or if additional questions arise, contact our Technical Consulting Services.

We currently offer the following services:

- Support and consulting services when establishing a company-wide security policy
- Security analysis services
- Individual consulting services on security in the R/3 environment
- Support services when establishing a Windows NT domain concept
- Consulting services when using the Internet Transaction Server
- CA900 Course: Technical Revision - System Security
- Workshop on the R/3 Authorization Concept

For further information, contact us in the Technical Consulting Department at: **+49 6227 / 7-41537**.

Feedback

We are also interested in knowing how well the *R/3 Security Guide* meets your needs. If you have comments pertaining to the contents or quality of this guide, use the Feedback Reply Form provided at the end of the guide and return it to us at the following address or fax number:

SAP AG
CCMS & Security Department
Postfach 1461
D-69190 Walldorf
Germany

Fax: **+49-6227 / 7-41198**

Chapter 2 : The R/3 Security Toolbox

The security of your R/3 System depends on a large number of factors. For example, it depends on the security of your operating system, your network topology, your authorization plan, and the communication methods that you use, just to name a few. Depending on your policy, you may or may not decide to take measures in all of these areas of your R/3 System.

For those areas where you decide to take measures, you need the appropriate tools, mechanisms, and guidelines. In this chapter, you will find the **R/3 Security Toolbox**. It contains descriptions of the various tools and mechanisms that apply to R/3 security. Table 2-0-1 lists the various areas in R/3 and where you can find the appropriate tools measures in this guide that apply to each.

Table 2-0-1 : The Security Toolbox

Topic	in Section:	on Page:
User Authentication	Chapter 2-1	2-3
R/3 Authorization Concept	Chapter 2-2	2-11
Network Infrastructure	Chapter 2-3	2-23
Operating System Protection	Chapter 2-4	2-37
R/3 Security under UNIX		2-37
R/3 Security under Windows NT		2-43
Logical Operating System Commands in R/3		2-53
Database Access Protection	Chapter 2-5	2-55
Access Using Database Tools		2-56
ORACLE under UNIX		2-57
ORACLE under Windows NT		2-64
INFORMIX under UNIX		2-70
ADABAS		2-73
DB2 Common Server under UNIX		2-81
DB2 Common Server under Windows NT		2-87
DB2/400		2-94
Protecting Your Productive System (Change & Transport System)	Chapter 2-6	2-99
Remote Communications (RFC & CPI-C)	Chapter 2-7	2-107
Secure Store & Forward Mechanisms (SSF) and Digital Signatures	Chapter 2-8	2-112
Logging and Auditing	Chapter 2-9	2-116
Special Topics	Chapter 2-10	2-124
R/3 Internet Application Components (IAC)		2-124
Protecting Application Link Enabling (ALE) Applications		2-137
R/3 Online Services		2-140
Virus Protection and Integrity Checks		2-142
Protecting Specific Tables, Authorizations Objects, etc.		2-142

**Note**

The topics of system management, high availability, database management, and data protection are also important topics related to security. Although we do not cover these topics directly in this guide, they do belong in your 'big picture'. Refer to the following sources for more information on these topics.

Table 2-0-2 : Sources for Information for Additional Areas of Interest

Topic	Documentation
System Management: CCMS	<ul style="list-style-type: none"> • R/3 Online Documentation: BC Computer Center Management System [A.4]
High Availability	<ul style="list-style-type: none"> • SAP Documentation: BC SAP High Availability Guide [E.3] • R/3 Online Documentation: BC SAP High Availability [A.19]
Backup, Restore, and Recovery	<ul style="list-style-type: none"> • R/3 Online Documentation: BC SAP Database Administration [A.11]
Protection of Personal Data	<ul style="list-style-type: none"> • SAP Documentation: Leitfaden Datenschutz für SAP R/3, Material Number 50024598 (Germany only) [E.4]

Chapter 2-1 : User Authentication

An unauthorized user, who manages to access a system under a known user in the system, can proceed to do whatever is possible under this known user. If the known user happens to have access to critical information, then the impersonator also has access to the same information. Therefore, providing secure authentication protects the availability, integrity, and privacy of your system at every level.

We describe how R/3 facilitates secure authentication in the following sections:

- **Passwords**
- **Protecting Standard Users**
- **Preventing Unauthorized Logons**
- **Security Measures when Using the Session Manager**
- **Security Measures when Using SAP Shortcuts**
- **Useful Procedures in User Authentication**
- **Additional Information on User Authentication**

You can provide additional security by using an external security product, which may include using smart cards for strong authentication. See *Chapter 2-3 : Network Infrastructure*, in the section titled *Secure Network Communications (SNC)*.

Passwords

R/3 provides standard measures for password protection. There are a number of password "rules" that apply to defining passwords; there are also measures for protecting the transport and storage of passwords. We explain these measures in the following sections.

Password Rules

The following rules apply to passwords in a standard R/3 System:

- First time dialog users are assigned an initial password that has to be changed immediately when used for the first time.
- The default minimum length for passwords in R/3 is 3. You can change this value (see Table 2-1-1).
- The maximum length is 8.
- The first character cannot be '?' or '!'.
• The first three characters of the password cannot appear in the same order as part of the user name.
- The first three characters cannot all be the same.
- The first three characters cannot include space characters.
- The password cannot be PASS or SAP*.

Chapter 2 : The R/3 Security Toolbox

- The password is case-insensitive for dialog entries. (R/3 converts lower case characters in the password to upper case.)
- A user can only change his or her password in the course of logging on.
- A user can change his or her password at most once a day. (The user administrator is excepted from this rule.)
- You cannot reuse the last five passwords.
- You can force users to have to change their passwords after a set period of time (see Table 2-1-1).
- You can also prohibit certain character combinations in the Table USR40 (see UP 2-1-1).
- As of Release 3.0C, you can also define your own checks in the customer exit SUSR0001 (see OSS Note 37724 [C.12]).

**Note**

Avoid using names, dates, or words that can be found in a standard dictionary for passwords. There are many programs available that can automatically determine users' passwords that fit in these categories.

You can make a password relatively safe by including a mixture of alphabetic and numeric characters with at least one special character in the middle of the password.

We especially advise the system administrator to use a complex password with the maximum length (8 characters) that contains at least one digit and special character.

Password Storage and Transport

Passwords are stored in the database in a one-way hash. For the transport between the front end and the application server, the data is compressed. For increased security, you can use Secure Network Communications (SNC) and an external security product. With SNC, you eliminate the need to send the password over the network altogether. For more information, see *Chapter 2-3 : Network Infrastructure*, in the section titled *Secure Network Communications (SNC)*.

Profile Parameters

Table 4-1-1 shows the profile parameters in R/3 that apply to passwords.

Table 2-1-1 : Profile Parameters Applying to Passwords

Parameter	Description	Default	Permitted value
login/min_password_lng	Minimum length	3	3 - 8
login/password_expiration_time	Number of days after which a password must be changed.	0 (no limit)	any numerical value

Protecting Standard Users

R/3 creates the standard users SAP*, DDIC, SAPCPIC and EARLYWATCH during the installation process in the clients as shown in Table 2-1-2. To protect them from unauthorized access, you need to change their default passwords (see UP 2-1-3). We also describe additional measures for each of the users below.

Table 2-1-2 : Default Passwords for Standard Users

User	Description	Clients	Default Password
SAP*	R/3 System super user	000, 001, 066 (as of Release 3.0D)	06071992
		all new clients	PASS
DDIC	ABAP Dictionary and software logistics super user	000, 001	19920706
SAPCPIC	CPI-C user for the R/3 System	000, 001	admin
EARLYWATCH	Interactive user for the Early Watch™ service in client 066	066	support



Note

To find out which clients you have in your system, display the Table T000 using Transaction SM31.

To ensure that the SAP* user has been created in all clients and that the standard passwords have been changed for SAP*, DDIC and SAPCPIC, use the report RSUSR003. (See OSS Note 40689 [C.13] for more information.)

Protecting SAP*

To protect SAP*, you need to take the following precautions:

- **Do not delete the user SAP*!** SAP* is hard-coded in the R/3 System code and does not require a user master record! If a user master record for SAP* does not exist in a client, then SAP* exists at code level, has the password PASS, is not susceptible to authorization checks, and has **all** authorizations. Therefore, **do not delete SAP*** from any client.

You should define a new super user and deactivate SAP* without deleting it (see UP 2-1-2).

- As an alternative, you can deactivate the automatic user SAP* by activating the profile parameter `login/no_automatic_user_sap*` or `login/no_automatic_user_sapstar` (depending on release). For more information, see OSS Note 68048 [C.27].



Note

If a user master record was created for SAP*, then the authorizations there will apply; they are not affected by this parameter's setting.

- Change the default password (see UP 2-1-3).

Protecting DDIC

To protect the user DDIC, note the following:

- Do not delete the user DDIC from the system. Do not delete its profiles. This user has special privileges tasks in the installation process, for software logistics, and for the ABAP Dictionary.
- Change DDIC's default password (see UP 2-1-3).

Protecting SAPCPIC

The SAPCPIC user is a non-dialog user that can be used for calling certain programs and function modules in the R/3 System. To prevent misuse, you should either change its password or lock the user. Both options have disadvantages that you need to take into account.

- **Changing SAPCPIC's Password**

After changing SAPCPIC's password (see UP 2-1-3), you need to adjust the following programs. This only protects from external unauthorized access because the password appears in plain text in the affected programs. Refer to OSS Note 29276 [C.8] for more information.

- **RSM51000 (Transaction SM51)**
- **RSCOLL00**
- **RSCOLL30**
- **LSXPGU01**

- **Locking SAPCPIC**

Locking the user SAPCPIC results in the following loss of functions:

Table 2-1-3 : Loss of Functions when Locking the User SAPCPIC

Report	Loss of Function	Release
RSM51000 (Transaction SM51)	No display of process information	Release 2.1/2.2
RSCOLL00	No compilation of data	prior to Release 3.0F
Batch jobs	The last return code remains in active status if the last step calls an external program or command. To receive the proper return code, you can include a dummy program as the last step in the batch job.	prior to Release 4.0

You need to decide which method is best for you.

EARLYWATCH

The user EARLYWATCH is the interactive user for the Early Watch™ service in client 066. To protect this user, take the following precautions:

- Change its default password (see UP 2-1-3).
- Lock the user and unlock it only when necessary. Re-lock it after using it.

Summary

To summarize, we recommend that you regularly review the following criteria for protecting the standard users:

- Maintain an overview of the clients that you have and ensure that no unknown clients exist.
- Ensure that SAP* exists and has been deactivated in all clients.
- Ensure that SAP* belongs to the group SUPER in all clients.
- Ensure that the default passwords for SAP*, DDIC, and EARLYWATCH have been changed.
- Ensure that the default password for SAPCPIC has been changed or that the user has been locked.
- Lock the users SAP* and EARLYWATCH. Unlock EARLYWATCH only when necessary.

Preventing Unauthorized Logons

The following measures exist in R/3 to protect against unauthorized logons:

- You can use the report RSUSR006 (available as of Release 3.0E) to find out whether any known user has unsuccessfully attempted to logon. This report records the number of incorrect logon attempts by a user and user locks. We recommend that you schedule this report to run on a regular basis (daily).
- As of Release 4.0, you can use the Security Audit Log (Transactions SM18, SM19 and SM20) to record all successful and unsuccessful log-on attempts. Unknown user names and terminal number from where the logon or logon attempt occurred are also included in this log. See *Chapter 2-9 : Logging and Auditing* for more details.
- The system terminates a session if a set number of consecutive unsuccessful attempts to log on under a single user-id is exceeded (as specified in the profile parameter `login/fails_to_session_end`).
- You can hinder unauthorized access over an already logged-on user by configuring your R/3 System to automatically log users off if they have been inactive for a set period. Specify this value in the profile parameter `rdisp/gui_auto_logout`.
- The system locks a user-id if a set number of consecutive unsuccessful attempts to logon is exceeded under a single user ID. Set the number of invalid logon attempts that are allowed in the profile parameter `login/fails_to_user_lock`.

The system removes such locks at midnight on the same day; however, you can also manually remove locks at any time. You can also explicitly set locks for specific users. As of Release 3.1G, you can also specify that R/3 should not remove user locks automatically. (Set this flag in the profile parameter `login/failed_user_auto_unlock`).

Chapter 2 : The R/3 Security Toolbox

- The System Log records all locks. See *Chapter 2-9 : Logging and Auditing* for more details.
- Prior to Release 3.1H, when a user logs on to R/3, the system displays the date and time of the last log-on. The user can then see whether the date and time are correct. As of Release 3.1H, you can access the information over the *System* → *Status* menu path.
- Increase the access protection to your system by having your end users activate screen savers with passwords.
- You can use the SAP Logon Pad to ensure that users cannot change the SAP Logon configuration.

The following profile parameters are relevant to preventing unauthorized logons:

Table 2-1-4 : Profile Parameters Applying to Preventing Unauthorized Logons

Parameter	Description	Default	Permitted value
login/fails_to_session_end	Number of invalid login attempts until session end	3	1 - 99
login/fails_to_user_lock	Number of invalid login attempts until user lock	12	1 - 99
login/failed_user_auto_unlock	Automatically remove user locks at midnight	Y	Y or N
rdisp/gui_auto_logout	Maximum idle time for a user in number of seconds	0 (no limit)	unrestricted

Security Measures When Using the Session Manager

The SAP Session Manager is a tool for system logon and session control. With the Session Manager, you can manage your sessions in one or more R/3 Systems and in different R/3 clients.

For Releases 3.0E - 3.1G under Windows NT, you should run a patch that consists of exchanging a DLL in the SAPgui directory. For more information, see OSS Note 80723 [C.29].

Security Measures When Using SAP Shortcuts

As of Release 4.0B, SAP Shortcuts are available. The SAP Shortcuts save the user's logon information on the client. This improves comfort and performance; however, the data is saved in plain text. Anyone with access to the local information on the frontend client has access to the logon information. Therefore, we recommend that you use SAP Shortcuts only if you can appropriately protect your front ends from unauthorized access.

Useful Procedures in User Authentication

UP 2-1-1 : Specifying Impermissible Passwords

To specify impermissible passwords:

Enter the passwords that you want to prohibit in the Table USR40. (Use the Transaction SM30).

You can use '?' and '*' as wildcard characters. The '?' stands for a single character and the * stands for any combination of characters of any length.



Example

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

The entry ***123*** prohibits any password that contains the sequence "123."

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

UP 2-1-2 : Defining a new Super User and Deactivating SAP*

You should define and deactivate SAP* in all clients that exist in Table T000. Proceed as follows:

1. Create a user master record for a new super user.
2. Assign the profile SAP_ALL to this super user.
3. If no user master record exists in the client, then create a user master record for SAP*.
4. Assign the SUPER user group to SAP* (in all clients). This ensures that no one can change the user master record accidentally.
5. Deactivate all authorizations for SAP* (in all clients) by deleting all of the profiles in the profile list.

UP 2-1-3 : Changing the Passwords for Standard Users

Change the passwords for all of the standard users in those clients where they exist as displayed in the Table T000. (SAP* should exist in **all** clients.)

To change the passwords, proceed as follows:

1. Logon as the current super user.
2. Select *Tools* → *Administration* → *Maintain users* → *Users*.
3. Enter the <user-id> (SAP*, DDIC, SAPCPIC, or EARLYWATCH) in the *User* field.
4. Select *Goto* → *Change password*.
A dialog appears.
5. Enter the new password.

Additional Information on User Authentication

For more information, refer to the following documentation:

- [R/3 Online Documentation: BC Users and Authorizations → Access Security: Logon Customizing and Protecting Standard Users](#) [A.28]
- [OSS Note 2467](#): Answers on the topic of "Security" [C.2]
- [OSS Note 4326](#): No user exists with superuser privileges [C.3]
- [OSS Note 29276](#): SAPCPIC: At which points are passwords visible [C.8]
- [OSS Note 37724](#): Customer exits in SAP logon [C.12]
- [OSS Note 40689](#): New reports for the User Information System [C.13]
- [OSS Note 68048](#): Deactivating the automatic user SAP* [C.27]
- [OSS Note 80723](#): AUTOlogin Shared Library correction [C.29]

Chapter 2-2 : R/3 Authorization Concept

The R/3 authorization concept allows you to protect transactions and programs from unauthorized use. R/3 does not allow a user to execute transactions or programs, unless he or she has explicitly defined authorizations for the activity. To accomplish this, R/3 programs and transactions include authority checks, which ensure that users have the correct authorizations for an action.



Note

If you develop your own transactions or programs, you must include the authority checks in your developments yourself; see the section titled *Authority Checks* on page 2-20.

To successfully enforce this approach, you need to establish a reliable authorization plan. You need to take the time and define which users you allow to perform which tasks in your R/3 System. Then, in R/3, you need to assign to each user the authorizations that he or she needs to perform those tasks.

The development of a stable and reliable authorization plan is an ongoing process. We advise you to regularly review your authorization plan to ensure that it continually applies to your needs.

In the rest of this chapter, we describe what you need to take into account when working with the R/3 authorization concept. We include an overview of the profile generator and the Authorization Infosystem, two tools that can help you with maintaining your authorizations. However, this is only a brief overview. For a complete description, we advise you to refer to the *Authorizations Made Easy Guide* [E.2], the R/3 online documentation, or the documentation provided in the *Additional Information on the R/3 Authorization Concept* section.

This chapter is divided into the following sections:

- **Maintaining Authorizations and Profiles with the Profile Generator**
- **Manually Maintaining Authorizations and Profiles**
- **The Authorization Infosystem**
- **Organizing Maintenance Tasks**
- **Authority Checks**
- **Deactivating Authority Checks**
- **Additional Information on the R/3 Authorization Concept**

Maintaining Authorizations and Profiles with the Profile Generator (PFCG)

We recommend you use the profile generator (available as of Release 3.1G) to maintain your authorizations and profiles.

The profile generator makes your job easier by automating certain processes and providing more flexibility in your authorization plan. For example, you can assign profiles to job positions instead of only to individuals. If a person changes positions within the company, the profile generator automatically changes the authorization profile with the new assignment.

The framework for the profile generator lies in the building of activity groups, which you base on your company's organization plan. These activity groups form the link between the user and the corresponding authorizations. The actual authorizations and profiles exist in R/3 as objects.

When you work with the profile generator, you work with a level of information that is a step away from the actual objects in R/3. Figure 2-2-1 shows how these two levels are separated, yet linked together with the profile generator.

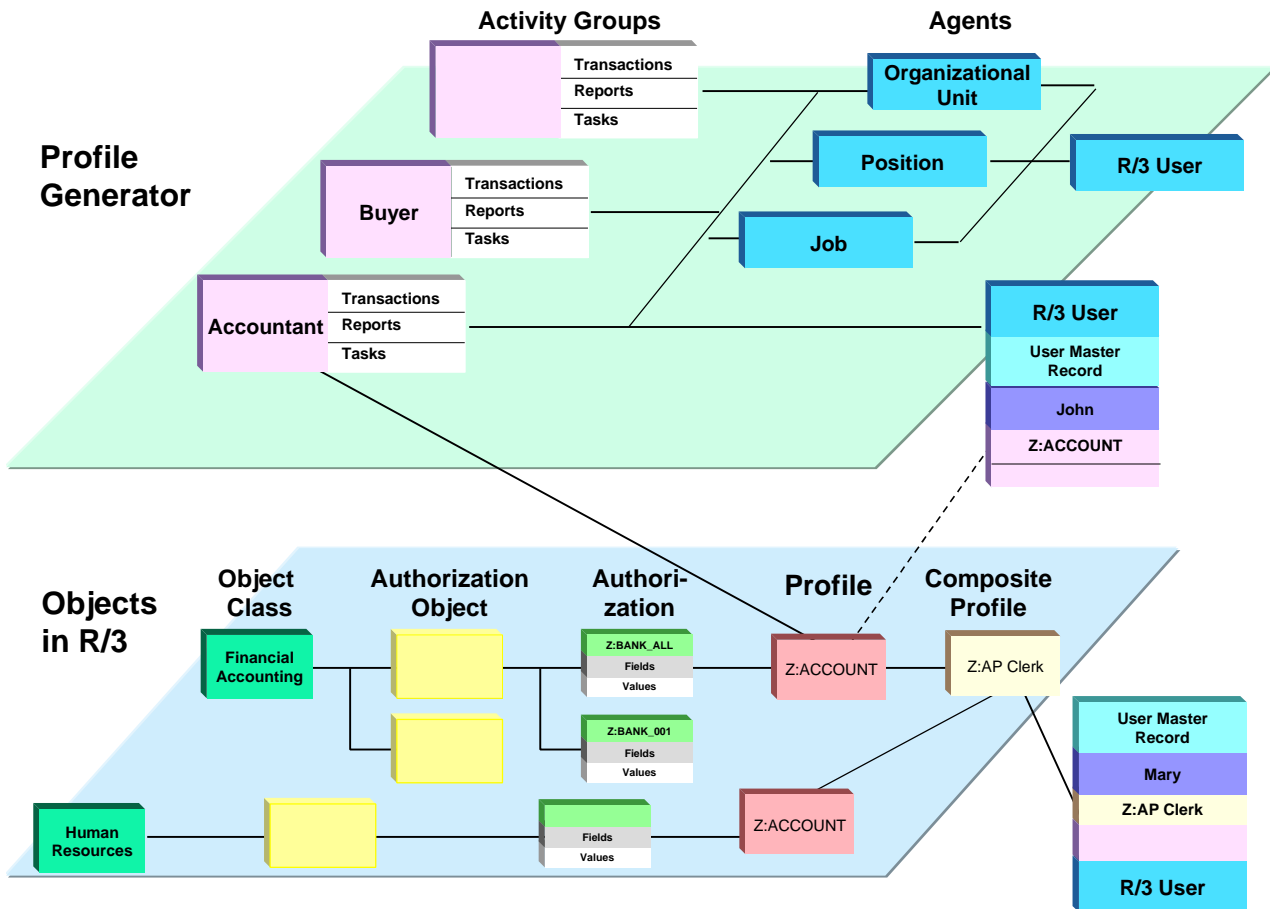


Figure 2-2-1: Authorization Maintenance in R/3 / Profile Generator

With the profile generator, you work in the upper level from Figure 2-2-1. You define the activity groups for your various job roles with the allowed activities. Based on this information, the profile generator determines the appropriate authorizations for a user belonging to the activity group.

The basic process is as follows:

1. Define Job Roles

For each application area in your company, define all of the job roles (for example, in a job role matrix). For each job role, determine the menu paths and transactions the users in this job role need to access. Determine the necessary access rights (display, change), as well as any restrictions that may apply.

2. Maintain Activity Groups in the Profile Generator (Transaction PFCG)

In the profile generator, create activity groups that correspond to the job roles. For each activity group, select those tasks (reports and transactions) that belong to the corresponding job role.

3. Generate and Maintain Authorization Profiles

In this step, the profile generator automatically builds the authorization profile that applies to the activity group. To accept or change the suggested profile, you must work your way through the profile tree structure and confirm the individual authorizations that you want to assign to the activity group.

4. Assign Activity Groups to Agents

You then assign the activity groups to any of the following:

- R/3 users
- Jobs
- Positions
- Organizational Units

By assigning activity groups to entities other than users, you increase the flexibility of your authorization concept. It is easier to maintain authorizations when a user changes jobs, for example.

5. Update User Master Records

In this step, you schedule a batch job that updates the user master records.

For more details, refer to the documentation provided in the *Additional Information on the R/3 Authorization Concept* section.

Manually Maintaining Authorizations and Profiles

You do not have to use the profile generator to maintain your profiles and authorizations. As an alternative, you can maintain them manually. In this case, you work directly with the lower level in Figure 2-2-1.

As with the profile generator, you need to first define all of the job roles in your company job role matrix. Then, for each job role, you define a set of authorizations. These authorizations consist of fields that contain values. The authority checks in R/3 use these values to determine if a user is allowed to perform specific actions. You can consolidate several authorizations into a single profile. You can also create composite profiles. You then assign each user those profiles that he or she needs to perform his or her job.

We describe the individual objects below:

- **Object Class**

The object class, for example Financial Accounting, groups together those authorization objects that apply to the class.

- **Authorization Objects**

An authorization object works as a template that you can use to define your authorizations. It contains a maximum of 10 fields per object.

- **Authorizations**

An authorization allows a user to perform a particular R/3 activity, based on a set of values that you define in the fields of the authorization object. (This particular activity may consist of sub-activities that also require authorizations. Note that these sub-authorizations are not necessarily included in the main authorization.)

Each authorization refers to exactly one authorization object and defines the permitted value range for each authorization field of this authorization object. In the above diagram, the authorization Z:BANK_ALL could be the authorization for all activities, and Z:BANK_0001 could be for a specific area (for example, authorizations for accounts receivable only).

- **Authorization Object Fields**

The fields in an authorization object are linked with data elements stored in the SAP ABAP Dictionary. The permissible values constitute an authorization. When an authorization check takes place, the system verifies the values provided by the user against those required to perform the action. The user may only perform the action if he or she satisfies the conditions for every field in the object. In our example, the authorization Z:BANK_0001 defines the values for the fields *Activity* and *Company code*. The field *Activity* could have the value '*', meaning that all activities are allowed, and the field *Company code* could have the value 03, meaning 'display' company codes.

- **Authorization Profiles**

You normally assign user authorizations in the user master records, not as authorizations, but as authorization profiles. You can create either single or composite profiles. In our example, Z:ACCOUNT is an authorization profile containing those authorizations applying to company codes.

- **User Master Records**

Each user that logs on to the SAP R/3 System must have a user master record. The user master record contains all the information pertaining to the user, including the authorizations.

In our example, a user with the Z:ACCOUNT profile defined in his or her user master record can then perform those activities defined in the authorizations contained in the profile.

**Note**

You assign the objects (authorizations, profiles, user master records, activity groups, etc.) per client. See the online documentation *BC Users and Authorizations → Transporting User Master Records, Authorizations and Profiles 0* and *BC Change and Transport Organizer [A.3]* or [A.25] on transporting these objects between clients or systems.

The Authorization Infosystem

The Authorization Infosystem (Transaction SUIM) offers you a range of selection criteria for users, profiles, authorization objects, authorizations, transactions, comparisons, where-used lists and change documents. With the Infosystem, you can quickly and easily retrieve authorization information from your R/3 System. The following are a few examples of lists that you can generate.

- Users with certain authorizations
- Authorizations that a particular user has
- All authorizations
- Profile comparisons
- Transactions that a specific user can execute
- Changes in the authorization profile for a user

We recommend that you regularly check the various lists that are important for you. Define a monitoring procedure and corresponding checklists to ensure that you continually review your authorization plan.

We especially recommend you determine which authorizations you consider critical and continually review which users have these authorizations in their profiles. Examples of authorization objects that you may consider critical include:

- S_ADMI_FCD
- S_USER_AUT
- S_TABU_DIS
- S_TABU_CLI
- S_DEVELOP
- S_TRANSPRT

Organizing Maintenance Tasks

We recommend that you divide your user authorizations tasks between different administrators. Each administrator should only be able to perform certain tasks. By separating these tasks, you ensure that no single superuser has total control over your user authorizations. You also ensure that more than one person approves all authorizations and profiles.

These administrators with our recommended activity lists are shown in Figure 2-2-2 and described in more detail in the following sections:

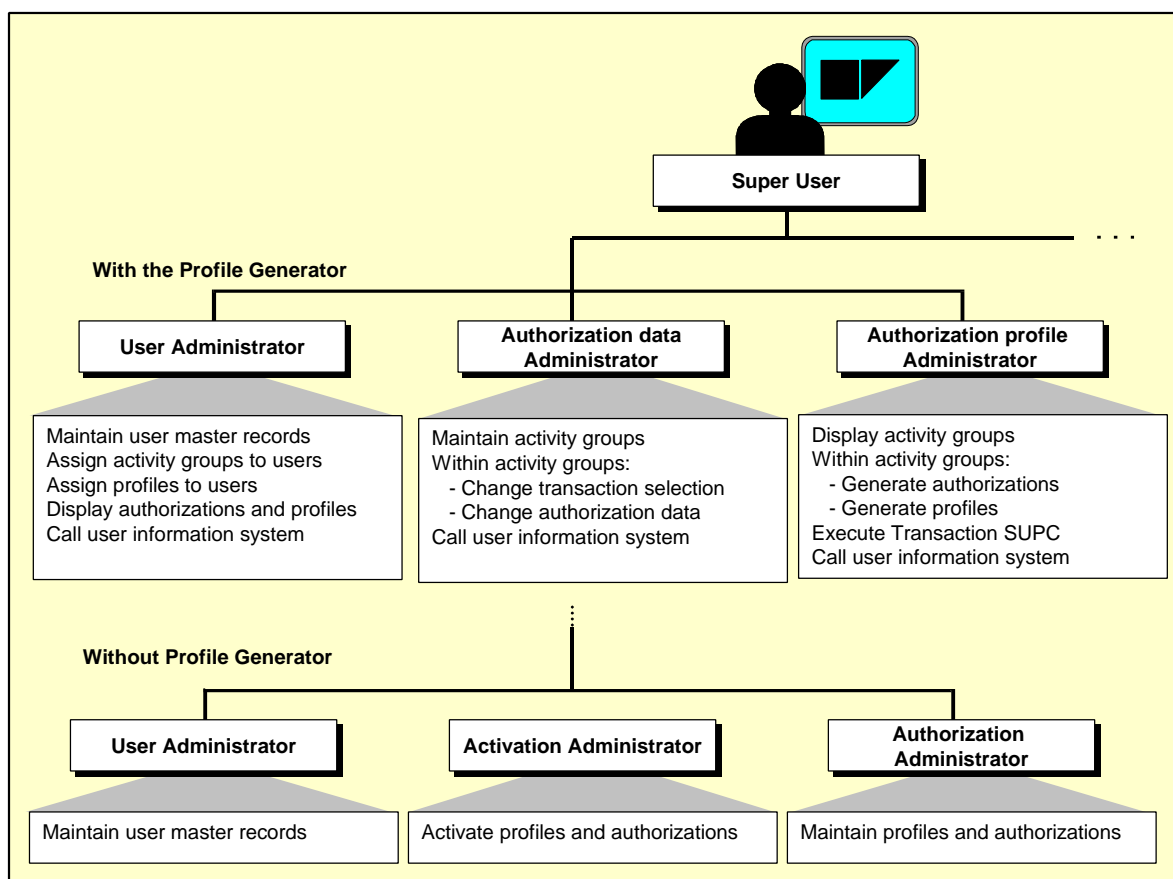


Figure 2-2-2: Organization of User Maintenance Tasks

 **Note**

To avoid confusion due to the slight differences in terminology, we have separated the following discussion between administration with or without the Profile Generator.

Organization Using the Profile Generator

If you use the profile generator, then we recommend that you divide the tasks between the following administrators:

- User administrator
- Authorization data administrator
- Authorization profile administrator

Assign your user and authorization administrators 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. Only administrators with the predefined profile S_A.SYSTEM can maintain users in the group SUPER.

How the Three Administrators Work Together

The **authorization data administrator** creates an activity group, chooses transactions and maintains the authorization data. Not having the appropriate authorization to generate the profile, he or she merely saves the profile.

The **authorization profile administrator** approves the data and generates the authorization profile(s).

The **user administrator** assigns the activity group to the users and adds the authorization profiles to the user master records.

Table 2-2-1 shows the tasks that you should assign to each administrator, those tasks that you should not assign, and the pre-defined templates that we provide for these tasks.

Table 2-2-1 : Organization of the User Administrators when using the Profile Generator

Permitted Tasks	Non-Permitted Tasks	Pre-defined Template
<u>User administrator</u>		SAP_ADM_US
<ul style="list-style-type: none"> • Maintain user master records • Assign activity groups to users • Assign profiles to users • Display authorizations and profiles • Use the user information system (Transaction SUIM) 	<ul style="list-style-type: none"> • Display or change activity group data • Change or generate profiles 	
<u>Authorization data administrator</u>		SAP_ADM_AU
<ul style="list-style-type: none"> • Maintain activity group data • Change authorization data in activity groups • Use the user information system (Transaction SUIM) 	<ul style="list-style-type: none"> • Change users • Generate profiles 	

Table 2-2-1 : Continued

Permitted Tasks	Non-Permitted Tasks	Pre-defined Template
<u>Authorization profile administrator</u>		SAP_ADM_PR
<ul style="list-style-type: none"> • Display activity groups and their data • Generate authorizations and authorization profiles based on existing activity groups • Examine Activity Groups for Existence of Authorization Profiles (Transaction SUPC) • Use the user information system (Transaction SUIM) 	<ul style="list-style-type: none"> • Change users • Change activity group data • Generate authorization profiles containing authorization objects beginning with S_USER (S_USER_AUT, S_USER_GRP, S_USER_PRO) 	

Organization without the Profile Generator

If you maintain your profiles manually, then we recommend that you divide the tasks between the following administrators:

- User administrator
- Authorization administrator
- Activation administrator

Assign your user and authorization administrators 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. Only administrators with the predefined profile S_A.SYSTEM can maintain users in the group SUPER.

How the Three Administrators Work Together

The **user administrator** creates and maintains the user master records.

The **authorization administrator** creates and maintains profiles and authorizations.

The **activation administrator** activates the profiles and authorizations.

We indicate in the following those authorization objects that you should assign to each administrator, as well as those authorizations that you should reserve for the super user.

Table 2-2-2 : Organization of the User Administrators When Maintaining Profiles Manually

Object	Fields	Values
<u>User administrator</u>		
<i>User Groups (S_USER_GRP)</i>	<i>User group</i>	Name(s) of permissible user groups
	<i>Administrator actions</i>	01 : Create user master records 02 : Change user master records 03 : Display user records 06 : Delete user master records
<i>Authorization Profile (S_USER_PRO)</i>	<i>Profile name</i>	Name(s) of permissible profiles
	<i>Administrator actions</i>	22 : Display profiles and enter them in user master records
<u>Activation administrator</u>		
<i>Authorization Profile (S_USER_PRO)</i>	<i>Profile name</i>	Name(s) of permissible profiles
	<i>Administrator actions</i>	06 : Delete profiles 07 : Activate profiles
<i>Authorizations (S_USER_AUT)</i>	<i>Object name</i>	Name(s) of permissible objects
	<i>Authorization name</i>	Name(s) of permissible authorizations
	<i>Administrator actions</i>	06 : Delete authorizations 07 : Activate authorizations
<u>Authorization administrator</u>		
<i>Authorization Profile (S_USER_PRO)</i>	<i>Profile name</i>	Name(s) of permissible profiles
	<i>Administrator actions</i>	01 : Create profiles 02 : Change profiles 03 : Display profiles 06 : Delete profiles 08 : Display change documents for profiles
<i>Authorizations (S_USER_AUT)</i>	<i>Object name</i>	Name(s) of permissible objects
	<i>Authorization name</i>	Name(s) of permissible authorizations
	<i>Administrator actions</i>	01 : Create authorizations 02 : Change authorizations 03 : Display authorizations 06 : Delete authorizations 08 : Display change documents for authorizations

Super User

Reserve the following *User Groups* authorizations for the super user:

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

Authority Checks

When a user wants to execute an action, he or she must have the corresponding authorizations needed to perform the action. To enforce this principle, users are susceptible to **authority checks** when they attempt to execute a transaction. The following methods of enforcing authority checks are available in R/3:

- **R/3 Start Transaction Authorization**

This method is available as of R/3 Release 3.0E. Every time a user calls a transaction, the system performs an authority check against the object S_TCODE. The user must have an authorization of this object type with the value <transaction> in his or her authorization profile to be able to start the designated transaction.

This applies not only to SAP transactions, but also to transactions that you define yourself (in Transaction SE93).

R/3 performs authority checks at the start of every transaction called over the menu or command line. Any transactions that are indirectly called are not included in this authority check. For more detailed transactions, which call other transactions, there are additional authority checks. (For more information on S_TCODE, see OSS Note 67766 [C.26]).

- **Additional Authorization for a Transaction**

When you create a transaction in SE93, you also have the option to assign an additional authorization to the transaction. This is useful if you can protect a transaction with a single authorization. If this is not the case, then consider other methods to protect the transaction (for example, the AUTHORITY-CHECK at program level).

- **AUTHORITY-CHECK at Program Level**

Use this measure for any transactions that you want to protect at program source level. In this way, you can also protect transactions that are indirectly called by other programs. Here, the programmer must include an ABAP AUTHORITY-CHECK statement in the program's source code. The statement includes the authorization object and required values for each authorization field. A user can only execute the program if he or she satisfies the authority check for this program.

- **Report Classes**

Another method of enforcing authority checks is by assigning reports to authorization classes (use the report RSCSAUTH). For example, you may want to assign all PA* reports to an authorization class belonging to PA (such as PAXxx). A user who wants to run this report must then have the appropriate authorization to run reports in this class. We do not deliver any pre-defined report classes; you need to determine which reports you want to protect in this way.

As of Release 3.0, you can also enter the authorization classes for reports over the maintenance functions for reporting trees. With this method, you have a hierarchical approach when assigning authorizations to the reports. For example, you can assign an authorization class to a reporting node and thereby, all reports attached to this node automatically belong to this class. You also have a more transparent overview of which authorization classes you have assigned to various reports.



Note

These report authorization assignments are overwritten during an upgrade. Therefore, after an upgrade, you need to restore your customer-specific report authorizations. For more information, see OSS Note 7642 [C.4] and the documentation for RSCSAUTH [E.1].

- **Table Classes**

R/3 also protects tables using table classes. This prevents users from accessing tables from general access tools (such as SE16). A user must not only have the authorization to run the tool, but he or she must also have the appropriate authorization to access tables that belong to the corresponding table class. Here, we do deliver pre-defined tables classes. These classes are defined in the Table TDDAT, and the authorization object that is checked is S_TABU_DIS.

Reducing the Scope of Authority Checks in R/3

When you use the profile generator, you have the option of reducing the scope of authority checks (Transaction SU24). As the profile generator generates a profile, it selects all of the authorizations that belong to an activity. These generated profiles are not always complete (especially in older releases of the profile generator) and you must manually add those authorizations that may not have been included. (This occurs mainly due to programs that call other programs, where the sub-program requires additional authorizations.) In such cases, to make the administration tasks with the profile generator somewhat easier, you may want to consider reducing the scope of authority checks.



Example

For example, if a user in PA calls a program that then proceeds to call a HR routine, the user must also have the corresponding HR authorizations. If you have not installed the HR component, then you may not want to have to assign to all of your PA users the additional HR authorizations that they need in order to run their PA reports. In this case, you may want to deactivate the authority checks for HR authorizations in these PA transactions.

Why reduce the scope of authority checks in the R/3 System?

As we mentioned, by reducing the scope of authority checks, you simplify the administration tasks involved with using the profile generator. However, you should be careful when deciding which authority checks to suppress. When you suppress authority checks, you also allow users to perform tasks for which you have not explicitly assigned to the user. You may want to consider reducing the scope of authority checks in the following cases:

- You do not use the authorization object associated with the authority check (as in our example above).
- The authority check against the object S_TCODE nevertheless protects the core transaction. (Note however, that the S_TCODE authority check is still only a very general protection measure. This alone is not a reason to suppress an authority check.)
- You want to avoid having to allow all values for an authorization fields for the authorization object.

Instead of assigning the wildcard value '*', you can suppress authority checks for specific objects in specific transactions. For other transactions, you can apply a standard authority check for the same authorization object.



Caution

When you reduce the scope authority checks, you allow users to perform activities without ensuring that the user has the proper authorizations. This may lead to undesirable effects. Consider the necessity of using this option carefully before suppressing any authority checks.

How can you reduce the scope of authority checks?

You use the Transaction SU24 to set check indicators to exclude certain authorization objects from authority checks. However, before running SU24 you need to have set and activated the system parameter, `auth/no_check_in_some_cases = Y`. You also need to run SU25 which copies the SAP check indicator defaults and field values from table USOBT and USOBX into the customer tables. You can then use SU24 to proof these defaults and then set the check indicators accordingly.

Consider the following when using the Transaction SU24:

- Carefully review the SAP defaults before accepting or changing them.
- Use this option for individual transactions only. Do not use it for bulk changes.
- Regularly monitor the contents of SU24 as part of your administration tasks. Take care of the following points:
 1. Ensure that `auth/no_check_in_some_cases` contains the desired value (Y or N).
 2. If this parameter contains a 'Y' value, then monitor the contents of SU24 carefully to ensure that these entries are set to their proper values.

Additional Information on the R/3 Authorization Concept

For more information, refer to the following documentation:

- [R/3 Online Documentation: BC Users and Authorizations \[A.27\]](#)
- [R/3 Online Documentation: BC Users and Authorizations → Transporting User Master Records, Authorizations and Profiles 0](#)
- [R/3 Online Documentation: BC Change and Transport Organizer \[A.3\] or \[A.25\]](#)
- [SAP Documentation: Authorizations Made Easy Guide \[E.2\]](#)
- [SAP ASAP Implementation Roadmap: Work-package 3.11 Establish Authorization Concept; Phase 3: Realization \[E.8\]](#)
- [IMG: Basis Components → System Administration → Users and Authorizations → Maintain authorizations and profiles using Profile Generator \[B.1\]](#)
- [OSS Note 67766: S_TCODE: Authorization check on start transaction \[C.26\]](#)
- [OSS Note 7642: Authorization protection of ABAP programs \[C.4\]](#)
- [R/3 Report Documentation: RCSCAUTH \[E.1\]](#)

Chapter 2-3 : Network Infrastructure

Your network infrastructure is extremely important in protecting your system. Your network needs to support the communication necessary for your business and your needs, without allowing access to unauthorized access. A well-defined network topology can eliminate many security threats based on software flaws (on both the operating system and application level) or network attacks such as eavesdropping. If users cannot log on to your application or database servers, then there is no way for intruders to compromise the machines and gain access to the R/3 database or files. Additionally, if users are not able to connect into the server LAN, they cannot exploit well-known bugs and security holes in network services on the server machines.

Again, your strategy and your priorities are the most important factor in deciding which level of security is necessary for your network infrastructure. We do offer general recommendations when establishing your network topology, which include using a firewall and the SAProuter to protect your local network. To protect R/3 communications, we also offer Secure Network Communications (SNC). We explain these topics in more detail in the following sections:

- **Network Topology**
- **Network Services**
- **Routers and Packet Filters**
- **The Firewall and SAProuter**
- **Security Concept for a Secure Network**
- **Protection of R/3 Communications with Secure Network Communications (SNC)**
- **Additional Information on Network Security**

Depending on your current situation, you may not be able or willing to implement the described secure network setup. However, we do offer suggestions and recommendations at various security levels. If the plan described here does not fit your needs, contact our consultants, who are also available to assist you in the process of setting up your network securely.

Network topology

R/3 is implemented as a three-tier client-server framework that includes the three levels: database server, application server(s) and front end(s). Depending on the size of your R/3 System, your physical network architecture may or may not reflect this three-tier framework. For example, a small system may not have separate application and database server machines (the work processes run on the same machine as the database). The system may also only have a limited number of front ends in a single subnet connected to the server machine. However, in a large R/3 System, several application servers usually communicate with the database server, as well as a large number of front ends. Therefore, the physical topology of your network can vary from simple to complex.

There are several possibilities to consider when organizing your network topology. The topology can vary from a single LAN segment to multiple IP subnets. We suggest that you at least place your R/3 application servers and your central instance (database server) in a separate subnet as indicated in Figure 2-3-1.

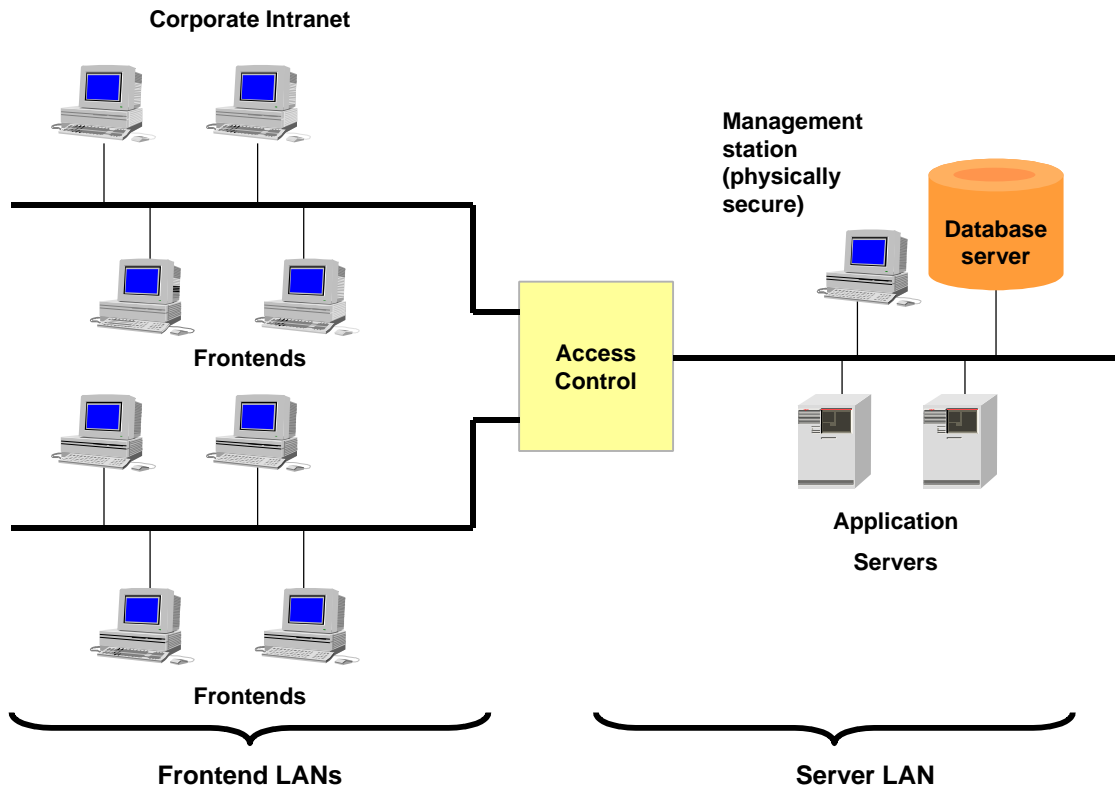


Figure 2-3-1: Separating Frontend LANs from the Server LAN

By placing your R/3 servers in a separate subnet, you increase the access control to your server LAN; thereby increasing the security level of your system.

 **Note**

We discourage placing R/3 servers into any existing sub-net without taking into account the appropriate security considerations.

If you have several systems (or groups of systems) with varying security-levels, then we recommend you create separate server LANs for each 'group' of related systems. Determining these system 'groups' and the security-levels that they require, is a very individual process. We do have consultants available for assistance.

Network Services

The servers are the most vulnerable part of your network infrastructure and you should take special care to protect them from unauthorized access. However, there are a number of network services that allow server access, and you should take appropriate precautions when using these services. In the following sections, we concentrate on those measures that you can take regarding general network services, as well as SAP-specific services. Additional precautions that apply to the operating system itself are included in *Chapter 2-4 : Operating System Protection*.

General Network Services

A typical Unix or NT server machine runs many network services of which only a few are actually needed for running an R/3 System. The names of these services are contained in the file `/etc/services`. This file maps the symbolic name of the service to a specific protocol and numeric port number. (Under Windows NT, the file is located at: `/winnt/system32/drivers/etc/services`.)

You can and should disable most of these network services on the server net (for example, NIS or NFS). Sometimes these services contain known errors that unauthorized users may be able to take advantage of to gain unauthorized access to your network (for example, `sendmail` and the NFS service). In addition, by disabling unused network services, you also decrease the vulnerability of denial-of-service attacks.

For an even higher level of security, we recommend you use static password files and disable insecure access services on the application and database servers.



You can list the "open" ports (ports on which a daemon or service is listening) of a UNIX or Windows NT server with the command `netstat -a`.

See also *Chapter 2-4 : Operating System Protection*.

SAP Network Services

The R/3 System also offers a variety of network services in its own infrastructure. Generally, R/3 programs use the ports in the range 3200-3700. However, a single R/3 System actually only needs to use a limited number of these ports. The ports used are determined by the SAP instance number (denoted by `<nn>` in the following description) or in some cases, by the System ID (denoted by `<sid>`).

You need to consider the following components of the R/3 System when devising your network infrastructure security plan:

- SAPgui and other frontend programs
- Load-balanced connections using the message server port
- External RFC or CPI-C client and server programs
- SAPlpd print daemon

SAPgui and other frontend programs **Port: 32<nn>**

The SAPgui connects to R/3 using the dispatcher process on the application server. The dispatcher uses port 32<nn>. Certain frontend programs can also open RFC connections to the gateway process. The gateway process uses port `sapgw<nn>` (33<nn>).

Message Server Port **Port: `sapms<sid>`**

The message server port (used by SAPlogon and RFC clients for load-balancing) is `sapms<sid>`. The port number is determined in the `services` file and must be resolvable at both the server and the client sides.

External RFC Programs **Port: `sapgw<nn>` (33<nn>)**

External RFC clients connect to the gateway process listening on port `sapgw<nn>` (33<nn>). Note that the gateway port is hard-coded based on the SAP instance number and can not be changed over the `services` file. The gateway process runs on each application server, but it is also possible to use a stand-alone gateway. External RFC server programs can be started in the following ways:

- manually (program registration on the gateway)
- by the gateway process
- by SAPgui

Although the server program is the passive part of the client-server connection, it must first open a connection to the gateway process. It uses the gateway port `sapgw<nn>` for registration as well as for further RFC communication.

For more information, see *Chapter 2-7 : Remote Communications (RFC & CPI-C)*.

SAPlpd **Port: 515 (on the firewall)**

The SAP program SAPlpd handles the R/3 print requests. SAPlpd usually runs on machines in the client network. The SAPlpd service listens at the printer port on the firewall (515). Note that print requests are initiated by the application servers. Therefore, you must configure your routers and packet filters to allow connections from machines in the server LAN to the printer port on client machines.

Summary

Table 2-3-1 shows the ports used by the various R/3 connections:

Table 2-3-1 : Ports used by R/3

Connection	Symbolic port name	Direction of Information Flow ¹⁾	Example: <nn> = 01
SAPgui – Application Server (dispatcher)	sapdp<nn> ²⁾	→ (outside - in)	3201
SAPgui – Message Server (load-balancing)	sapms<sid>	→ (outside - in)	3600 ³⁾
External RFC client – Application Server (gateway)	sapgw<nn> ²⁾	→ (outside - in)	3301
RFC Server – Application Server	sapgw<nn> ²⁾	← (inside - out)	3301
Application Server – SAPIpd	printer	→ (outside - in)	515
anyone – SAProuter	sapdp99 ⁴⁾	→ (outside - in)	3299 ⁴⁾

- 1) *outside - in*: indicates a communication path from the client network to the server network;
inside - out: indicates a communication path from the server network to the client network.
- 2) Connections that use SNC use the ports `sapdp<nn>s` (47<nn>) and `sapgw<nn>s` (48<nn>).
- 3) Defined in `/etc/services`.
- 4) Default - can be configured to any port.



Note

You can reduce the number of required ports by using a SAProuter. When using a SAProuter, only one port (default 3299) must be accessible to clients.

Routers and packet filters

Routers are devices that implement algorithms to route different network protocols according to source and destination addresses. All modern IP-routers also support packet filtering at the IP level.

By specifying a set of rules based on IP addresses and TCP ports, you can select which kinds of network services are accessible over the network. You should configure your router/packet filter to route connections to a defined subset of ports only, based on the services that you require.

The Firewall and SAProuter

The firewall is a system of hardware and software components that define which connections are allowed to pass back and forth between communication partners. It allows only desired connections to pass through and 'blocks' other requests. A common scenario for using a firewall is to control communication between a company's internal Intranet and the external Internet (via proxy).

The SAProuter is a software program developed and provided by SAP to transport R/3 connections across firewalls.

We recommend that you combine the SAProuter and firewall to control access to your network. We describe both of these elements in the following sections.

Firewall

By using a firewall between communication partners (for example, between an Intranet and the Internet), you can allow a defined set of services to pass between the communication partners. For example, you can allow users in your company's Intranet to use Internet services such as mail or http. In this example, you would protect your company Web servers with a firewall system. You can also use a firewall system to shield company Intranets that contain sensitive information.

The components of a firewall system work on different network layers. At the lower layers, routers and packet filters block IP packets based on a predefined set of (simple) rules. Application-level gateways or proxies implement application-dependent protocols such as http or ftp and transfer data between networks (for example, between internal and external networks).

Figure 2-3-2 shows an example firewall scenario. Note that the machines in the so-called "demilitarized zone" are not directly accessible from either the internal or the external networks. The routers/packet filters are configured to allow only connections for specified network services.

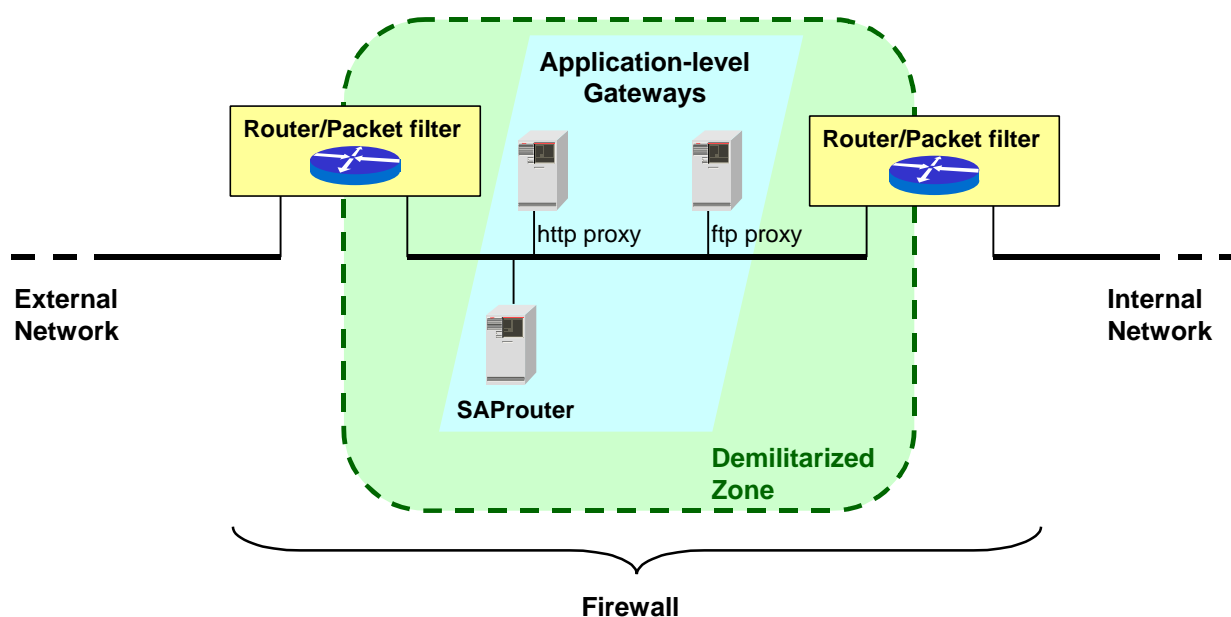


Figure 2-3-2: Firewall

SAProuter

The SAProuter is a software program developed by SAP to transport R/3 connections across firewalls. The SAProuter is a proxy at the NI layer (Network Interface - NI is SAP's abstract network protocol based on TCP/IP). In addition, it implements the logging of connections at various levels of detail.

You can couple multiple SAProuters, making it possible to connect R/3 Systems in networks with identical or private IP addresses.

The SAProuter complements and does not replace the firewall. We recommend that you use the SAProuter and a firewall together. A SAProuter alone does not protect your R/3 network.



Note

If you use the R/3 Online Service System (OSS), you must use a SAProuter.

You can also use the SAProuter to:

- Control and log the connections to your R/3 System, for example, from a SAP service center.
- Set up an indirect connection when programs involved in the connection cannot communicate with each other due to the network configuration.
- Resolve address conflicts when using non-registered IP addresses.
- Improve network security by
 - Protecting your SAProuter from unauthorized external access with a password.
 - Allowing access from particular SAProuters only.
 - Only allowing protected communication from a securely authenticated partner using SNC.
- Increase performance and stability by reducing the R/3 System load within a local area network (LAN) when communicating with a wide area network (WAN).

When using the SAProuter, you only have to open a single port on the firewall for a connection to the port on the machine running the SAProuter. All SAPgui, SAPipd and RFC connections must pass through this one port (3299 per default).

You specify the IP addresses and address patterns that can access your R/3 Systems in the configuration file `saproutab`. You can also have important SAProuter activities logged, such as connection setup and closure.



Example

The following is a sample SAProuter configuration file where the main instance's hostname is `appsrv1_TST_21`:

```
# sample saproutab
# permit connections from 155.152.22 subnet
# to the application servers (appsrv2..appsrv4)
# allow only dispatcher connections
P 155.152.22.* appsrv2 sapdp21
P 155.152.22.* appsrv3 sapdp21
P 155.152.22.* appsrv4 sapdp21
# only admin PC (IP address 155.152.23.3) can access appsrv1
P 155.152.23.3 appsrv1 sapdp21
# allow all access to message server for load-balancing
# for appsrv1
P 155.152.*.* appsrv1 sapmsTST
```

**Note**

You can restrict the ability to administer the SAProuter by one of the following entries:

```
# sample saproustab

# allow only local administrative requests
P localhost localhost 3299

# allow administrative requests from admin PC only
P 155.152.23.3 <SAProuter_host> 3299

# allow administrative requests only with password
P * <SAProuter_host> 3299 <password>
```

**Note**

In addition to the dispatcher port, you also need to open the gateway port `sapgw<nn>` in `saproustab` if you want to allow external RFC connections. (SAPgui uses RFC for certain actions such as non-modal F1 help or SAPKale).

If you use load balancing, then you have to open the port for `sapms<sid>`.

**Note**

For more information on configuring the SAProuter, see OSS Note 30289 [C.9] or the online documentation *BC SAProuter* [A.20].

Security Concept for an R/3 Network

Figure 2-3-3 shows an example R/3 network topology that should be sufficient for most R/3 Systems. The security concept consists of a router/packet filter in conjunction with an accordingly configured SAProuter.

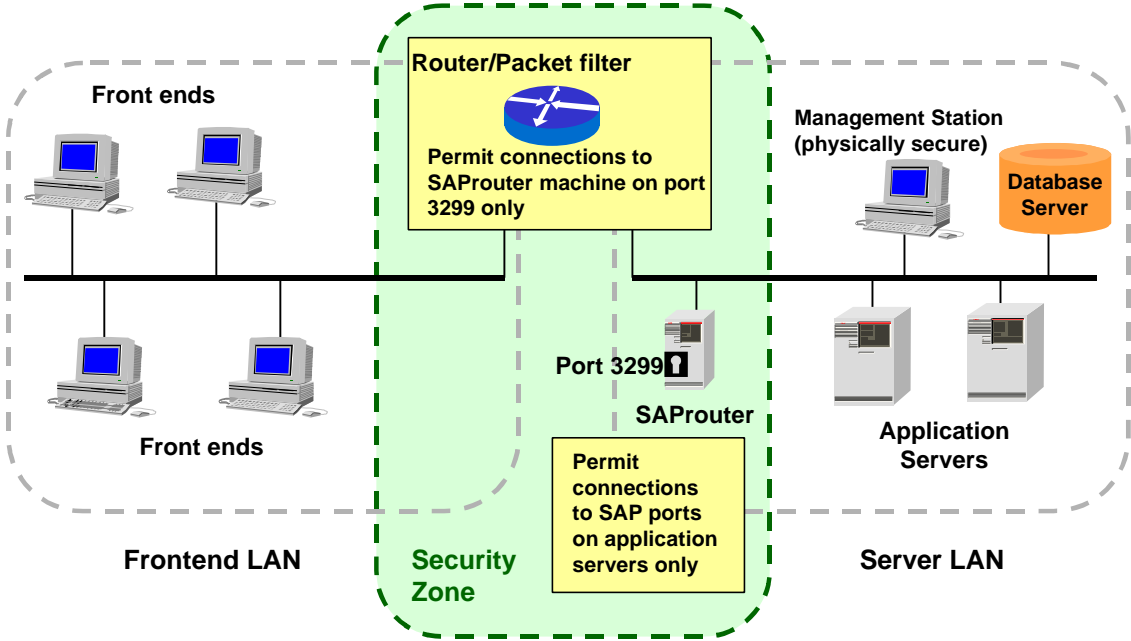


Figure 2-3-3: Recommended R/3 Network Topology

We suggest using this or a similar setup for productive and other security-critical R/3 Systems.

The main security elements of this configuration are the router/packet filter and the machine running the SAProuter proxy. The router/packet filter is configured to allow only TCP connections from machines in the frontend LAN to the port 3299 (the default SAProuter port) on the SAProuter machine. The SAProuter is configured to explicitly allow or deny connections from a defined subset of client machines.

Using this setup, machines in the "open" frontend LAN cannot directly access the application or database servers. All front ends connect to a single port on the machine running the SAProuter software. The SAProuter machine opens a separate connection to one of the application servers. Figure 2-3-4 illustrates this two-way connection.

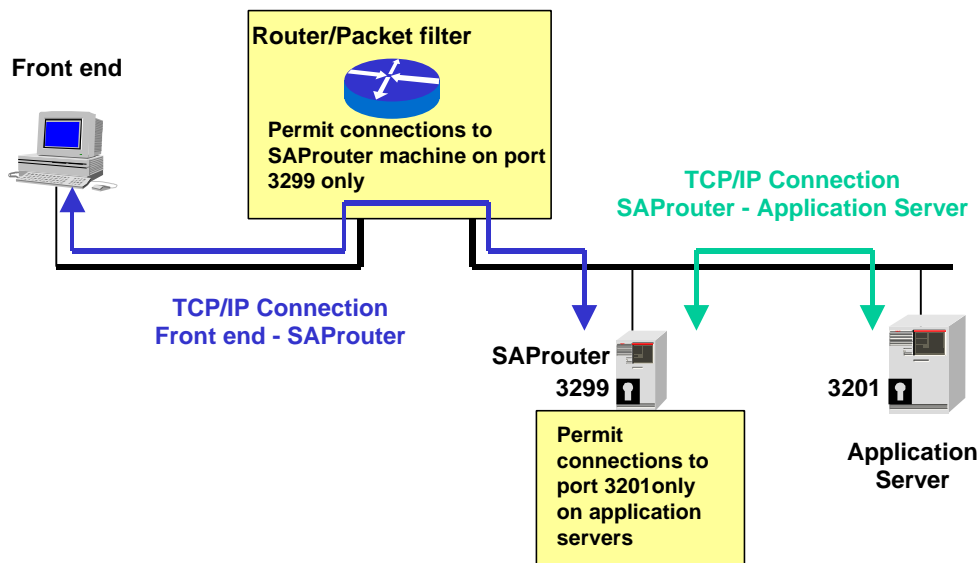


Figure 2-3-4: Two-way Connection Using the SAProuter and a Router/Packet Filter

Secure Network Communications (SNC)

SNC is a software layer in the R/3 architecture that provides an interface to an external security product. With SNC, you can strengthen the security of your R/3 System by implementing additional security functions that R/3 does not directly provide (for example, the use of smart cards for user authentication).

SNC provides security at the application level. This means that a secure connection between the components of an R/3 System (for example, between SAPgui and the R/3 application server) is guaranteed, regardless of the communication link or transport medium (see Figure 2-3-5). You therefore have a secure network connection between two SNC-enabled communication partners.

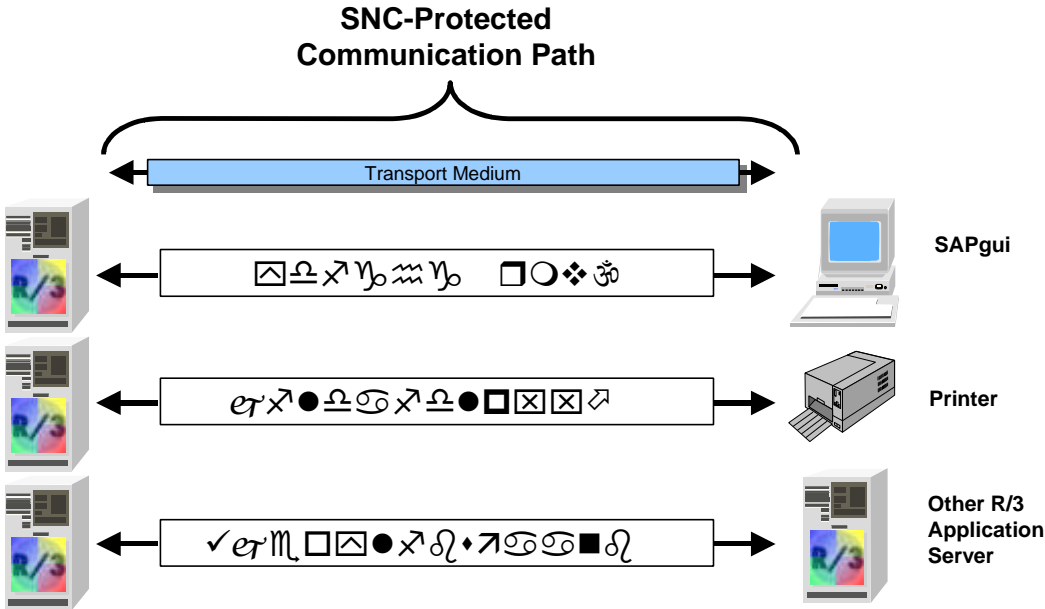


Figure 2-3-5: Application Level Protection Provided by SNC

SNC Protection Levels

You can apply three different levels of protection to SNC protected communication paths:

- **Authentication only**
 Authentication only provides non-disclosing authentication between the communication partners. This is the minimum protection level and always provided when using SNC. (No actual data protection is provided!)
- **Integrity Protection**
 Integrity protection detects any changes in the data which may have occurred between the originator and the receiver.
- **Privacy Protection**
 Privacy protection encrypts the messages being transferred to make eavesdropping useless. This is the maximum level of protection provided by SNC. Integrity protection (as well as authentication) is also included at this level.

R/3 Communication Paths that can be protected with SNC

For Releases as of 3.1G, you can apply SNC protection to the connections between the R/3 application server and SAPgui or between R/3 and SAPlpd. As of 4.0, you can also apply SNC protection to RFC and CPI-C connections. There are a few exceptions, for example, neither the Session Manager nor SAP Shortcuts support SNC protection at this time.

Table 2-3-2 shows the communication paths in R/3 that you can protect with SNC:

Table 2-3-2 : SNC-Protected Communication Paths

From:	To:	Using/Over:	SNC Protection as of Version:
SAPgui	→ R/3		3.1G
R/3	→ SAPlpd		3.1G
ext. Prog.	→ R/3	RFC / CPIC	4.0A
R/3	→ R/3	RFC / CPIC	4.0A
R/3	→ ext. RFC Program	RFC	4.0A
R/3	→ ext. CPIC Program	CPIC	4.0A
SAProuter	→ SAProuter		SAProuter Version 30

You cannot apply SNC protection to the communication path between your R/3 application servers and your database. Therefore, we recommend you keep your application and database servers in a secured LAN that you protect with a firewall in combination with a SAProuter (see Figure 2-3-6).

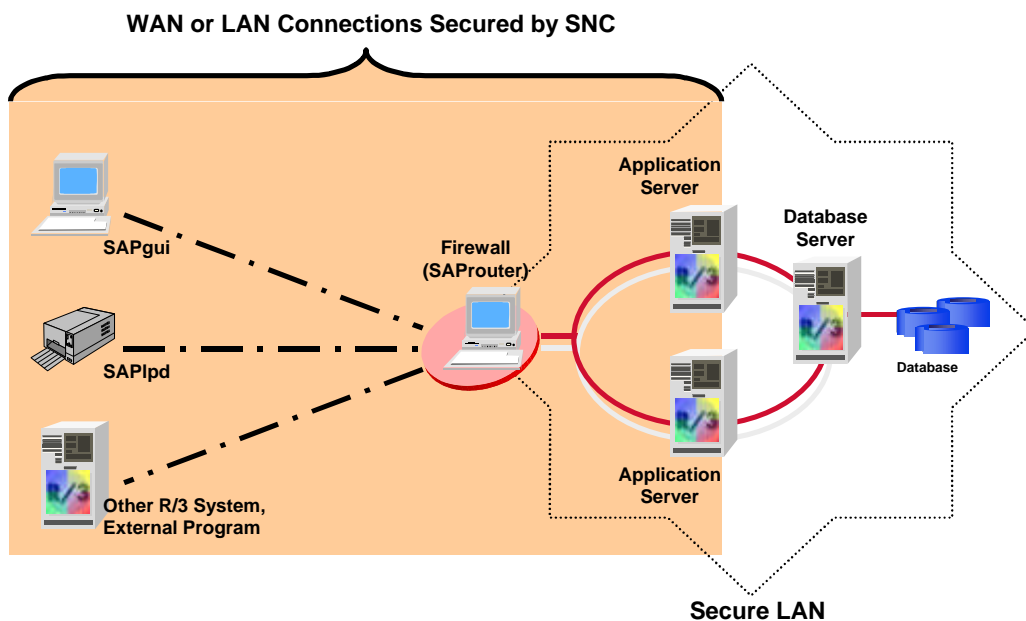


Figure 2-3-6: Network Area Protected with SNC

You can also use SNC between two SAProuters to build a secure tunnel between networks (see Figure 2-3-7). You can use this infrastructure to secure connections if you have components belonging to a release earlier than Release 3.1G.

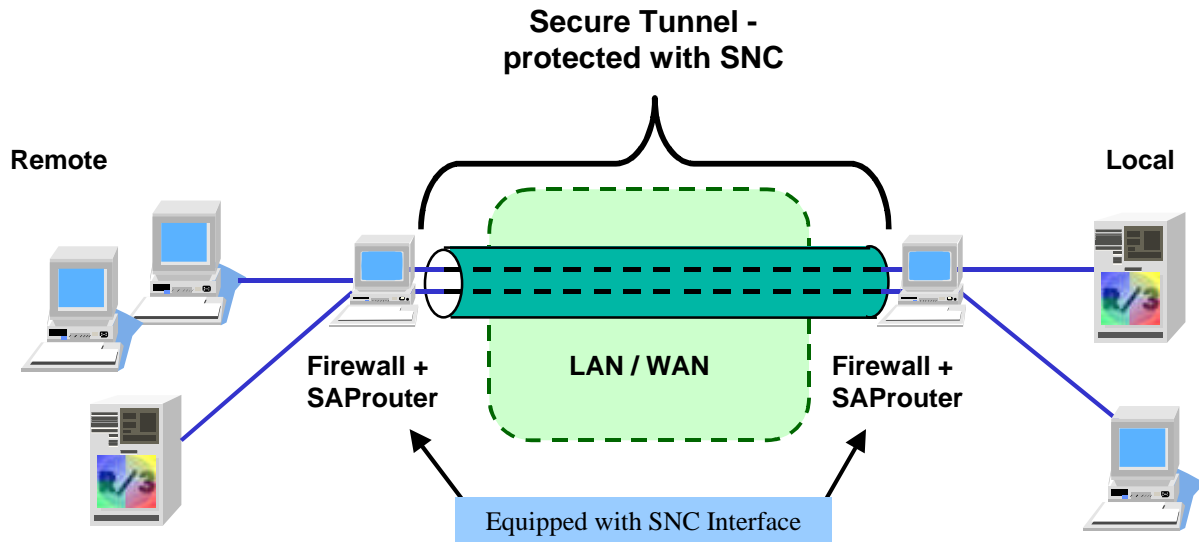


Figure 2-3-7: SNC Protection between SAProuters

External Security Products

R/3 integrates the SNC functions in the system components (for example, the R/3 Kernel, SAPgui, or RFC Library) as a layer between the R/3 kernel layer and the library provided by the external security product. The SNC layer communicates with the external library over the GSS-API V2 (Generic Security Services Application Programming Interface Version 2). This standard was developed with SAP participation by the IETF (Internet Engineering Task Force).

The external product is not included in the SAP R/3 Software. You must purchase the product from the appropriate vendor. The product must meet the following requirements:

- The product must provide the entire functionality of the IETF-defined GSS-API V2 interface.
- The product must provide Single Sign-On.
- The functions must be dynamically loadable.
- The product must be available on platforms supported by SAP.
- The product must be certified by SAP for interoperability with SAP R/3.

Note

For more details on the availability of external security products, see OSS Note 66687 [C.25].

Additional Information on Network Security

For more information, refer to the following documentation:

- [R/3 Online Documentation: BC SAProuter](#) [A.20]
- [R/3 Online Documentation: SAP Network Security](#) [A.35]
- [SAP Documentation: The SNC User's Guide](#) [E.6]
- [SAP Documentation: Secure Network Communications and Secure Store & Forward Mechanisms with R/3](#), Material Number 50014335 [E.7]
- [OSS Note 30289](#): SAProuter documentation [C.9]
- [OSS Note 66687](#): Network security products SECUDE and Kerberos [C.25]

Chapter 2-4 : Operating System Protection

Because the R/3 System manages certain information at the operating system level, the security of your R/3 System is also dependent on the security of the operating system under which it operates. In general, we cannot guarantee the security of the operating system; however, we do offer recommendations for increasing R/3 security under UNIX or Windows NT. These recommendations are included in the following sections:

- **R/3 Security under UNIX**
- **R/3 Security under Windows NT**
- **Logical Operating System Commands in R/3**

R/3 Security under UNIX

In this section, we cover the following aspects pertaining to security under the UNIX operating system. When appropriate, we include our recommendations and any measures that you need to take.

- **Protecting Specific UNIX Properties, Files and Services**
- **Protected R/3 Directory Structures under UNIX**
- **Setting Access Privileges for R/3 under UNIX**
- **Additional Information on UNIX Security**

Protecting Specific UNIX Properties, Files and Services

You need to take precautions when using the following Unix properties, files or services:

- SUID/SGID
- `passwd` (password file)
- Yellow Pages (NIS)
- Network File System (NFS)
- BSD Remote Services for `rlogin` and `remsh/rsh`

SUID/SGID

The SUID/SGID property gives programs extended privileges that exceed the privileges possessed by the caller.

Every UNIX system contains a large number of these programs for administrative purposes. These programs may contain known errors that unauthorized users may be able to take advantage of in order to assign new access rights to themselves.

For example, the `SENDMAIL` program is such a SUID program. We suggest that you only use versions of `SENDMAIL` (or similar SUID programs) in which known errors have been corrected.

passwd (Password File)

Although UNIX hashes passwords before storing them in this file, a user could use a dictionary-attack program to discover password information in this file.

You can improve security by using a shadow password file that allows only the user `root` to access the password information.

Yellow Pages (NIS)

You can use the NIS service (Network Information System) to manage user data and passwords centrally. It allows every UNIX machine in a local area network to read the password file using the `ypcat passwd` command, including shadow password files.

You should be aware of the fact that on some platforms an intruder could replace the password file with a manipulated password file using the NIS transmission protocol.

Before using NIS, consider the necessity of the service. There are usually alternatives available and for security reasons, we recommend that you avoid using this service.

Network File System (NFS)

The NFS service is frequently used in the R/3 environment to make transport and work directories accessible over the network.

The authentication procedure is based on network addresses. You should be aware that it is possible for users to gain unauthorized access over NFS by using counterfeit network addresses (IP Spoofing).

Therefore, be cautious when assigning write authorization for NFS paths. Avoid distributing the HOME directories of users across NFS. Export to certain clients only.

Note that in those areas where NFS is often used (for example, for establishing a global directory for application servers or in the Transport Management System), there are often alternative solutions. Again, we recommend that you consider other alternatives before deciding to use this service.

BSD Remote Services for *rlogin* and *remsh/rsh*

These services permit remote access to UNIX machines. At logon, the files `/etc/host.equiv` and `$HOME/.rhosts` are checked. If either of these files contains the hostname or the IP address of the connection originator or a wildcard character (+), then the user can log on without having to supply a password.

You should be aware that the UNIX services for `rlogin` and `remsh/rsh` are especially dangerous in regard to security. If possible, deactivate these services in the `inetd.conf` file.

Summary

To summarize the precautions that you should take, especially pertaining to NIS, NFS and the BSD remote services, adhere to the following guidelines:

- If you do use these services, then use them only within a secure LAN.
- Do not export directories that contain SAP data to arbitrary recipients using NFS. Export to "trustworthy" systems only.
- Protect the following users: `root`, `<SID>adm` and `<DB><SID>`. These should be the only users that exist on your application servers and your main instance. After installation, you should lock `<DB><SID>` on your application servers.
- For critical users, empty the `.rhosts` files and assign access rights equal to 000.
- Either delete the file `/etc/hosts.equiv` or make sure that it is empty.
- Keep your operating system up to date regarding security-related patches that are released by your OS vendor.

Protected R/3 Directory Structures under UNIX

For security reasons, the R/3 System together with the user data is stored in a special directory structure in the operating system and is protected with defined access authorizations.

Figure 2-4-1 shows how the R/3 directory structure is established in the UNIX file system:

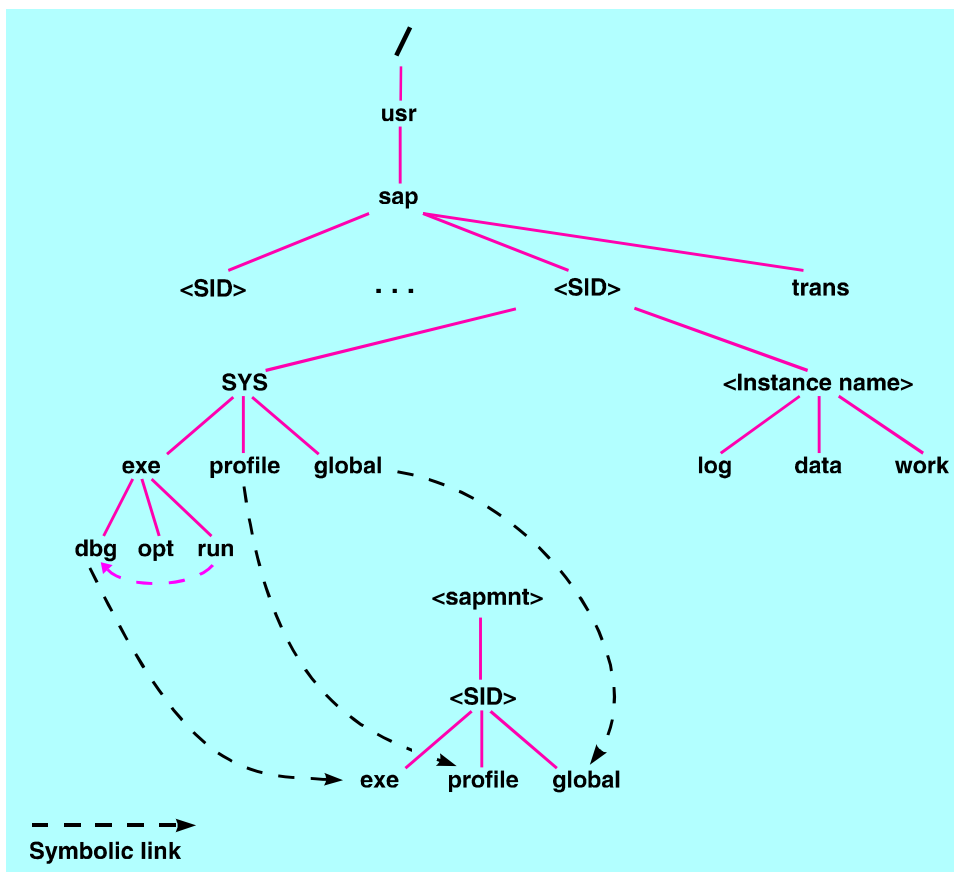


Figure 2-4-1: R/3 Directory Structure under UNIX

Setting Access Privileges for R/3 Directories under UNIX

We recommend that you restrict the UNIX file and directory access privileges as shown in Table 2-4-1:



Note

As of Release 3.0D, the access rights shown in Table 2-4-1 are automatically set in the installation procedures.

Table 2-4-1 : Setting Access Privileges for R/3 Directories and Files under Unix

SAP Directory or File(s)	Access Privilege in Octal Form	Owner	Group
/sapmnt/<SID>/exe	775	<sid>adm	sapsys
/sapmnt/<SID>/exe/saposcol	4755	root	sapsys
/sapmnt/<SID>/global	700	<sid>adm	sapsys
/sapmnt/<SID>/profile	755	<sid>adm	sapsys
/usr/sap/<SID>	751	<sid>adm	sapsys
/usr/sap/<SID>/<Instance ID>	755	<sid>adm	sapsys
/usr/sap/<SID>/<Instance ID>/*	750	<sid>adm	sapsys
/usr/sap/<SID>/SYS	755	<sid>adm	sapsys
/usr/sap/<SID>/SYS/*	755	<sid>adm	sapsys
/usr/sap/trans	775	<sid>adm	sapsys
/usr/sap/trans/*	770	<sid>adm	sapsys
/usr/sap/trans/.sapconf	775	<sid>adm	sapsys
<home directory of <sid>adm>	700	<sid>adm	sapsys
<home directory of <sid>adm>/*	700	<sid>adm	sapsys

UMASK

Newly created files have rights determined by UMASK definitions. An UMASK is a four digit octal number that specifies those access rights that are **not** to be given to newly created files. You can define UMASKS in any of several files, to include:

- .login
- .cshrc
- .profile
- /etc/profile

As with UNIX access rights, the corresponding octal positions represent user, group, and world access, and the value of the digit represents which access privileges should be removed (remove none = 0, remove write = 2, remove all = 7).

You can use the UMASK to automatically restrict permissions for newly created files. For example, by defining a UMASK of 0027, you specify that all newly created files have the access rights 750.

Additional Information for UNIX

For more information on UNIX security (and more), see the following Internet links:

- <http://www.cert.org> [D.1]
- <http://www.itd.nrl.navy.mil/ITD/5540/ieee/cipher/> [D.5]

R/3 Security under Windows NT

Windows NT manages administration tasks and provides access protection over its domain concept. A domain is a group of several computers that share a common user and security database. Within each domain, you define and administer your users and groups.

An R/3 System that runs under Windows NT also uses the domain concept to manage administration tasks and to protect the servers from unauthorized access. In the following sections, we explain how R/3 uses this concept to protect its resources, as well as any measures that you yourself should take. The sections include:

- **Windows NT Users and Groups in an R/3 Environment**
- **R/3 in the Windows NT Domain Concept**
- **Protecting the R/3 Resources**
- **Additional Information for Windows NT Security**

Windows NT Users and Groups in an R/3 Environment

This section introduces the Windows NT technology for administering the users and user groups needed to run an R/3 System. In order to simplify your administrative tasks, we suggest you add all Windows NT users to user groups that are granted the appropriate rights at the operating system level. In this section, you will find the necessary group and user information to operate your R/3 System under Windows NT securely.

Groups

Windows NT supports two levels of groups:

- **Global Groups**

You create global groups at the domain level. Global groups are known to all servers within the domain.

- **Local Groups**

You create local groups on a single server. They are only known on that server.

Exception: If you define a local group of users on **one** domain controller (PDC or BDC), the group is known on **all** domain controllers within the domain.

Global Groups

Global user groups are valid within an NT domain, not only on one server. Therefore, we recommend that you bundle the domain users into different activity groups, depending on their tasks. The domain administrator may export these activity groups to other domains, so the respective user can access all resources needed to administer the R/3 System.



Example

Examples of global groups include:

- `SAPadmin` contains all of the R/3 System administrators
- `SAPservices` contains all of the R/3 System programs
- `SAPusers` contains all of the R/3 application users
- `Domain Admins` contains all NT domain administrators

Although you may choose the name of the group as you wish, the standard global group for R/3 administrators is defined as `SAP_<SID>_GlobalAdmin` according to the SAP R/3 Installation Guide on Windows NT.

Local Groups

Local user groups (as well as local users) exist locally on one server. During installation, user rights are assigned to local users instead of groups. (For example, the user `<SID>ADM` receives the user right *Log on as a service*.) However, to simplify user administration, we recommend you assign server resources to local groups instead of single users. You can then assign the appropriate global users and groups to the local group. Thereby, you have better control over who belongs to which group, and what their tasks are.



Example

Create the local group `NT Administrators`. Add the local users who should belong to the group (for example, any local NT administrators `<Local_NT_Admin>`), and the global users who should belong (for example, `<Domain>\Domain Admins`) to the group.



Note

Local user groups increase the security and validity scope of user rights. However, be careful when using domain controllers. A single local user right defined on a domain controller is valid on all domain controllers. We therefore do not recommend installing R/3 on a domain controller!

Although you may choose the name of the group as you wish, the standard local group for R/3 administrators is defined as `SAP_<SID>_LocalAdmin` according to the SAP R/3 Installation Guide on Windows NT.

The following relationships are possible between users, local groups and global groups:

- A user can be a member of both a local group and a global group.
- A global group can be included in a local group. You may also export a global group to another Windows NT domain.

If several users need the same rights for a certain set of resources, you can create a group. It is then no longer necessary to assign each individual user his or her rights to each of the files. Instead, you assign the rights to a group. Thereby, all of the users in the group automatically receive the rights as assigned to the group. The same applies to the users in a global group that is itself the member of a local group.

Users

Table 2-4-2 shows the users that exist or are needed in an R/3 System on Windows NT. The appropriate precautions that you should take are included below.

Table 2-4-2 : Users and their Functions under Windows NT

User type	User	Function and Rights
Windows NT users ¹⁾	Administrator	The local superuser who has unlimited access to all local resources.
	Guest	A local guest account who has guest access to all local resources.
R/3 users	<SID>ADM	The R/3 administrator who has unlimited access to all local R/3-related resources.
	SAPservice<SID>	A special user who runs the R/3-related Windows NT services.
Database users ²⁾	<DBservice>	One or more special users who run database-specific Windows NT services or access the database resources with utility programs.
	<DBuser>	Some databases also need certain users at the operating system level.

1) NT automatically creates the users Administrator and Guest during installation. They are not needed for R/3 operations.

2) The database users included in the table are typical users. However, the exact users that you need depend on the database you use.

Windows NT superuser Administrator

The Windows NT built-in superuser Administrator has unlimited access to all Windows NT resources. For example, he or she can:

- Create, manage, and become the owner of all data files, hard disks, and file shares.
- Create and manage local users and their rights.
- Create and manage peripherals, kernel services, and user services.

Chapter 2 : The R/3 Security Toolbox

To protect this user from unauthorized access, you should disable it. Change the user name and hide its password. Create other users for administrative tasks and limit their rights to those tasks for which they are used (for example, user administrators, backup operators or server operators).

<SID>ADM

<SID>ADM is the Windows NT superuser for R/3 administration. This user is created during the installation process, normally as a domain user for the R/3 System. This user can therefore logon to all Windows NT machines in the domain. <SID>ADM also needs full access to all R/3 instance-specific resources such as files, shares, peripheral devices (for example, tape drives or printers), and network resources (for example, the SAProuter service).

**Note**

During installation or upgrade, you need to assign <SID>ADM to the Domain Administrators group. In this status, <SID>ADM has the same rights as the Administrator in a normal Windows NT environment.

To protect this user from unauthorized access, take the following precautions:

- Cancel group membership in the groups Administrators or Domain Administrators.
- Change its password regularly.
- Restrict its access rights to R/3 instance-specific resources only.

Although <SID>ADM may access R/3 files, a different user runs the R/3 System itself, namely SAPservice<SID>.

SAPservice<SID>

SAPservice<SID> is also created during installation. It is usually created as a domain user to run the R/3 System and to manage database resources. This user may logon locally on all Windows NT machines in the domain.

Since R/3 must run even if no user is logged onto the local Windows NT machine, the R/3 System runs as a Windows NT Service. Therefore, during installation, the user SAPservice<SID> receives the right to *Log on as a service* on the local machine.

SAPservice<SID> also administers the R/3 System and database resources within the Computing Center Management System (CCMS). Therefore, it needs full access to all R/3 instance-specific and database-specific resources such as files, shares, peripheral devices, and network resources.

**Note**

It is rather difficult to change this user's password. To change an NT service's password, you need to stop the service, edit it, and restart it. Therefore, to change this user's password, you need to stop the R/3 System.

To protect SAPservice<SID>, take the following precautions:

- Cancel the user right *Log on locally*.
- Restrict its access rights to R/3 instance-specific and database-specific resources only.

- Prevent this special service user from logging on to the system interactively. This prevents misuse by users who try to access it from the presentation servers. You then do not have to set an expiration date for the password and you can disable the setting `change passwd at logon`.

<DBservice> and <DBuser>

As with the R/3 System itself, the database must also run even if no user is logged on to the Windows NT machine. Therefore, the database must also run as a service. During the database installation process, the user <DBservice> receives the right to *Log on as a service* on the local machine.

In addition, the various databases require various operating system users for their administration. Table 2-4-3 shows the various operating system users required:

Table 2-4-3 : Database Users

Database	Operating System User	Function
ORACLE	SYSTEM	runs the R/3 System ¹⁾
INFORMIX	<sid>adm	runs the R/3 System
	informix	database administrator
	sapr3	database user
ADABAS	<sid>adm	runs the R/3 System
DB2/CS	SYSTEM	runs the R/3 System

1) SQL*Net V2 may be run by the user `SAPservice<SID>`.



Note

You should be aware that the user `SYSTEM` is a virtual user with no password. (You cannot logon as user `SYSTEM`.) However, this user has complete access to the local Windows NT system.



Note

For descriptions on how to change these users' passwords, refer to the appropriate sections in *Chapter 2-5 : Database Access Protection*.

R/3 in the Windows NT Domain Concept

As previously mentioned, we recommend that you create two separate domains for your R/3 System. Figure 2-4-2 shows the basic idea behind the two-domain concept for R/3 under Windows NT. In the figure, we have called the two domains `MASTER` and `SAP`.

- In the `MASTER` domain, you set up your domain users (to include your R/3 users) and your `MASTER` domain administrator.
- In the `SAP` domain, you set up your R/3 application and database servers, any R/3 or database services, your R/3 and NT administrators, and your `SAP` domain administrator.

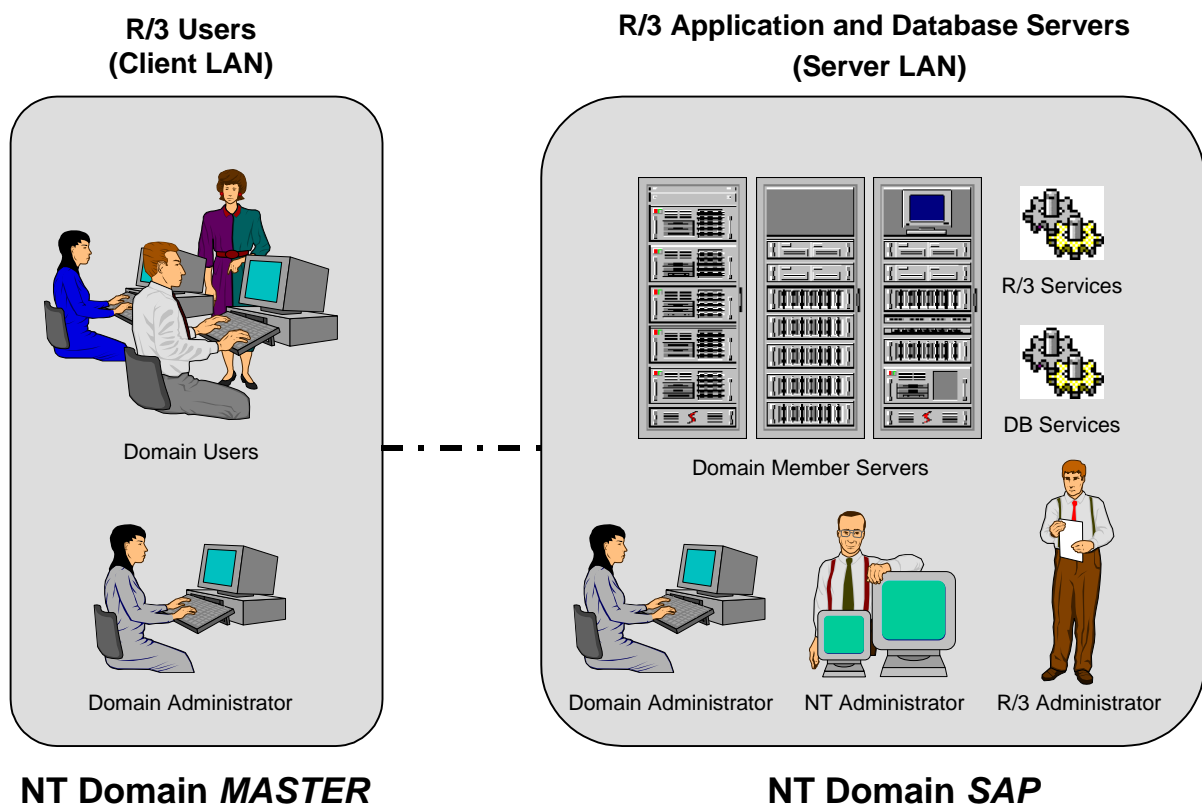


Figure 2-4-2: NT Domains `MASTER` and `SAP`

Defining Access Rights

With the master domain model, you can define your user rights as follows (see Figure 2-4-3):

1. Define your users within a company-wide user database in the NT domain `MASTER`.
2. Export the users of the master domain to other domains (resource domains) using global groups.
3. Within the resource domains, assign the imported global user groups to the appropriate local user groups.
4. Assign the corresponding local user rights to the local user groups.

We also recommend that you install your R/3 System in a separate NT domain (*SAP* in Figure 2-4-2). With this set-up, you can give your system administrator all those rights that he or she needs to maintain the R/3 without interfering with other Windows NT resource domains.

Note that the global groups have unrestricted access to the resources in the corresponding domains, whereas the users and groups in the *SAP* domain have restricted access to R/3 and database-specific resources only.

Note

A sample configuration of access rights is included in the appendix of every R/3 installation guide for Windows NT (as of Release 3.0F).

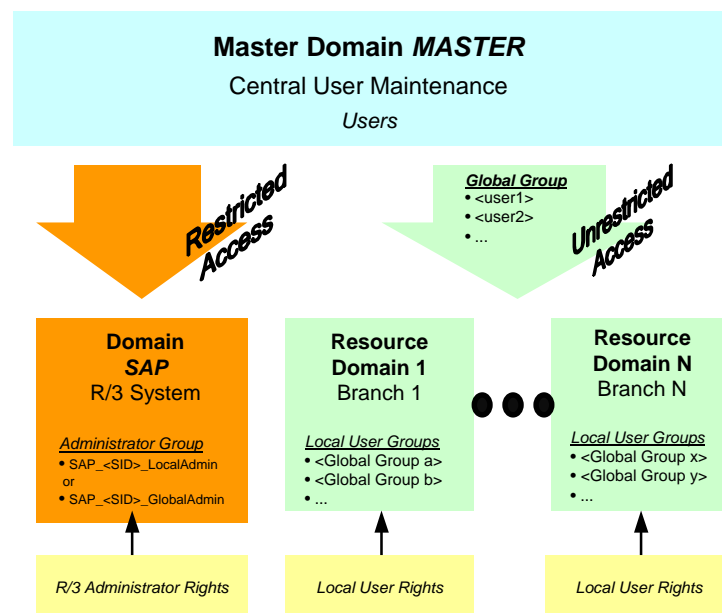


Figure 2-4-3: Windows NT and R/3 Administration Users and Groups

Note

Trusted Domain Concept:

If you set your R/3 System up in a trusted domain concept, all users defined in the master domain may also log on in the R/3 domain with their respective user rights. Therefore, a trusted domain concept does raise security concerns.

However, the standard R/3 System does **not** require a trusted domain concept between the *SAP* domain and other Windows NT domains.

For security reasons, we do **not** recommend establishing a trusted domain concept for R/3 under Windows NT. Consider alternatives for transferring information between domains!

If, however, you do need to use Windows NT specific services from a neighboring domain (for example, network printing with the Print Manager or file transfer batches with operating system commands such as `xcopy` or `move`), Windows NT forces you to set up a trusted relationship. In this case, establish the trusted relationship preferably in **one** direction so that only the *SAP* domain trusts the *MASTER* domain and not vice versa.

Protecting the R/3 Resources

In R/3, the resources you need to protect are as follows:

- All data relevant to R/3 (under \usr\sap\...)
- Named pipes, which are used for R/3 System administration
- Shared memory in the R/3 System
- Dynamically created files (Files Created by ABAP)
- All the database files that R/3 uses

We describe how to protect each of the resources below. We also include a description on how to protect resources for an installation that consists of several R/3 Systems.

All Data Relevant to R/3

The following points apply to the Windows NT domain concept and the installation of your R/3 System:

- Regardless of whether the R/3 System is installed centrally or as a distributed system, you should set up one domain that contains the R/3 application and database servers (domain SAP in the above examples).
- We strongly recommend that you set up all your R/3 servers in one domain. For short-term test installations or demonstration purposes only, you may install a central R/3 System that is not located in a domain. However, we recommend this set-up for limited use only. It is difficult to introduce the domain concept to a system that is already in use.
- In a central installation on a server in a domain, all R/3 administrators are members of the local group SAP_<SID>_LocalAdmin.
- In a distributed installation with several server machines in the domain, a global group is set up for the R/3 System (SAP_<SID>_GlobalAdmin). This global group itself is a member of the server's local groups and contains the R/3 administrators. This also simplifies the administration in the client/server environment, since new users that need R/3 administration rights only need to become members of the global group.
- The R/3 administrator <SID>ADM, who performs the R/3 System installation, has to be a member of the NT administration group during the installation. Once the installation is complete, this is no longer necessary. You should cancel its membership in this group.
- Windows NT uses access control lists to provide access protection for files and directories. To protect R/3 files and directories, you need to make entries in the access control lists at the file level. The files are located in the path: \usr\sap\<sid>\....

Take the following precautions when introducing the Windows NT user concept:

- Create all R/3-relevant users as domain users, and not as local users.
- Create global user groups on the domain controller. Set up the domain users as members of these global groups.
- Create local user groups on every R/3 server. Set up the global groups as members of the local groups.
- Assign access rights or resources to local groups only. This simplifies the server administration tasks. (This strategy is equally applicable to central installations and to local installations.)
- Create at least two users for the system administration:
 - <SID>ADM
 - SAPService<SID>
- Take the precautions for each user as previously described in the section *Windows NT Users and Groups in an R/3 Environment*.

Named Pipes and Shared Memory

Named pipes are required for starting and stopping the R/3 System. They inherit the access rights of the executable file `sapntstartb.exe`. The SAPgui application `sservermgr.exe` is used at the front end to send the start/stop messages to the named pipe, where `sapntstartb.exe` is waiting for these messages.

As long as `sapntstartb.exe` has been assigned the appropriate access protection, only authorized users (belonging to the local group `SAP_<SID>_LocalAdmin`) can use `sservermgr.exe` to start or stop the R/3 System.

The shared memory is used by the R/3 dispatcher and the work processes for certain activities, such as exchanging administration information. Because R/3 creates the entire shared memory, the user who starts the R/3 System is allocated exclusive access rights for this shared memory.

In order to avoid access conflicts during operation of the R/3 System with certain internal tools (`dpmon.exe`, `gwmon.exe`), you must ensure that the same user who started the R/3 System starts these tools.

Dynamically Created Files (Files Created by ABAP)

Because R/3 uses ANSI stream file I/O, a file created by ABAP inherits access rights from the folder in which it was created. Only the owner of the files or the administrator can change the access rights. When ABAP statements create these files, they are then owned by the R/3 System, and the owner is either `<SID>ADM` or `SAPService<SID>` respectively.

Database Files

The database provider or the database administrator is responsible for protecting the data at the database level. You should therefore consult the documentation supplied by the database vendor on the subject of data protection and security.

For R/3 specifics, see the appropriate section in *Chapter 2-5 : Database Access Protection*.

Installation with Several R/3 Systems

If there are several R/3 Systems on the server(s), it is possible to perform the administration tasks separately using different local and global groups. Assign the access rights appropriately for the files in the directory (to include sub-directories) `\usr\sap`. You can distinguish between the administrators and groups by using the names of the R/3 Systems (for example, `<sid1>`, and `<sid2>`). All administrators should have access to the two directories at the `\usr\sap` top level.

If there are several R/3 Systems installed on a single server, then an additional area of shared memory exists. This memory is created by `saposcol.exe` and is used jointly by the OS Collector and all R/3 Systems. Therefore, give *Full Control* access rights to the `SAP_<SID>_LocalAdmin` local groups for the executable file `saposcol.exe`. In order to avoid access conflicts here, start `saposcol.exe` before R/3.

Additional Information on Windows NT Security

For current updates on the development of Windows NT security, see the following Web site:

- <http://www.microsoft.com/security> [D.6]
- <http://NTBugTraq.ntadvice.com> [D.7]

Logical Operating System Commands in R/3

Users can execute logical operating system commands as external commands in R/3.

Both the maintenance and execution of external commands is protected with R/3 authorizations. External commands can be maintained and executed either on-line (from the CCMS menu) or in ABAP programs, using special function modules.

In this section, we provide a short overview of this subject. For more detailed information, see the online documentation *BC Computing Center Management System → External Operating System Commands [A.6]*.



Caution

Note that every user with either programmer authorization or debugging authorization can execute any commands as user <sid>adm. This is another reason to be careful with assigning programming or debugging authorizations!

Executing External Commands

You can execute external commands using the Transaction SM49.

R/3 contains detailed information for each external command, including the operating system command itself, the pre-defined parameters in their full length, and information about whether additional parameters are permitted.

Before R/3 executes an external command, the additional parameters are checked. If impermissible characters are found, the command is not executed and the SECURITY_RISK exception is raised.

Users who execute external commands need to have the authorization S_LOG_COM with the following fields defined:

- *Command* (name of external command)
- *Opsystem* (operating system for which the command was defined)
- *Host* (symbolic hostname of the target system)

The fields *Command* and *Opsystem* are used to uniquely identify the external command, while *Host* defines the authorizations for executing commands on certain target computers.

The authorization S_LOGCOM_ALL (based on the authorization object: S_LOG_COM), which allows for the execution of all commands, is included in the standard delivery in the authorization profiles S_A.SYSTEM and S_A.ADMIN.



Note

To call external commands in your own developments, you should use the function module COMMAND_EXECUTE instead of CALL_SYSTEM. With COMMAND_EXECUTE, you can enforce a more extensive authorization check by including authorization profile arguments in the parameter ADDITIONAL_PARAMETERS. In addition, unlike CALL_SYSTEM, COMMAND_EXECUTE does not use RFC for its purposes. For more information, see the online documentation *BC Basis Programming Interfaces → Programming with External Operating System Commands [A.2]*.

Maintaining External Commands

You can modify these external commands and set up additional security mechanisms. You can also extend the range of the pre-defined commands supplied by SAP with your own commands and parameters. (You cannot change SAP commands in customer systems, however.)

To maintain external commands, use the Transaction SM69.

You can specify a function module to call before executing the command that checks the entry for correct parameters. We deliver the function module DUMMY_COMMAND_CHECK that you can use as a template for your individual command check modules. (Do not change the original. We suggest you copy it and change the copy.)

To maintain external commands, you need to have the authorization object S_RZL_ADM with the value '01' in the field *Activity* in your authorization profile.

Additional Information on Logical Operating System Commands in R/3

For more information, see:

- [R/3 Online Documentation: BC Computing Center Management System → R/3 System Administration → External Operating System Commands \[A.6\]](#)
- [R/3 Online Documentation: BC Basis Programming Interfaces → Programming with External Operating System Commands \[A.2\]](#)

Chapter 2-5 : Database Access Protection

The security of the database is generally the responsibility of the database provider and your database administrator. As with your network infrastructure, most of the measures that you can take depend highly on your strategy and priorities.

There are a number of general measures, as well as database-specific measures, that you can take to increase the protection of your database. Details are included in the appropriate sections.

General Recommendations

The following recommendations apply to database access protection in general, regardless of the specific database that you use:

- We recommend that you only use R/3 tools to access the database (see the section titled *Access Using Database Tools*).
- Change the initial password for SAPR3 (<SID>OFR on AS/400).
- Do not permit any access to USR* tables.
- Do not permit write access to the T000 table.
- Decide which other R/3 tables you need to protect and set their access rights accordingly. These may be general tables (for example, SAPUSER or RFCDES) or tables specific to an area of application (such as PA* or HCL*).

The rest of this chapter concentrates on security measures on accessing the database using database tools as well as individual measures for the various database products with the corresponding operating systems:

- **Access Using Database Tools**
- **ORACLE under UNIX**
- **ORACLE under Windows NT**
- **INFORMIX under UNIX**
- **ADABAS (under both UNIX and Windows NT)**
- **DB2 Common Server under UNIX**
- **DB2 Common Server under Windows NT**
- **DB2/400**

Access Using Database Tools

As previously mentioned, we recommend you only use R/3 tools to access the database. We offer our own tools for database access, for example, SAPDBA. These tools are sufficient for operating your R/3 System. However, it is possible to use other applications and tools for connecting to the database. You should be aware of the implications of using such tools.

Access Using R/3 Tools / SAPDBA

For certain database administration tasks, for example, creating back-ups and archives, we offer the tool SAPDBA. SAPDBA runs under CCMS and supports the databases ORACLE and INFORMIX. Within R/3, we also have additional tools that assist in tasks such as reorganization. (For more information, see the online documentation *BC SAP Database Administration* [A.11] under the appropriate database section.)

All R/3 tools access the database over the user `SAPR3 (<SID>OFR` on AS/400).

Direct Access Over External Applications (not recommended)

Certain applications use the R/3 SQL interface or the Open Database Connectivity (ODBC) interface to connect directly to the database. In regard to security, we do **not** recommend that you access the database using such tools. However, if you do decide to use such tools, then we advise you to take the following precautions:

- Do **not** use the user `SAPR3`. Create other users for such purposes.
- Restrict their access rights to the necessary tables only.
- Assign read access only to these users.



Caution

If you do allow direct access to the database, then we can no longer guarantee data consistency or authorization security. The data consistency mechanisms and authorization concept in R/3 only apply to database access using R/3 tools.

ORACLE under UNIX

We describe the measures that you need to take for an ORACLE database under UNIX in the following sections:

- **Changing Passwords of Database Standard Users (ORACLE / UNIX)**
- **Protecting SAPDBA Operations (ORACLE / UNIX)**
- **Setting Access Privileges for Database-Related Files and Directories (ORACLE / UNIX)**
- **Setting Access Privileges for SAPDBA Tools (ORACLE / UNIX)**
- **Useful Procedures for ORACLE under UNIX**
- **Additional Information for ORACLE under UNIX**

Changing Passwords of Database Standard Users (ORACLE / UNIX)

Table 2-5-1 shows the users for which you need to change passwords, along with the tool used for the procedure. See the section titled *Useful Procedures for ORACLE under UNIX* to find out how to proceed with changing the passwords.

Table 2-5-1 : Changing the Passwords for ORACLE Standard Users (ORACLE / UNIX)

User	Type	Method used to change password
<sid>adm	UNIX user	UNIX command passwd
ora<sid>	UNIX user	UNIX command passwd
SYS (internal)	database user	svrmgr1 or sqldba, chdbpass
SYSTEM	database user	svrmgr1 or sqldba, chdbpass
SAPR3	database user (R/3)	OPS\$ connect mechanism

SAPR3 and the OPS\$ connect mechanism

For the database, the R/3 System is a single user, SAPR3. To protect this user, and thereby to protect the database, you have to use a special password procedure called the **OPS\$ connect mechanism**. In this procedure, the system creates a special database user, OPS\$<sid>adm, and the SAPUSER table. The password for SAPR3 is stored in this table.

When a SAP R/3 program accesses the database, it first logs on to the database using the OPS\$ connect mechanism. It then retrieves the password for SAPR3 from the SAPUSER table and logs on a second time under the SAPR3 user.

Chapter 2 : The R/3 Security Toolbox

You need to consider the following points:

- Protect access to the `SAPUSER` table and the `SAPR3` user password by changing the password for `<sid>adm` regularly.
- Consequently, after changing the password for `SAPR3` in an R/3 System that you use as an import system, test imports no longer work correctly. You could override this problem by assigning `OPSS` users in the import system for all of the export systems. However, we recommend that you keep `OPSS` users to a minimum and accept the fact that test imports no longer work (see OSS Note 27928 [C.7]).
- To prevent someone from working around the `OPSS` connect mechanism by using an `.rhosts` file, deactivate the UNIX service `rlogin` in the `inetd.conf` file.

**Caution**

In a distributed system, the client is responsible for the authorization checks of the operating system user `OPSS<sid>adm`. Therefore, ensure that only authorized users can access PC clients with direct access to the database server.

**Note**

Do not change the value of the ORACLE parameter `REMOTE_OS_AUTHENT` to `FALSE` in order to prevent access as `OPSS<sid>adm` from clients. R/3 work processes need to be able to log on to the application servers as the `OPSS<sid>adm` user; therefore, this parameter needs to be set to the value `TRUE`.

You can use either the tool `sqldba` (or `svrmgr1`) or `chdbpass` to change the passwords for the users `SYS` and `SYSTEM`. `chdbpass` is described below.

Changing the passwords using `chdbpass`

You can use the `chdbpass` tool for the following tasks:

- Change the passwords of `SYSTEM` and `SYS` users.
- Set up the `OPSS` connect mechanism.
- Change the password of the `SAPR3` user.
- Change the password of the `OPSS<sid>adm` user.
- Reset all passwords to the ORACLE or SAP initial values, after which you should change the passwords. (Use this function in certain cases, for example, if users have forgotten their passwords.)

The following ORACLE restrictions apply to passwords that this tool changes:

- The maximum length of the password is 30 characters.
- You cannot use special characters or German umlaut characters.
- The character of a password cannot be numeric.

You can find the `chdbpass` tool on the *SAP Kernel CD* in the directory `<CD-Dir>/UNIX/COMMON/INSTALL`.

The tool writes a log to the following file: `$ORACLE_HOME/sapreorg/chdbpass.log`.



Caution

`chdbpass` asks for the password of the database user `SYSTEM`.

Check the authenticity of `chdbpass` very carefully before executing it. If you have reason to believe that the file has been tampered with, then reinstall it.

In addition, **prevent unauthorized access to the `chdbpass.sh` file!**

Protecting SAPDBA Operations (ORACLE / UNIX)

SAPDBA divides operations into two categories, standard and expert. For example, you may want to restrict who can execute operations such as `RESTORE`, as in comparison to `BACKUP`. You can protect certain SAPDBA operations with a password, allowing only "expert" users to execute them. You set these categories within the SAPDBA utility.

You also need to protect the password file `passwd.dba`. Refer to the online documentation for information on where the file is located, how to set the initial password and how to change the password. (See *BC Database Administration: ORACLE* → *Starting and Using the SAPDBA Program* → *SAPDBA: Expert Mode* → *Defining the Password*. [A.18])

Setting Access Privileges for Database-Related Files and Directories (ORACLE / UNIX)



Note

As of Release 3.0D, the access rights as shown in Table 2-5-2 are automatically set in the installation procedures.

We recommend that you restrict the UNIX file and directory access privileges as shown in Table 2-5-2 (see UP 2-5-3):

Table 2-5-2 : Setting Access Privileges for ORACLE Directories and Files (ORACLE / UNIX)

ORACLE Directory or File	Access Privilege in Octal Form (3.x / 4.0)	Owner	Group	Comment
/oracle/<SID>/sapdata*	700 / 755	ora<sid>	dba	
/oracle/<SID>/sapdata*/*	700 / 755	ora<sid>	dba	
/oracle/<SID>/sapdata*/*/*	600 / 640	ora<sid>	dba	• data files
/oracle/<SID>/saparch	700 / 700	ora<sid>	dba	
/oracle/<SID>/saparch/*	640 / 640	ora<sid>	dba	• archive files
/oracle/<SID>/sapreorg	700 / 755	ora<sid>	dba	
/oracle/<SID>/sapbackup	755 / 755	ora<sid>	dba	
/oracle/<SID>/dbs	755 / 755	ora<sid>	dba	
/oracle/<SID>/sapcheck	700 / 755	ora<sid>	dba	
/oracle/<SID>/sapstat	700 / 755	ora<sid>	dba	
/oracle/<SID>/saptrace	700 / 755	ora<sid>	dba	
/oracle/<SID>/saptrace/*	700 / 755	ora<sid>	dba	
/oracle/<SID>/saptrace*/*	600 / 640	ora<sid>	dba	
/oracle/<SID>/origlog*	700 / 755	ora<sid>	dba	• redo log directories
/oracle/<SID>/origlog*/*	700 / 755	ora<sid>	dba	• redo log files
/oracle/<SID>/mirrlog*/*	700 / 755	ora<sid>	dba	• redo log files
/oracle/<SID>/mirrlog*/*	700 / 755	ora<sid>	dba	• redo log files

Setting Access Privileges for SAPDBA Tools (ORACLE / UNIX)

If you use the CCMS backup planning tool, which uses the SAPDBA tools, then you should note the following:

- For ORACLE versions < 7.3, so that BRBACKUP can start up and shut down the database, the user <sid>adm must belong to the UNIX group dba (DB role: SYSDBA).
- In ORACLE versions >= 7.3, assign <sid>adm to the group oper. BRBACKUP then logs on with **connect / as sysoper**.

In ORACLE Version 7.3, the group dba has been split into the groups dba and oper. The group oper (DB role: SYSOPER) is an administrator group that is restricted to operator operations. oper can start or shut down the database, perform backups, etc., but has no read or write authorizations.

- BRBACKUP must also have full access to the SAPR3 tables SDBAD, SDBAH and tables defined in the XDB interface.
- SAPDBA only executes from CCMS when the database is open. Appropriate database privileges are necessary for the operations:
 - -check, -next, -checkopt, -analyze
- SAPDBA must have write permissions to the following tables:
 - SDBAD, SDBAH, DBSTATC, DBSTATTORA, DBSTATHORA, DBSTATIORA, DBSTAIHORA, SAPDBAPRIV, and tables defined in the XDB interface.

Useful Procedures for ORACLE under UNIX

UP 2-5-1 : Changing the Passwords for <sid>adm and ora<sid> (ORACLE / UNIX)

To change the passwords for <sid>adm and ora<sid>, proceed as follows:



Note

If you use Network Information Service (NIS), you should also refer to the NIS guide and the operating system documentation. (Changing the password with an activated NIS may be different from changing it with `passwd`.)

1. Logon as user <sid>adm.
2. Enter the `passwd` command at the UNIX prompt.
3. Enter the old and new passwords.

Repeat steps 1 to 3 for the user ora<sid>.

UP 2-5-2 : Changing the Passwords for SYS, SYSTEM, and SAPR3 using chdbpass (ORACLE / UNIX)

To change the passwords for SYS, SYSTEM, and SAPR3, perform the following:

Mounting and Starting chdbpass

1. Logon as user ora<sid>.
2. Ensure that the database is started and the R/3 System is stopped.
3. Mount the *SAP Kernel CD* (see the document *R/3 Installation on UNIX - OS Dependencies*).
4. Copy chdbpass from the upgrade or installation CD to the \$ORACLE_HOME/sapreorg directory by entering the following command:

```
cp <CD-DIR>/UNIX/COMMON/INSTALL/chdbpass $ORACLE_HOME/sapreorg/chdbpass
(<CD-DIR> is the CD mount point).
```

5. Enter the following commands to select the directory and start chdbpass.

```
cd $ORACLE_HOME/sapreorg
```

```
./chdbpass
```

Changing passwords

chdbpass first makes sure that the environment variables ORACLE_HOME and ORACLE_SID are correctly set.

6. Confirm the settings.
7. Enter the current password for the SYSTEM user.



Note

chdbpass performs all database actions under this user.

8. Choose the menu option you want as indicated in the following table:

To:	Choose Menu Path:	What you need to know:
Set up the OPS\$ connect mechanism and change the password of SAPR3	a) <i>Initialize OPS-Connect and change password of SAPR3</i>	You are first asked to specify the password for the new user OPS\$<sid>adm and then the new password for SAPR3
Change the password of SYS	c).....	
Change the password of SYSTEM	d).....	

UP 2-5-3 : Setting Access Privileges for Files and Directories (ORACLE / UNIX)

Saving Current Settings

Before changing the access privileges, we advise you to save your current settings. Enter the following commands:

```
cd /oracle/<SID>
ls -lR > oracle_perm.txt

cd /usr/sap
ls -lR > sap_perm.txt

cd /sapmnt
ls -lR > sap_sw.txt
```

Setting Access Privileges

To change the access privileges for a file or directory use the `chmod` command as shown below:

```
chmod <access privileges in octal> <file or directory>
```



Example

```
chmod 700 /oracle/<SID>/sapdata*
chmod 700 /oracle/<SID>/sapdata**
chmod 600 /oracle/<SID>/sapdata**/*
.
.
.
```



Caution

Do not use `chmod` recursively. It is very easy to make unintended changes to authorizations when doing so.

Additional Information for ORACLE under UNIX

For more information, refer to the following documentation:

- [R/3 Online Documentation: BC SAP Database Administration: Oracle](#) [A.17]
- [R/3 Online Documentation: BC Database Administration: ORACLE → Starting and Using the SAPDBA Program → SAPDBA: Expert Mode → Defining the Password](#) [A.18]
- [OSS Note 27928: Consequences in transport during password change](#) [C.7]

ORACLE under Windows NT

We describe the measures that you need to take for an ORACLE database under Windows NT in the following sections:

- **Changing Passwords of Database Standard Users (ORACLE / Windows NT)**
- **Setting Access Rights for Database-Related Files and Directories (ORACLE / Windows NT)**
- **Setting Access Rights for SAPDBA Tools (ORACLE / Windows NT)**
- **Useful Procedures for ORACLE under Windows NT**
- **Additional Information for ORACLE under Windows NT**

Changing Passwords of Database Standard Users (ORACLE / Windows NT)

The following table shows the users for which you need to change passwords, along with the tool used for the procedure. See the section titled *Useful Procedures for ORACLE under Windows NT* to find out how to proceed with changing the passwords.

Table 2-5-3 : Changing the Passwords for ORACLE Standard Users (ORACLE / Windows NT)

User	Type	Method used to change password
SAPService<SID>	OPPS\$ user	OPPS\$ user mechanism (see below)
<SID>ADM	OPPS\$ user	OPPS\$ user mechanism (see below)
SYS (internal)	database user	SVRMGR30, SVRMGR23, SQLDBA72
SYSTEM	database user	SVRMGR30, SVRMGR23, SQLDBA72
SAPR3	database user (R/3)	OPPS\$ user mechanism (see below)

OPPS\$ user mechanism under Windows NT

For the database, the R/3 System is a single user, SAPR3. Under Windows NT, only the operating system users of the R/3 System have access to the password of the user SAPR3, and therefore access to the database. These are generally the users SAPService<SID> and <SID>ADM; however, you may assign other names for these users. In the following discussion, we refer to the operating system users as SAPService<SID> and <SID>ADM.

To prevent unauthorized access to the database, use the ORACLE OPPS\$ user mechanism to create the users SAPService<SID> and <SID>ADM, and change the password for SAPR3.

**Note**

With the ORACLE network protocol SQL*Net V1, you can only use this mechanism in central systems. With SQL*Net V2, you can use it in both central and distributed R/3 Systems. However, when you use the OPS\$ in a distributed system, you must set the following parameter in the file `init<SID>.ora`:

```
remote_os_authent=TRUE
```

Create OPS\$ users for the following:

- Users who must be able to logon to the database from outside an R/3 System.

Use this for example, for users who start the program `tp`, which connects to the database. In this case, we suggest using the user `<SID>ADM` of this system and the user `<SID>ADM` of other R/3 Systems as needed to access the database.

- Windows NT users who run the R/3 System.

In this case, we suggest using the user `SAPService<SID>` of this system and the user `<SID>adm` of other R/3 Systems as needed to access this database.

Setting Access Privileges for Database-Related Files and Directories (ORACLE / Windows NT)

Under Windows NT, you should protect all data files, all executable files, all ORACLE files, as well as all R/3 files. To protect the ORACLE files, assign the following access rights:

- Assign the local group `SAP_<SID>_Local_admin` and the local user `SYSTEM` full control access rights for all ORACLE files.
- Assign other groups and users no access rights for the ORACLE files.

Table 2-5-4 shows the files and the corresponding access rights:

Table 2-5-4 : Setting Access Privileges for DB2/CS Directories and Files (ORACLE / Windows NT)

ORACLE Directory	Access Privilege	for user/group
<code><drive>:\ORANT</code>	<i>Full Control</i>	<code>SAP_<SID>_LocalAdmin, SYSTEM</code>
<code><drive>:\oracle\<sid></code>	<i>Full Control</i>	<code>SAP_<SID>_LocalAdmin, SYSTEM</code>
<code><drive>:\usr\sap</code>	<i>Full Control</i>	<code>SAP_<SID>_LocalAdmin, SYSTEM</code>

Measures to take for the other files are included in *Chapter 2-4 : Operating System Protection*.

Setting Access Privileges for SAPDBA Tools (ORACLE / Windows NT)

If you use the CCMS backup planning tool, which uses the SAPDBA tools, then you should note the following:

- For ORACLE versions < 7.3, so that BRBACKUP can start up and shut down the database, the user <SID>ADM must belong to the Windows NT local group ORA<SID>DBA (DB role: SYSDBA).
- In ORACLE versions >= 7.3, assign <SID>ADM to the local group ORA_<SID>_OPER. BRBACKUP then logs on with **connect / as sysoper**.

In ORACLE Version 7.3, the group dba has been split into the groups ORA_<SID>_DBA and ORA_<SID>_OPER. The group ORA_<SID>_OPER (DB role: SYSOPER) is an administrator group that is restricted to operator operations. ORA_<SID>_OPER can start or shut down the database, perform backups, etc., but has no read or write authorizations.

- BRBACKUP must also have full access to the SAPR3 tables SDBAD, SDBAH and tables defined in the XDB interface.
- SAPDBA only executes from CCMS when the database is open. Appropriate database privileges are necessary for the operations:
 - -check, -next, -checkopt, -analyze
- SAPDBA must have write permissions to the following tables:
 - SDBAD, SDBAH, DBSTATC, DBSTATTORA, DBSTATHORA, DBSTATIORA, DBSTAIHORA, SAPDBAPRIV, and tables defined in the XDB interface.

Useful Procedures for ORACLE under Windows NT

UP 2-5-4 : Specifying the Name of the User that Starts R/3 - SAPService<SID> (ORACLE / Windows NT)

To specify the user that starts R/3, perform the following:

1. From the WinNT task bar, choose *Start* → *Settings* → *Control Panel*.
2. Choose *Services*.
3. In the service list, choose the R/3 Service *SAP<SID>_<Instance_ID>*.
4. Choose *Startup*.
5. In the field *This account* in the group *Log on As*, specify the user who starts the R/3 System.

UP 2-5-5 : Creating an OPS\$ User for <SID>ADM (ORACLE / Windows NT)

To create an OPS\$ user for <SID>ADM, perform the following:

1. If the R/3 System is running, then stop it.
2. Logon as user <SID>ADM to the host where the R/3 database for the R/3 System is located. You must execute all of the following commands on this host.
3. Start *sqldba72* (or *svrmgr23*, *svrmgr30*)
4. Logon to the database with **connect internal**.
5. Execute the following commands in succession. Replace <password> with the new password for the user *SAPR3*.

```
create user OPS$SAPService<SID> identified externally;

grant connect, resource to OPS$SAPService<SID>;

connect /

create table SAPUSER
( USERID VARCHAR2(20), PASSWD VARCHAR2 (20));

insert into SAPUSER values ('SAPR3', '<password>');

connect internal

alter user SAPR3 identified by <password>;
```

UP 2-5-6 : Creating an OPSS User for SAPService<SID> (ORACLE / Windows NT)

To create an OPSS user for SAPService<SID>, perform the steps below. First, note the following:

 **Note**

If you are currently logged on as <SID>ADM, (for example you have just completed the procedure above), then you can skip steps 1 and 2.

1. If the R/3 System is running, then stop it.
2. Logon as user <SID>ADM to the host where the R/3 database for the R/3 System is located. You must execute all of the following commands on this host.
3. Start `sqldba72` (or `svrmgr23`, `svrmgr30`).
4. Logon to the database with `connect internal`.
5. Execute the following commands in succession. Replace <password> with the new password for the user SAPR3.

```
create user OPSSSAPService<SID> identified externally;

grant connect, resource to OPSSSAPService<SID>;

create public synonym sapuser for OPSS<SID>ADM.SAPUSER;

connect /

grant select on sapuser to OPSSSAPService<SID>;
```

UP 2-5-7 : Changing the Password of SAPR3 (ORACLE / Windows NT)

If you have already created the OPSS user as described above, the password for the SAPR3 user can be changed at any time. Perform the following steps (replace <new password> with the password for the user SAPR3):

1. If the R/3 System is running, then stop it.
2. Logon as user <SID>ADM to the host where the R/3 database for the R/3 System is located. You must execute all of the following commands on this host.
3. Start `sqldba72` (or `svrmgr23`, `svrmgr30`).
4. Logon to the database with `connect internal`.
5. Execute an update on the SAPUSER table by entering the following command:

```
update OPSSSAPService<SID>.SAPUSER set PASSWD='<new password>' where
USERID='SAPR3';
```

6. Change the password for SAPR3 in the database with the command:

```
alter user sapr3 identified by <new password>;
```

Additional Information for ORACLE under Windows NT

For more information, refer to the following documentation:

- [R/3 Online Documentation: BC SAP Database Administration: Oracle](#) [A.17]
- [OSS Note 50088: Creating OPS\\$ users on Windows NT/Oracle](#) [C.19]
- [OSS Note 48736: Set up ORACLE SQL*Net V2 under Windows NT](#) [C.18]

INFORMIX under UNIX

We describe the measures that you need to take for an INFORMIX database under UNIX in the following sections:

- **Changing the Passwords of the Database Standard Users (INFORMIX / UNIX)**
- **Setting Access Privileges for Database-Related Files and Directories (INFORMIX / UNIX)**
- **Useful Procedures for INFORMIX**
- **Additional Information for INFORMIX**

Changing the Passwords of the Database Standard Users (INFORMIX / UNIX)

Table 2-5-5 shows the users for which you need to change passwords, along with the tool used for the procedure.

When you change the password for `sapr3`, you also need to update the `SAPUSER` table in the database. Otherwise, R/3 work processes cannot connect successfully to the INFORMIX database. See UP 2-5-8 to find out how to change the passwords, as well as how to update the `SAPUSER` table.

Table 2-5-5 : Changing the Passwords for INFORMIX Standard Users (INFORMIX / UNIX)

User	Type	Method used to change password
<sid>adm	UNIX and DB user	UNIX command <code>passwd</code>
informix	UNIX and DB administrator	UNIX command <code>passwd</code>
sapr3	UNIX and database user (R/3)	UNIX command <code>passwd</code>

Note

Prior to Release 2.1J/2.2D, the environment variable `INFORMIX_DB_PASSWD` was needed when changing the passwords. If you have updated from an older release, you should delete this environment variable and remove any references to it from script files.

Setting Access Privileges for Database-Related Files and Directories (INFORMIX / UNIX)

We recommend that you restrict the UNIX file and directory access privileges as shown in Table 2-5-6 (see UP 2-5-11):

Table 2-5-6 : Setting Access Privileges for INFORMIX Directories and Files (INFORMIX / UNIX)

INFORMIX Directory or File	Access Privilege in Octal Form	Owner	Group	Comment
/informix/<SID>/sapdata	755	informix	informix	
/informix/<SID>/sapdata/*	755	informix	informix	
/informix/<SID>/sapdata/*/*	777	---	---	• link
/informix/<SID>/sapreorg	775	informix	sapsys	
Raw devices for INFORMIX database	660	informix	informix	• Refer to the raw devices as pointed to by the links in the <physdev><i> directories.

Useful Procedures for INFORMIX

UP 2-5-8 : Changing the passwords for <sid>adm, sapr3, and informix (INFORMIX / UNIX)

To change the passwords for <sid>adm, sapr3, and informix, perform the following steps:

Note

If you use Network Information Service (NIS) , you should also refer to the NIS guide and the operating system documentation. (Changing the password with an activated NIS may be different from changing it with `passwd`.)

1. Logon as user <sid>adm.
2. Enter the `passwd` command at the UNIX prompt.
3. Enter the old and new passwords.
4. Repeat steps 1 to 3 for the users `sapr3` and `informix`.
5. Update the `SAPUSER` table by entering the following commands at the UNIX command prompt:

```
su - <sid>adm
```

```
echo "update sapuser set passwd='<sapr3_passwd>' where userid='sapr3';" | dbaccess <sid>
```

UP 2-5-9 : Setting Access Privileges for Files and Directories (INFORMIX / UNIX)**Saving Current Settings**

Before changing the access privileges, we advise you to save your current settings. Enter the following commands:

```
cd /informix/<SID>
ls -lR > informix_perm.txt

cd /usr/sap
ls -lR > sap_perm.txt

cd /sapmnt
ls -lR > sap_sw.txt
```

Setting Access Privileges

To change the access privileges for a file or directory use the `chmod` command as shown below:

```
chmod <access privileges in octal> <file or directory>
```

**Example**

```
chmod 755 /informix/<SID>/sapdata
chmod 755 /informix/<SID>/sapdata/*
chmod 777 /informix/<SID>/sapdata/**
.
.
.
```

**Caution**

Do not use `chmod` recursively. It is very easy to make unintended changes to authorizations when doing so.

Changing Owner and Group

To change the owner and group of the INFORMIX devices, use the commands `chown` and `chgrp` respectively. See the following example to change the owner and group for a device to `informix`:

**Example**

```
chown informix <name of device>
chgrp informix <name of device>
```

Additional Information for INFORMIX

For more information, refer to the following documentation:

- [R/3 Online Documentation: BC SAP Database Administration: INFORMIX \[A.16\]](#)

ADABAS

We describe the general measures that you need to take for an ADABAS database (under all operating systems) in the following sections:

- **Changing the Passwords of Database Standard Users (ADABAS / All)**
- **Protecting CONTROL Operations (ADABAS / All)**
- **Measures Specific to ADABAS under UNIX (ADABAS / UNIX)**
- **Measures Specific to ADABAS under Windows NT (ADABAS / Windows NT)**
- **Useful Procedures for ADABAS**
- **Additional Information for ADABAS**

Changing the Passwords of Database Standard Users (ADABAS / All)

Table 2-5-7 shows the database users for which you need to change passwords, along with the tool used for the procedure. See the section titled *Useful Procedures for ADABAS* to find out how to proceed with changing the passwords.

Table 2-5-7 : Changing the Passwords for ADABAS Standard Users (ADABAS / All)

User	Type	Method used to change password
CONTROL	database user (SYSUSER)	CONTROL
SUPERDBA	database user (SYSUSER)	CONTROL
OPERATOR (see Note below)	database user (SYSUSER)	CONTROL
SAPR3	database user (R/3)	XSQL or XQUERY



Note

You may or may not have to change the password for the user `OPERATOR`. In the following text (as well as in the Useful Procedures), we refer to `OPERATOR`. However, if you do not need to change the password, then you can ignore `OPERATOR` in the corresponding actions. The following guidelines apply:

- **Prior to ADABAS Release 6.2:** You only need to change the password for `OPERATOR` if you use this user. If you do not use `OPERATOR`, then you do not need to change its password.
- **As of ADABAS Release 6.2:** Here, you do not need to change password for `OPERATOR`. It is a restricted user for the `xcontrol` tool only.

SYSUSERS

The SYSUSERS are CONTROL, SUPERDBA and OPERATOR. You change their passwords using the CONTROL tool. See UP 2-5-10 for instructions on changing the passwords.

Note the following:

- After changing the passwords for SUPERDBA and OPERATOR, you can logon to the database without having to restart the database.
- The start and stop scripts log on to the database by using the XUSER file. Therefore, when you change the passwords of the CONTROL, SUPERDBA or OPERATOR, you must also update the XUSER file. You must update the file once as user <sid>adm and also as sqd<sid>. The steps required for this procedure are also included in UP 2-5-11.

SAPR3

For the database, the R/3 System is a single user, SAPR3. There are two ways to change the password for SAPR3.

1. As user SAPR3 (See UP 2-5-12).
2. As user SUPERDBA (See UP 2-5-13).

As with the SYSUSERS, you must also update the XUSER file. See UP 2-5-14.

Protecting CONTROL Operations (ADABAS/All)

ADABAS divides its database operations into two categories, critical and uncritical. For example, you may want to restrict who can execute operations such as RESTORE, as in comparison to BACKUP. Therefore, there are two levels of users, the CONTROL user and the operator user. A CONTROL user can execute more operations than an operator user. For example, only an operator user can perform tasks such as starting and stopping the database, backing up the database and logs, as well as history and log control. The CONTROL user can perform more critical operations such as restoring the database.

Measures Specific to ADABAS under UNIX (ADABAS / UNIX)

We describe the measures that you need to take for an ADABAS database under UNIX in the following sections:

- **Changing the Passwords of Operating System Users (ADABAS / UNIX)**
- **Setting Access Privileges for Database-Related Files and Directories (ADABAS / UNIX)**

Changing the Passwords of Operating System Users (ADABAS/UNIX)

Table 2-5-8 shows the UNIX users for which you need to change passwords, along with the tool used for the procedure. See UP 2-5-15 to find how to proceed with changing the passwords.

Table 2-5-8 : Changing the Passwords for ADABAS Standard Users (ADABAS / UNIX)

User	Type	Method used to change password
<sid>adm	UNIX user	UNIX command passwd
sqd<sid>	UNIX user	UNIX command passwd

Setting Access Privileges for Database-Related Files and Directories (ADABAS / UNIX)

The access rights are automatically set in the installation procedures. The script that executes this procedure is `bin/x_install`. You can find it in the directory `/adabas/<SID>/db` and the user `ROOT` can run it at any time. The script sets the UNIX file and directory access privileges as shown in Table 2-5-9:

Table 2-5-9 : Setting Access Privileges for ADABAS Directories and Files (ADABAS / UNIX)

ADABAS Directory or File	Access Privilege in Octal Form	Owner	Group	Comment
<code>/adabas/<SID>/sap*</code>	750	sqd<sid>	dba	
<code>/adabas/<SID>/sapdata/*</code>	750	sqd<sid>	dba	
<code>/adabas/<SID>/saplog/*</code>	750	sqd<sid>	dba	
<code>/adabas/<SID>/sapsys/*</code>	750	sqd<sid>	dba	
<code>/adabas/<SID>/dbsys</code>	750	sqd<sid>	dba	
<code>/adabas/<SID>/dbsys/sys</code>	660	sqd<sid>	dba	
Raw devices for ADABAS database	660	sqd<sid>		<ul style="list-style-type: none"> • Refer to the raw devices used as Data and Logdevspaces. • The privileges of the nodes are also 660; not only the links contained in the directories <code>/adabas/<SID>/sapdata</code> and <code>saplog</code>.

You can also change the access privileges at any time with the `chmod` command (see UP 2-5-16).

Measures Specific to ADABAS under Windows NT

We describe the measures that you need to take for an ADABAS database under Windows NT in the following sections:

- **Changing the Passwords of Operating System Users (ADABAS / Windows NT)**
- **Setting Access Rights for Database-Related Files and Directories (ADABAS / Windows NT)**

Changing the Passwords of Operating System Users (ADABAS / Windows NT)

Under Windows NT, you need to change the password of the user <sid>adm.

Setting Access Privileges for Database-Related Files and Directories (ADABAS / Windows NT)

If you use an ADABAS D database under Windows NT, then the Devspaces of the database are automatically protected. Only the group of administrators has full access privileges for the devspaces and all other users have no access.

In addition, you must protect the directory %DBROOT%\config. This directory contains the configuration files of the databases. Set the following access privileges for the directory %DBROOT%\config and all the files it contains:

- Full control access privileges for the local group Administrators
- No access privileges for other groups or users

If you want to exclude all other users from access to the database with database tools, you must set the following privileges for the directory %DBROOT% and all its subdirectories:

- Full control access privileges for the local group Administrators
- No access privileges for all other groups or users

Useful Procedures for ADABAS

UP 2-5-10 : Changing the Passwords for the Users CONTROL, SUPERDBA, and OPERATOR (ADABAS / All)

To change the passwords for CONTROL, SUPERDBA, and OPERATOR, proceed as follows:



You can only change CONTROL's password in "cold mode"¹; you can only change the passwords for SUPERDBA and OPERATOR in "warm mode".

In the CONTROL main menu:

1. Choose the menu path *CONFIGURATION* → *ALTER PARAMETERS* → *SYSUSERS*.
2. In the *ALTER CONTROLUSER* menu, enter the name of the <user> and a new password.

You must also confirm the new password.

3. Choose *OK* to save the password.

Perform these steps for the users CONTROL, SUPERDBA, and OPERATOR.

UP 2-5-11 : Updating the XUSER File for the Users CONTROL and SUPERDBA. (ADABAS / All)

To update the XUSER file for the users CONTROL and SUPERDBA, proceed as follows:

1. Start the XUSER tool with the user <sid>adm.
2. Logon using the user SAPR3 and the SAPR3 password.

User CONTROL

3. Use the function key F4 to page to USERKEY c.
4. Enter the new password of the user CONTROL.
5. Save it by pressing F5.

User SUPERDBA

6. Use the function key F4 to page to USERKEY w.
7. Enter the new password of the user SUPERDBA.
8. Save it by pressing F5.

Repeat steps 1-8 as user sqd<sid> instead of <sid>adm.

¹ The ADABAS server has three modes of operation: offline, cold, and warm. In offline mode, the ADABAS server is not running and the database server kernel has not been started. In cold mode, the ADABAS server has been started, however, you can only perform certain maintenance activities. Warm mode is the normal operating mode.

UP 2-5-12 : Changing the Password of SAPR3 As User SAPR3 (ADABAS / All)

To change the password of SAPR3 as user SAPR3, proceed as follows:

**Note**

If you use XQUERY for changing the password, you must set the SQLMODE to ADABAS in the command line before you execute the command.

1. Call XSQL (or XQUERY) from the operation system level without any additional options.

You will be automatically logged on (over the XUSER file) as user SAPR3.

2. To change the password, enter the following command:

```
ALTER PASSWORD <oldpassword> to <newpassword>
```

3. Update the XUSER file for user SAPR3. (See UP 2-5-14.)

UP 2-5-13 : Changing the Password of SAPR3 As User SUPERDBA (ADABAS / All)

To change the password of SAPR3 as user SUPERDBA, proceed as follows:

**Note**

If you use XQUERY for changing the password, you must set the SQLMODE to ADABAS in the command line before you execute the command.

1. Start XSQL (or XQUERY) from the operation system level by entering the following command:

```
xsql -u superdba,<password>
```

2. To change the password, enter the following command:

```
ALTER PASSWORD <user> <newpassword>
```

3. Update the XUSER file for user SAPR3 (See UP 2-5-14).

UP 2-5-14 : Updating the XUSER File for the User SAPR3 (ADABAS / All)

To update the XUSER file for user SAPR3, proceed as follows:



You need to perform this procedure using both the users <sid>adm and sqd<sid> on all application servers.

1. Start the XUSER tool with the user <sid>adm.
2. Logon using the user SAPR3 and the old SAPR3 password.
3. In the first menu, USERKEY: DEFAULT, enter the new password for SAPR3.
4. Save the password by pressing F5.
5. Use the function key F4 to page to USERKEY <sid>.
6. Enter the new password for SAPR3.
7. Save it by pressing F5.

Repeat steps 1-7 with the user sqd<sid> instead of <sid>adm.

UP 2-5-15 : Changing the Passwords for <sid>adm and sqd<sid> (ADABAS / UNIX)

To change the passwords for <sid>adm and sqd<sid>, proceed as follows:



If you use Network Information Service (NIS), you should also refer to the NIS guide and the operating system documentation. (Changing the password with an activated NIS may be different from changing it with `passwd`.)

1. Logon as user <sid>adm.
2. Enter the `passwd` command at the UNIX prompt.
3. Enter the old and new passwords.

Repeat steps 1 to 3 for the user sqd<sid>.

UP 2-5-16 : Setting Access Privileges for Files and Directories (ADABAS / UNIX)**Saving Current Settings**

Before changing the access privileges, save your current settings. Enter the following commands:

```
cd /adabas/<SID>  
ls -lR > adabas_perm.txt
```

```
cd /usr/sap  
ls -lR > sap_perm.txt
```

```
cd /sapmnt  
ls -lR > sap_sw.txt
```

Setting Access Privileges

To change the access privileges for a file or directory use the `chmod` command as shown below:

```
chmod <access privileges in octal> <file or directory>
```

**Example**

```
chmod 750 /adabas/<SID>/sap*  
chmod 750 /adabas/<SID>/sapdata/*  
chmod 750 /adabas/<SID>/saplog/*  
.  
.
```

**Caution**

Do not use `chmod` recursively. It is very easy to make unintended changes to authorizations when doing so.

Additional Information for ADABAS

For more information, refer to the following documentation:

- [R/3 Online Documentation: ADABAS \(Software AG\) \[A.12\]](#)

DB2 Common Server under UNIX

The concept outlined here applies to Release 4.0B and later releases.

General Information

Under UNIX, DB2 common server runs with an “authentication = server”, which means that the user ID and password provided on connect or attach are verified by DB2 using operating system services from within the database server. Remote and local application servers connect to DB2 using user `sapr3` or they attach for specific purposes as user `<sid>adm`.

R/3 DB2 common server additionally maintains the user IDs and passwords for `<sid>adm` and `sapr3` in the file:

```
/usr/sap/<SID>/SYS/global/dscdb6.conf
```

This file is accessible from all application servers over NFS (AIX) or NT shares (NT). Passwords are stored encrypted. R/3 DB2 common server provides functions for the following:

- to create `dscdb6.conf`
- to retrieve users IDs and passwords
- to update passwords in `dscdb6.conf` and in the operating system simultaneously

For all the `dscdb6.conf` accesses described in this chapter, the environment variable `DB2DB6EKEY` is used to encrypt or decrypt the requested password.



Note

Prior to DB2 Version 5, the environment variable used for encrypting and decrypting the password was called `DB6EKEY`. As of Version 5, the variable is now called `DB2DB6EKEY`. In the following discussion, we refer to it as `DB2DB6EKEY`.

`DB2DB6EKEY` is set initially during installation to the value `<SID><db_server_hostname>`. You can change this value at any time, but if you do, then you also need to update the `sapr3` and `<sid>adm` passwords (see the section titled *Changing the Passwords of Database Standard Users*).

The SAP profiles `.dbenv_<hostname>.csh` and `.dbenv_<hostname>.sh` contain the `DB2DB6EKEY` value. This environment variable is set when `<sid>adm` and `db2<sid>` log on.

The measures that you need to take for a DB2 common server database under UNIX, as well as useful procedures and additional information are provided in the following sections:

- **Changing the Passwords of Database Standard Users (DB2/CS / UNIX)**
- **Protecting SAP-DB2admin Operations (DB2/CS / UNIX)**
- **Setting Access Privileges for Database-Related Files and Directories (DB2/CS / UNIX)**
- **Useful Procedures for DB2 Common Server under UNIX**
- **Additional Information for DB2 Common Server under UNIX**

Changing the Passwords of Database Standard Users (DB2/CS / UNIX)

Table 2-5-10 shows the UNIX users for which you need to change passwords, along with the tool used for the procedure. See UP 2-5-17 (for `db2<sid>`) and the online documentation *BC SAP Database Administration: DB2 common server: Users* (for `<sid>adm` and `sqd<sid>`) for information on how to proceed with changing the passwords.

Table 2-5-10 : Changing the Passwords for DB2/CS Standard Users (DB2/CS / UNIX)

User	Type	Method used to change password
<code>db2<sid></code>	UNIX and database user	UNIX command <code>passwd</code>
<code><sid>adm</code>	UNIX and database user	DB2 Control Center
<code>sqd<sid></code>	UNIX and database user	DB2 Control Center

`db2<sid>`

This user is the DB2 instance owner. It is the DB2 system administrator and the R/3 database administrator. It is authorized to execute database and Database Manager administration functions such as:

- Creating a database
- Creating or changing a tablespace
- Updating DB2 parameters
- Backing up or restoring the database
- Changing the passwords of the users `sapr3` and `<sid>adm`

`db2<sid>` belongs to the operating system group `SYSADM` and has the DB2 authority `SYSADM`. `SYSADM` has the highest level of DB2 authority and includes all lower-level authorities.

Use the standard operating system utilities (command `passwd`) to change the password of `db2<sid>` (see UP 2-5-17). It is not necessary for the password to be the same on all hosts in your R/3 System.

<sid>adm

This user is the R/3 System administrator. <sid>adm is authorized to start and stop the R/3 System and the DB2 Database Manager.

<sid>adm belongs to the operating system groups SYCTRL and SAPSYS and has the DB2 authorities DBADM and SYCTRL. DB2-specific monitoring functions invoked by R/3 application server functions require SYCTRL authority.

Use the DB2 Control Center *Managing Passwords* function to change the password. (For more information, see the online documentation *BC SAP Database Administration: DB2 common server → Managing Passwords of R/3 Admin Users* [A.14].)

sapr3

This user is the owner of all R/3 database objects (tables, indexes and views). All R/3 application server connections and accesses are done on behalf of `sapr3`.

`sapr3` belongs to the operating system group SAPSYS and is created only on R/3 Systems that have the R/3 DB2 database installed (not on remote application servers). `sapr3` has the DB2 authorities CREATETAB, BINDADD and CONNECT.

Use the DB2 Control Center *Managing Passwords* function to change the password. (For more information, see the online documentation *BC SAP Database Administration: DB2 common server → Managing Passwords of R/3 Admin Users* [A.14].)

Changing the Encryption Key DB2DB6EKEY

The environment variable DB2DB6EKEY contains the key used for the encryption of the <sid>adm and `sapr3` passwords stored in file `dscdb6.conf`. You can change DB2DB6EKEY at any time, but if you do, note the following:

- You must change the DB2DB6EKEY value in all `.dbenv_<hostname>.csh` and `.dbenv_<hostname>.sh` profiles on all R/3 hosts.
- `.dbenv_<hostname>.csh` resp. `.dbenv_<hostname>.sh` is invoked when `db2<sid>` and `<sid>adm` log on.
- You must change the passwords of `<sid>adm` and `sapr3` immediately after you have altered the DB2DB6EKEY.

Protecting SAP-DB2admin Operations (DB2/CS / UNIX)

You can perform security-critical and less critical operations with the R/3 database administration tool SAP-DB2admin.

The first category includes the RESTORE and BACKUP commands. Since these database backups should only be performed in a protected and controlled environment, only the DB2 database administrator (`db2<sid>`) can execute these commands. Ensure that once you have made a database backup, no unauthorized persons have access to the storage medium.

Only the <sid>adm user is authorized to start and stop the R/3 System from SAP-DB2admin.

Setting Access Privileges for Database-Related Files and Directories (DB2/CS / UNIX)



Note

As of Release 3.0D, the access rights as described in the following table are automatically set in the installation procedures.

We recommend that you restrict the UNIX file and directory access privileges as shown in Table 2-5-11 (see UP 2-5-18):

Table 2-5-11 : Setting Access Privileges for DB2/CS Directories and Files (DB2/CS / UNIX)

DB2 common server Directory or File	Access Privilege in Octal Form	Owner	Group
/db2/<SID>	755	db2<sid>	sysadm
/db2/<SID>/log_dir	750	db2<sid>	sysadm
/db2/<SID>/log_retrieve (as of Release 4.0B)	750	db2<sid>	sysadm
/db2/<SID>/log_archive	2755	db2<sid>	sysadm
/db2/<SID>/log_archive/<SID>	755	db2<sid>	sysadm
/db2/<SID>/sapdata*	700	db2<sid>	sysadm
/db2/<SID>/sapdata*/*	600	db2<sid>	sysadm
/db2/<SID>/saparch	777	db2<sid>	sysadm
/db2/<SID>/dbs (prior to Release 4.0B)	4755	db2<sid>	sysadm
/db2/<SID>/sapbackup (prior to Release 4.0B)	777	db2<sid>	sysadm
R/3 Directory or File	Access Privilege in Octal Form	Owner	Group
<sapmnt>/exe	755	<sid>adm	sapsys
<sapmnt>/global	700	<sid>adm	sapsys
<sapmnt>/profile	755	<sid>adm	sapsys
/usr/sap/trans	775	<sid>adm	sapsys
/usr/sap/<SID>	755	<sid>adm	sapsys
/usr/sap/<SID>/SYS	755	<sid>adm	sapsys
/usr/sap/<SID>/<instance directory>	755	<sid>adm	sapsys
/usr/sap/<SID>/SYS/exe/run/dscdb6up	4750	root	sysadm
/usr/sap/<SID>/SYS/exe/run/db6util	4755	<sid>adm	sapsys
/usr/sap/<SID>/SYS/exe/run/dmdb6srp	4755	<sid>adm	sapsys
/usr/sap/<SID>/SYS/exe/run/brarchive	4755	db2<sid>	sapsys
/usr/sap/<SID>/SYS/exe/run/brrestore	4755	db2<sid>	sapsys
/usr/sap/<SID>/SYS/global/dscdb6.conf	600	<sid>adm	sapsys
/usr/sap/<SID>/SYS/exe/run/sddb6utl	4755	db2<sid>	sapsys
/usr/sap/<SID>/SYS/exe/run/backint (prior to Release 4.0B)	755	<sid>adm (adm<sid> prior to Release 4.0B)	sapsys

Useful Procedures for DB2 Common Server under UNIX

UP 2-5-17 : Changing the password for db2<sid> (DB2/CS / UNIX)

To change the password for db2<sid>, proceed as follows:



If you use Network Information Service (NIS), you should also refer to the NIS guide and the operating system documentation. (Changing the password with an activated NIS may be different from changing it with `passwd`.)

1. Logon as user db2<sid>.
2. Enter the `passwd` command at the UNIX prompt.
3. Enter the old and new passwords.

UP 2-5-18 : Setting Access Privileges for Files and Directories (ADABAS / UNIX)

Saving Current Settings

Before changing the access privileges, we advise you to save your current settings. Enter the following commands:

```
cd /db2/<SID>
ls -lR > db2_perm.txt

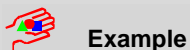
cd /usr/sap
ls -lR > sap_perm.txt

cd /sapmnt
ls -lR > sap_sw.txt
```

Setting Access Privileges

To change the access privileges for a file or directory use the `chmod` command as shown below:

```
chmod <access privileges in octal> <file or directory>
```



```
chmod 755 /db2/<SID>
chmod 750 /db2/<SID>/log_dir
chmod 2755 /db2/<SID>/log_archive
.
.
.
```

UP 2-5-18 : Continued



Caution

Do not use `chmod` recursively. It is very easy to make unintended changes to authorizations when doing so.

Additional Information for DB2 Common Server under UNIX

- R/3 Online Documentation: *BC SAP Database Administration: DB2 common server* [A.13]
- R/3 Online Documentation: *BC SAP Database Administration: DB2 common server* → *Managing Passwords of R/3 Admin Users* [A.14]
- IBM Documentation: *IBM DB2 Universal Database Administration Guide, IBM DB2 Universal Database Troubleshooting Guide* [E.9]

DB2 Common Server under Windows NT

The concept outlined here applies to Release 4.0B and later releases, and to Release 3.1I systems that are running with DB2/CS Version 5.0 and the SAP-DB2admin based on the DB2 Control Center.

General Information

R/3 work processes connect to the database server first as the user `<sid>adm` and then as user `sapr3`.

To authenticate the user, DB2 common server checks the local security database first. If the user is not found, it then checks in the security database of the Primary Domain Controller in the current domain. If the user is still not found, it continues to check in all trusted domains until either the user is located or all the security databases have been checked. If the user is located in a security database, the password and membership of a particular group, for example `SYSADM`, are checked using only the information in this security database. If the user is not found, access is refused.



Note

The search for a user in a security database always starts at the database server.

A user ID and password are required to establish a connection to the database.

The connection information (for example, the password) is provided as an encrypted string by a password service. Use the DB2 Control Center *Managing Passwords* function to manage the passwords of `<sid>adm` and `sapr3`.

The encrypted passwords for the users `<sid>adm` and `sapr3` are stored in the file `dscdb6.conf` during installation of the R/3 System. The stored passwords must match the passwords that are stored in the security database for the respective user.

You can find the file `dscdb6.conf` over the following path:

```
\\<%DSCDB6HOME%>\sapmnt\<SID>\SYS\global\dscdb6.conf
```

In an exclusively NT environment, the environment variable `DSCDB6HOME` contains the name of the database server.

In a system environment where the database server operates under an operating system other than NT, `DSCDB6HOME` should contain the name of a server where you can access the file `dscdb6.conf` via the above-mentioned path.

The environment variable `DB2DB6EKEY` holds the key for decoding the passwords. The value of this environment variable must be identical on all application servers, the central instance, and on the R/3 database server (all systems have the same `<SID>`). You can change this variable to another value as described in *Assigning Environment Variables*.



Note

Prior to DB2 Version 5, the environment variable used for encrypting and decrypting the password was called `DB6EKEY`. As of Version 5, the variable is now called `DB2DB6EKEY`. In the following discussion, we refer to it as `DB2DB6EKEY`.

Chapter 2 : The R/3 Security Toolbox

After authentication of the user by the database security process, a check is made to see in which database authorization groups the user belong. The Windows NT system groups `SYSADM` and `SYSCTRL` are used in combination with SAP R/3. Membership of these groups is only checked with the security database in which the user was located.

The assignment of the Windows NT system groups to the corresponding database groups is executed using parameters in the database instance. The parameter `SYSADM_GROUP` defines the database administration group, and `SYSCTRL_GROUP` is the database control group. In an R/3 environment, the parameter `SYSADM_GROUP` is set to `SYSADM` and the parameter `SYSCTRL_GROUP` to `SYSCTRL` during installation.

The measures that you need to take for a DB2 common server database under Windows NT, as well as additional information are provided in the following sections:

- **Assigning Users and Groups (DB2/CS / Windows NT)**
- **Managing the Passwords of the Database Standard Users (DB2/CS / Windows NT)**
- **Assigning Environment Variables (DB2/CS / Windows NT)**
- **Setting Access Privileges for Database-Related Files and Directories (DB2/CS / Windows NT)**
- **Useful Procedures for DB2 Common Server under Windows NT**
- **Additional Information on DB2 Common Server under Windows NT**

Assigning Users and Groups (DB2/CS / Windows NT)

Table 2-5-12 and Table 2-5-13 show the users and groups that are required when running an R/3 System with the DB2 common server database under Windows NT:

Table 2-5-12 : DB2/CS Standard Users under Windows NT (DB2/CS / Windows NT)

User	Function
<sid>adm	SAP system administrator
sapse<sid>	SAP service account
db2<sid>	database administrator
sapr3	user for R/3 database objects

Table 2-5-13 : DB2/CS Standard Groups under Windows NT (DB2/CS / Windows NT)

Group	Function
SAP_<SID>_GlobalAdmin	domain-level R/3 administration group
SAP_<SID>_LocalAdmin	local groups on an application server
SYSADM	Database system administrator group
SYSCTRL	Database system control group

User: SAP System Administrator (<sid>adm)

The SAP system administrator is the user who administers the R/3 System. This user also performs the installation procedure.

User: SAP Service Account (sapse<sid>)

The SAP service account user is a virtual user. You generally start the R/3 System with this user account. You do not log on to the R/3 System with this account. This user account must have the local user rights to *Log on as a service* and has to be a member of the local administrator group. The name of this user must be sapse<sid>.

Group: SAP <SID> GlobalAdmin

This global group is a domain-level R/3 administration group for organizing SAP system administrators. The sole function of a global group is to gather users together at domain level so that they can be placed in the appropriate local groups. The members of this group are the domain users <sid>adm and sapse<sid>.

**Note**

The group SAP_<SID>_GlobalAdmin is used only when the R/3 System belongs to an NT domain. You do not need the group SAP_<SID>_Global_Admin if you are installing locally.

Group: SAP <SID> LocalAdmin

Irrespective of the type of installation, you have to create the local group SAP_<SID>_LocalAdmin.

Only local groups are created and maintained on an application server. A local group can only be given permissions and rights to the system where it is located. If the system is part of the domain, the local group can contain users and global groups from the domain.

Working with or without a Domain Controller

If you are working **with** a domain controller, then note the following:

- The members of the group SAP_<SID>_LocalAdmin are the global group SAP_<SID>_GlobalAdmin, and on the database server, the domain user db2<sid>.
- The groups SYSADM and SYSCTRL are created on the domain controller.

If you are working **without** a domain controller, then note the following:

- The members of the group SAP_<SID>_LocalAdmin are the users <sid>adm, sapse<sid> and db2<sid>.
- The groups SYSADM and SYSCTRL are created locally.

**Note**

If all R/3 servers are domain controllers, then the local group exists at domain level and only has to be defined once for all domain controllers.

Managing the Passwords of the Database Standard Users (DB2/CS / Windows NT)

Table 2-5-14 shows the users for which you have to use the DB2 control center *Managing Passwords* function to change passwords. This is the only way to ensure user and password consistency within the R/3 environment. For more information see *BC SAP Database Administration: DB2 common server*.

Table 2-5-14 : Managing the Passwords for DB2/CS Standard Users (DB2/CS / Windows NT)

User	Type
<sid>adm	database user (SAP system administrator)
Sapr3	database user (R/3)

**Note**

If you inadvertently delete or destroy the file `dscdb6.conf`, you can recreate it. See UP 2-5-21.

Assigning Environment Variables (DB2/CS / Windows NT)

Table 2-5-15 shows the values of the environment variables as they are assigned in the installation procedures. We recommend that you keep these values with the exception of `DB2DB6EKEY`. You can change the value of `DB2DB6EKEY` at any time. However, changing the value of the environment variable `DB2DB6EKEY` is difficult and must be executed on every server in the R/3 System where a dialog process is running (all systems have the same <SID>). Also, because the NT system can be destroyed by incorrect entries in the Registry, only allow an experienced NT administrator to change it. For details, on how to change it, see UP 2-5-20.

Table 2-5-15 : Environment Variables for DB2/CS under Windows NT (DB2/CS / Windows NT)

Environment Variable	Value
DB2INSTANCE	DB2<SID>
DB2DBDFT	<SID>
DSCDB6HOME	<database server name>
DB2DB6EKEY	<SID><database server name> (default)

Setting Access Privileges for Database-Related Files and Directories (DB2/CS / Windows NT)

We recommend that you restrict the file and directory access privileges as shown in Table 2-5-16:

**Table 2-5-16 : Setting Access Privileges for DB2/CS Directories and Files
(DB2/CS / Windows NT)**

DB2 common server Directory	Access Privilege	for user/group
<drive>:\sqllib	<i>Full Control</i>	Administrators, SYSTEM, SAP_<SID>_LocalAdmin
<drive>:\sqllib\db2<sid>	<i>Full Control</i>	Administrators, SYSTEM, SAP_<SID>_LocalAdmin
<drive>:\db2<sid>	<i>Full Control</i>	SAP_<SID>_LocalAdmin, SYSTEM
<drive>:\db2	<i>Full Control</i>	Everyone
<drive>:\db2\<sid>	<i>Full Control</i>	SAP_<SID>_LocalAdmin, SYSTEM
<drive>:\db2\<sid>\sapdata*	<i>Full Control</i>	db2<sid>, SYSTEM
<drive>:\db2\<sid>\log_dir	<i>Full Control</i>	db2<sid>, SYSTEM
<drive>:\db2\<sid>\log_archive	<i>Full Control</i>	SAP_<SID>_LocalAdmin, SYSTEM
<drive>:\db2\<sid>\sapreorg	<i>Full Control</i>	SAP_<SID>_LocalAdmin, SYSTEM

Useful Procedures for DB2 Common Server under Windows NT

UP 2-5-19 : Recreating the File `dscdb6.conf` (DB2/CS / Windows NT)

To recreate `dscdb6.conf`, proceed as follows:

1. Log on to the database server as user `db2<sid>`.
2. Open a command line window.
3. Check whether the environment variables `DSCDB6HOME`, `DB2DB6EKEY`, `DB2INSTANCE` and `DB2DBDFT` are set correctly. You can display the current values with:

```
echo %<variable_name>%
```

4. Call the program `db6util.exe`:

```
db6util -c sapr3 <password1> <sid>adm <password2> <SID> <file>
```

where:

<code><password1></code> :	Password of the user <code>sapr3</code>
<code><password2></code> :	Password of the user <code><sid>adm</code>
<code><file></code> :	Name of a file in which the actions are logged.

5. Look in the log file to see whether or not the action was executed successfully.
6. Execute a connection test by executing the following command:

```
R3trans.exe -d
```

7. Look in the file `trans.log` in the local directory to see if errors occurred during this connection test.



Note

You can find `db6util.exe` in the following path:

```
\\<hostname>\sapmnt\<SID>\SYS\exe\run
```

where:

`<hostname>` is the name of the NT Server where the central instance was installed.

UP 2-5-20 : Changing the Environment Variable DB2DB6EKEY (DB2/CS / Windows NT)

To change DB2DB6EKEY, proceed as follows:

**Note**

If the users <sid>adm and db2<sid> are domain users, you only have to execute steps 6, 7, 8, and 9 once; otherwise, you have to repeat the steps on every host in the R/3 System.

1. Stop the R/3 System and all application servers.
2. Make a database back up.
3. Log on as the administrator.
4. Stop the SAP Service SAP<SID>_Instancenummer.
5. Change the value of DB2DB6EKEY in the NT system database with the program regedit.
 - a) Start regedit.exe.
 - b) Choose the key: HKEY_LOCAL_MACHINE\SOFTWARE\SAP\<SID>\Environment.
 - c) Select DB2DB6EKEY → Edit → Modify.
 - d) Set the new value.
 - e) Select OK.
6. Start the SAP Service SAP<SID>_Instancenummer.
7. Log off and log on again as user <sid>adm.
8. Call the program ntreg2env. This program is used to update the environment variables for the current user (now <sid>adm). If there are several R/3 Systems, select the correct <SID>.
9. Log off and log on again as user db2<sid>.
10. Call the program ntreg2env. This program is used to update the environment variables for the current user (now db2<sid>). If there are several R/3 Systems, select the correct <SID>.
11. Log off from the R/3 System.
12. On the server %DSCDB6HOME% only: Execute the above steps to update/create the file dscdb6.conf.
13. Start the R/3 System.

Additional Information on DB2 Common Server under Windows NT

For more information, refer to the following documentation:

- [R/3 Online Documentation: BC SAP Database Administration: DB2 common server \[A.13\]](#)
- [IBM Documentation: IBM DB2 Universal Database Administration Guide, IBM DB2 Universal Database Troubleshooting Guide \[E.9\]](#)

DB2/400

The OS/400 operating system provides a broad range of facilities for managing security objects. Access to objects (such as libraries and files) can be regulated by:

- Object Authorities
- User Profiles
- Group Profiles
- Authorization Lists

For detailed information on setting up system security, refer to the IBM books:

- *OS/400 Security - Basic* [E.10]
- *OS/400 Security - Reference* [E.11]

We describe the measures that you need to take for a DB2 database under AS400 in the following sections:

- **General Description of the DB2/400 Security Concept (DB/400)**
- **Changing the Passwords of Standard R/3 Users (DB2/400)**
- **Useful Procedures for Database Access Protection (DB2/400)**
- **Useful Procedures for DB2/400**
- **Additional Information for DB2/400**

General Description of the DB2/400 Security Concept (DB2/400)

Figure 2-5-1 shows the user security concept for R/3 on AS/400 at operating-system level:

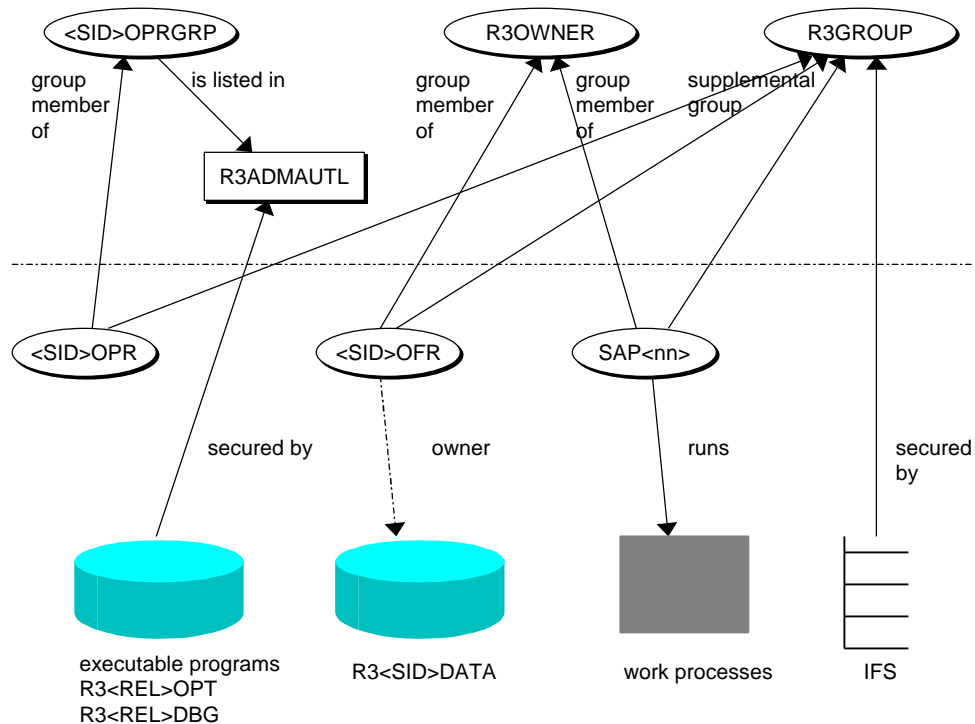


Figure 2-5-1: DB2/400 User Security Concept

We describe the individual user and group profiles below.

User Profiles

`<SID>OPR`

`<SID>OPR` (system operator) is the user profile of the R/3 System administrator. This user is only allowed to do administrative tasks, such as starting and stopping R/3 instances.

The commands `<SID>OPR` is allowed to use are listed as objects in the `R3TASKS` menu. `<SID>OPR` has no access to the contents of the database.

<SID>OFR

<SID>OFR (system officer) is the user profile of the R/3 System superuser. This user has all authorizations for the R/3 System and the R/3 database R3<SID>DATA. <SID>OFR can perform all the tasks that it is authorized to perform and it has certain additional rights. However, <SID>OFR has no special rights outside the R/3 environment. It also has no special rights to other R/3 Systems (with different SAP System IDs) that may run on the same AS/400. Note that <SID>OFR is not the same as QSECOFR, which is the superuser of the AS/400 system.

SAP<nn>

SAP<nn> runs the work processes. ("nn" represents the instance number.) The objects created by this user belong to the group R3OWNER.

Group Profiles

<SID>OPRGRP

<SID>OPRGRP is the group profile for <SID>OPR and thus allows the definition of multiple <SID>OPR users.

R3OWNER

R3OWNER is the default owner for the R/3 libraries and all R/3 System objects. It is not possible to sign on as R3OWNER. It is the group profile for <SID>OFR and SAP<nn>.

R3GROUP

R3GROUP is the primary group of the R/3 Integrated File System (IFS) objects. It is the supplemental group of all other R/3 generated user profiles. Its only purpose is to authorize R/3 users to IFS objects.

Superuser for AS/400

QSECOFR

QSECOFR is the superuser for AS/400. This user is not necessary to run and maintain the R/3 System. During installation of R/3, adopted authorities of QSECOFR are used (for creating the user profiles, for example).

Properties of Objects Created during R/3 Installation

The following applies to the objects created during the installation of R/3:

- They are owned by R3OWNER with the exception of the database library R3<SID>DATA, which is owned by <SID>OFR.
- IFS objects (directories and stream files) belong to the primary group R3GROUP.
- Public is always excluded. (No authorization is given to other users.)

Security Levels

The security level (QSECURITY) system value specifies the level of security to be enforced on the AS/400 system. Changes to this value take effect at next IPL (Initial Program Load).

The system offers five levels of security:

- **10** : No system-enforced security
- **20** : Sign-on security
- **30** : Sign-on and resource security
- **40** : Sign-on and resource security; integrity protection
- **50** : Sign-on and resource security; enhanced integrity protection

The AS/400 system is shipped at security level 40 which provides sign-on and resource security, as well as integrity protection. (The default level is 30 prior to V4R2).

If you want to change the security level, use the Work with System Values (WRKSYSVAL) command. You should use at least level 30 for operating R/3 and we recommend using the level 40. For more information, see "System Value QSECURITY" in Chapter 2 of the guide *Installing R/3 on IBM AS/400* [E.12].

Changing the Passwords for Database Standard Users (DB2/400)

Table 2-5-17 shows the users for which you need to change passwords, along with the tool used for the procedure. See UP 2-5-21 for the description on how to proceed with changing the passwords.

Table 2-5-17 : Changing the Passwords for DB2/400 Standard Users (DB2/400)

User	Function	Method used to change password or profile
<SID>OPR	R/3 System administrator	CHGPWD, CHGUSRPRF
<SID>OFR	R/3 System superuser	CHGPWD, CHGUSRPRF
SAP<nn>	user that runs the work processes	CHGUSRPRF

Note the following:

- To change user passwords use CHGPWD.
- To change user profiles use CHGUSRPRF.

**Note**

Change the initial passwords of <SID>OFR and <SID>OPR to protect your system against unwanted access!



Note

If you are using distributed directories on multiple AS/400s via /QfileSvr.400, you must use the same passwords on all the AS/400s for each of the users (<SID>OPR, <SID>OFR, and SAP<nn>).

On AS/400, the only user profiles apart from <SID>OFR that are allowed to access the database library R3<SID>DATA are the profiles R3SERVER and SAP<nn>. You cannot sign on with these user profiles.

Useful Procedures for DB2/400

UP 2-5-21 : Changing the passwords for <SID>OFR and <SID>OPR Using CHGPWD (DB2/400)

1. Sign on to the database server as user <SID>OFR.
2. Enter the CHGPWD command in the command line.
3. Enter the old and new passwords.

Repeat steps 1-3 for the user <SID>OPR.

Additional Information for DB2/400

For more information, refer to the following documentation:

- [R/3 Online Documentation: BC SAP Database Administration: DB2/400](#) [A.15]
- [IBM Documentation: OS/400 Security - Basic](#) [E.10]
- [IBM Documentation: OS/400 Security - Reference](#) [E.11]
- [IBM Documentation: Installing R/3 on IBM AS/400](#) [E.12]
- [IBM Documentation: SAP R/3 Implementation for AS/400](#), Material Number SG24-4672 [E.13]

Chapter 2-6 : Protecting Your Productive System (Change & Transport System)

To protect the integrity and availability of your productive system, we recommend that you separate your productive system from your development system. We recommend at least two R/3 Systems, and from a security point of view, we recommend three separate systems. With this landscape, you can thoroughly test your developments before making changes in your productive system.

The following topics pertain to protecting your productive system by separating your systems:

- **The R/3 System Landscape**
- **Configuring the System Landscape for Changes**
- **Defining the Transport Process**
- **Responsibilities and their Corresponding Authorizations in R/3**
- **Emergency Corrections in the Productive System**
- **Additional Information for the Change and Transport System**

The R/3 System Landscape

It is possible to develop, test, and run production within one R/3 System. However, to prevent development activities from interfering with your production system, we recommend that you separate your development system from your productive system. We suggest a three-tier system that consists of separate development, quality assurance, and productive systems. The three systems share a common transport directory. With this set-up, you can thoroughly make and test changes without interfering with your productive operations. Figure 2-6-1 shows the basic set-up for our recommended three-tier system landscape.



Note

As of Release 3.1H, the Transport Management System (TMS) is available (Transaction STMS) . With this tool, you no longer need to manually set-up the common transport directory and you can also start imports from within R/3. See the online documentation *BC Transport Management System [A.24]* for more information.

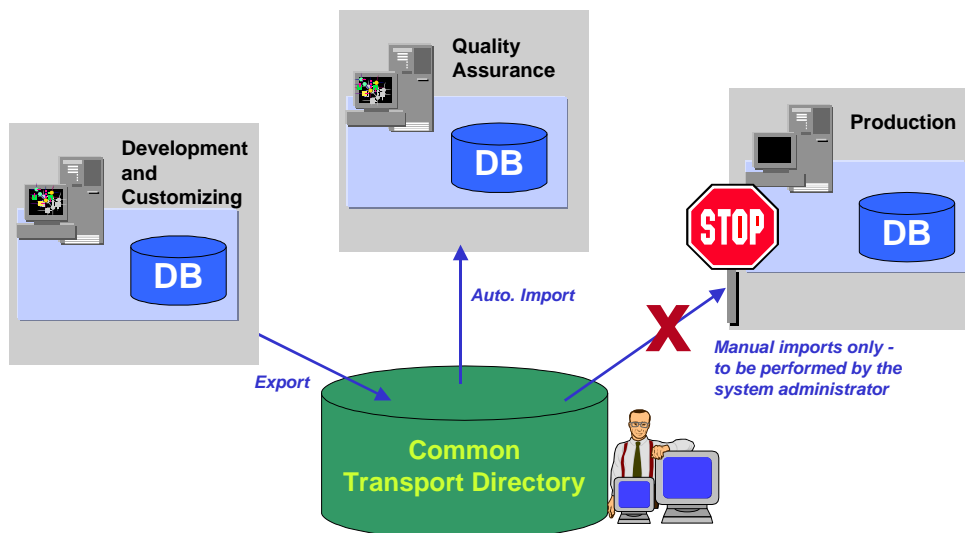


Figure 2-6-1: Recommended Three-Tier System Landscape

The Three-Tier System Landscape

With the three-tier system landscape, you make all of the changes to your system (to include Customizing) in a separate development system. You export these changes to a common transport directory. You then import these changes into a quality assurance system where you can thoroughly test them. Once you are satisfied that the changes are safe, you can then import them from the common transport directory into your productive system.

By following this recommendation, you provide for the following security measures:

- You ensure that changes take place in only one location, namely the development system.
- Your developers do not have access to productive data.

If you want to test with productive data, copy the subset of data that you want to use in the tests into the quality assurance system, and perform your tests there.

- You can thoroughly test changes in a separate quality assurance system before they take effect in your productive system.
- You control the point in time when changes take effect in the productive system.
- You can reduce accidental or unauthorized changes to productive data by controlling when, from whom, and from which systems transfers take place.
- You can keep a record of changes for tracing or auditing purposes.

Note

If you discover errors in the quality assurance system that result in the need to make further changes, we recommend that you make the changes in the development system and re-import them into the quality assurance system.

The Common Transport Directory

To store the data files between transports, we recommend you use the common transport directory as shown in Figure 2-6-1. The three systems use this directory for all exports and imports. All transports should run over this directory.

To protect the integrity, validity, and consistency of the data being transported, consider the following points:

- The common transport directory is generally mounted using NFS mount. To prevent misuse, place those systems that share the transport directory in a separate secure LAN (see *Chapter 2-3 : Network Infrastructure*.)
- Only the system administrator should be able to execute imports (using `tp` or `R3trans`).
- Archive the data in the transport directories so that you can review the transport activities if necessary. This is especially important for the transport logs and the `TPPARAM` configuration file (see OSS Note 41731 [C.14] or 41732 [C.15]).
- If you have several R/3 Systems, separate them into logically differentiated system landscapes.
- If you use TMS, you may want to consider using a separate transport directory for the productive system.

If you consider this option, then take the following points into account:

- You increase security by making it harder for unauthorized persons to import data into the productive system.
- However, you cannot start the import into the productive system within R/3. The system administrator (and we recommend only the system administrator) has to use `ftp` to initiate the import.
- You no longer receive the return values or logs in the export system.
- In addition, you also have to copy any transport files from Hot Packages into both directories.

Configuring the System Landscape for Changes

You need to define the changes that are allowed in each of the individual systems that you have in your complete system set-up (use Transaction SE06). Use the Transaction SE03 to view the settings. There are differences in the configuration possibilities between the Releases 3.0/3.1 and Release 4.0. Therefore, we discuss them separately in the following sections.

Releases 3.0/3.1

In the Releases 3.0 and 3.1, you can set the following change options:

- *Objects cannot be changed*

We recommend this setting for the productive system.

- *Only original objects (with correction system)*

You can only change the objects if the original is in the system.

Chapter 2 : The R/3 Security Toolbox

- *All customer objects (with correction system)*

With this setting, you can make repairs to customer objects, even if the original exists in another system.

- *All objects (with correction system)*

You need this setting if you need to modify or repair objects from the SAP standard. This setting also includes the full scope of changes to customer objects.

For more information, see the online documentation *BC Transport System → Setting up the Workbench Organizer and the Transport System → Setting the System Change Option [A.26]*.

Release 4.0

In Release 4.0, you can set the following change options in Transaction SE06:

- Repository and Client-Independent Customizing not modifiable

You cannot change any objects. We recommend this setting for productive systems.

- Repository and Client-Independent Customizing modifiable

You can change objects according to the specific settings for each namespace.

For modifiable systems, you have to define to what extent you can make changes for each namespace. You can:

- Allow changes to all objects (Choose: *Edit → Select all*)

With this setting, you can modify or repair objects from the SAP standard. This also includes the full scope of changes to customer objects.

- Allow changes to your own objects only (Choose: *Edit → Select all own*)

With this setting, you can modify all of your own objects. (Own objects are objects belonging to namespaces with a producer role. If you use this setting, then these namespaces are marked as changeable.)

- Assign changes for each namespace individually.

With this setting, you can change all objects belonging to namespaces that are set to changeable.

For more information, see the online documentation *BC Change and Transport Organizer → Setting up the System Group → Setting the System Change Option [A.26]*.

Defining the Transport Process

In addition to setting the change options, you also need to define the transport process. You need to determine how you bring changes from your development successfully into your productive system. This involves defining the transport path (the series of systems) and defining the process itself (the series of exports and imports).

The Transport Path

As with the change options, you define the transport path in the Transaction SE06. You enter the systems that exist in your landscape and, in addition to their change options, you define which systems transport to and from other systems. You must also enter this transport path in the `TPPARAM` file. (Change this file at the operating system level.)

The Transport Process

Not only do you need to define the transport path, you also need to define the process used for transports. This is more an organizational measure than a technical measure that consists of determining who performs which tasks. In this section, we briefly describe the technical transport process in R/3 and the next section, *Responsibilities and their Corresponding Authorizations*, explains more about the roles and responsibilities that apply.

In general, the following steps list the individual activities involved in the transport process in R/3. (Note that we do not define the corresponding roles here. You need to define your roles yourself.)

The Transport Process in R/3:

1. Release the change request to transport in Transaction SE09 or SE10.

Based on the change request, the Workbench Organizer generates files that reside in a common transport directory at the operating system level. It also generates a control file, data file, and log file for each released and exported change request.

2. Review the log files to ensure that the export was successful. If there were errors, you need to correct them before continuing.
3. Import the R/3 objects into the database of the target system. Here, you must use the operating system command `tp`.

You can use automatic import for imports into the quality assurance system; however, not for imports into the productive system.

Again, the Workbench Organizer displays log files that you should review.

4. Test your imports thoroughly. If errors occur, repair the objects in the source system and re-export them into the quality assurance system.

5. If additional systems exist in the complete system landscape, then you need to import the objects into the other systems as well. This is normally not done automatically and you need to use the `tp` command at the operating system level. You should review all of the generated log reports to ensure that no errors occurred.

**Note**

You can access the log files with the Workbench Organizer (Request Hierarchy).

Responsibilities and their Corresponding Authorizations in R/3

For your changes and transports to successfully take effect in your productive system, you need to have a well-organized administration team with defined roles and responsibilities. Changes to the productive system should not be the responsibility of one single person. You should define and document the various roles and corresponding activities. The communication flow between the individuals in these roles should also be well defined and practiced.

In this section, we discuss the responsibilities that apply to the transport process and their corresponding authorizations in R/3. The roles we discuss here are suggestions based on the architecture of the process as defined in R/3. You may have to adjust them accordingly to apply them to your needs.

For example, we suggest that you distribute the roles between the following individuals:

- **Team Members / Developers**

Team members are responsible for releasing their own tasks in the Workbench Organizer.

- **The Project Leader**

The project leader is responsible for tasks such as:

- Defining and organizing a project using change request management
- Verifying the contents of a change request prior to release

(For example, ensuring that syntax checks have been performed for all objects with Transaction SE09.)

- Confirming the success of the release/export
- Verifying that the change request was successfully imported
- Confirming that the imported change request contained necessary objects and proper functionality

- **The Administrator**

The administrator is responsible for the operating system task of transporting. He or she issues the appropriate `tp` commands to activate the import of change requests and verify the success of an import. The administrator is not responsible for testing the contents of a change request.

- **The Quality Assurance (QA) Team**

The QA Team tests the entire functionality and integration of the individual components from the change request in the quality assurance system.

Chapter 2-6 : Protecting Your Productive System (Change & Transport System)

Table 2-6-1 shows the corresponding pre-defined authorizations in R/3 that apply to the various roles (the corresponding objects include S_CTS_ADMI and S_TRANSPRT).

Table 2-6-1 : Authorization Profiles for Change and Transport Roles

Role	Authorization Profile
Quality Assurance (QA) Team	not pre-defined in R/3
Administrator (Transport superuser)	S_CTS_ALL
Project Leader	S_CTS_PROJEC
Team Members / Developers	S_CTS_DEVELO
End Users	S_CTS_SHOW

Emergency Changes in the Productive System

Generally, users should not have programming, debugging with replace, or transport authorizations in your productive system. As previously mentioned, changes should occur in a single system, namely the development system. Table 2-6-2 shows those authorizations that apply to development and transport, which you should **not** give to users in your productive system.

Table 2-6-2 : Authorizations for Development and Transport

Authorization Object	Purpose	Comment
S_ADMI_FCD	Executing Operating System Commands from within R/3 (Transaction SM52)	<ul style="list-style-type: none"> with REPL value
S_DEVELOP	ABAP Workbench authorizations (programming and debugging - Transactions SExx)	<ul style="list-style-type: none"> with activity 02 (change) development object type PROG and DEBUG
S_TRANSPRT	Change and Transport authorizations	

For more information on debugging authorizations, see the OSS Notes 52937 [C.20] and 65968 [C.24].



Caution

If you do have to make emergency changes in the productive system, define a procedure to make the changes where you have supervised control over what happens. Give a single user temporary authorizations for the Transaction SE38 and make sure that someone approves these changes. Once the user has made the changes, remove the authorization!

Additional Information for Change & Transport System

For more information, refer to the following documentation:

- [R/3 Online Documentation: BC Transport System \(3.0/3.1\)](#) [A.25]
- [R/3 Online Documentation: BC Change and Transport Organizer \(4.0\)](#) [A.3]
- [R/3 Online Documentation: BC Transport Control](#) [A.23]
- [R/3 Online Documentation: BC Transport Management System](#) [A.24]
- [R/3 Online Documentation: BC Transport System → Setting up the Workbench Organizer and the Transport System → Setting the System Change Option](#) [A.26]
- [OSS Note 13202](#): Security Aspects in ABAP Programming [C.6]
- [OSS Note 41731](#): Deletion of data in transport directory (2.1/2.2) [C.14]
- [OSS Note 41732](#): Deletion of data in transport directory (3.0) [C.15]
- [OSS Note 27928](#): Consequences in transport during password change [C.7]
- [OSS Note 52937](#): Debugging authorizations (Releases 3.0A to 3.0F!) [C.20]
- [OSS Note 65968](#): ABAP debugging authorizations as of Release 3.1G [C.24]

Chapter 2-7 : Remote Communications (RFC & CPI-C)

The Remote Function Call (RFC) and CPI-C interface are techniques that you can use for communicating between SAP R/3 Systems and external systems or modules.

RFC enables applications to call SAP function modules that are located on other systems, and the CPI-C interface allows for program-to-program communication between SAP Systems and external programs or systems.

There are several security measures that you should take when using RFC or CPI-C communications in your R/3 System. We describe these measures in the following sections:

- **General Security Measures**
- **RFC Authorizations**
- **Trusted System Networks (RFC)**
- **Authorizations for External Server Programs (RFC & CPI-C)**
- **Secure Network Communications for Remote Communications (RFC & CPI-C)**
- **Additional Information for Remote Communications**

General Security Measures

As already stated, RFC is a technique for enabling both SAP and external applications to call SAP function modules that are located on other systems. RFC is an important means of communication in the R/3 System landscape. We offer a number of interfaces that rely on RFC for their communications (for example, ALE, BAPIs, and the RFC function modules themselves). We recommend that you use these pre-defined interfaces to access the database for business processing actions that involve dependencies instead of accessing the database directly. For more information, see the Interface Advisor in SAPNet. (See *Service* → *index* → *Interface Advisor*.)

The RFC interface exists for either R/3 and R/2 Systems, or for non-SAP systems:

- **ABAP interface (R/3 and R/2 Systems)**

An ABAP program can call a remote function with the CALL FUNCTION... DESTINATION statement. The DESTINATION parameter indicates the system where the function called is located. If the destination system is an R/3 System, then the function module called must be an ABAP function module that has been marked as "remote" in the function library.

- Remote functions can be called either synchronously or asynchronously.
- Remote debugging is also possible for communications with an R/3 System as destination (as of Release 3.0C).

- **RFC-API: The calling interface for external programs (non SAP systems)**

If either the calling partner or the called partner is not an ABAP program, then it must be programmed as a RFC communication partner. The R/3 System is shipped with the RFC-API (Application Programming Interface). You can install the SAP library in external systems to support the development of RFC partner programs.

Security Aspects

To ensure that your RFC or CPI-C connections operate securely, consider the following points and take the appropriate measures:

- Allow RFC access from known and designated systems only.

Systems that you allow to communicate with one another using RFC should be protected by the appropriate network measures (see *Chapter 2-3 : Network Infrastructure*). Either keep systems in a self-contained secure LAN, or control access using SAProuters and packet-filters.

- RFC connection requests are authenticated in R/3 using the standard password mechanism. (The user making the RFC request must remotely log on to the target system with a user-id and password.)
- Include authority checks in your own function modules that can be called using RFC.
- Restrict authorizations for maintaining RFC destinations (Transaction SM59). With the Transaction SM59, a user can remotely logon to an RFC destination (if the user in the target system is a DIALOG user).

The necessary authorization objects are S_ADMI_FCD with the value NADM and S_TCODE with the value SM59.

- Restrict access to the table RFCDES.

The RFC users and passwords are stored in this table, encrypted with a static key. However, note that R/3 itself can decrypt the passwords. Therefore, restrict access to this table.

You should not store DIALOG users' information in this table. R/3 requests the DIALOG user's login information at the time of connection. Give only minimal rights to CPIC users in target systems.

- See OSS Note 43417 [C.16] to find out how to prevent misuse of the RFC Software Development Kit.
- Do not install the RFC Software Development Kit in your productive system, neither on your application servers nor on your front ends.
- Restrict possible external CPI-C or RFC server programs by making entries in the `secinfo` file (see the section titled *Authorizations for External Server Programs (RFC and CPI-C)*).
- Disable remote monitoring of your SAP Gateways by setting the profile parameter `gw/monitor` to 1 (see OSS Note 64016 [C.23]).
- As of Release 4.0, you can apply Secure Network Communications (SNC) protection to RFC calls and CPI-C connections.

RFC Authorizations

When assigning RFC authorizations to users in R/3, you need to consider the following points:

- The necessary authorization object for using RFC is S_RFC.
- The user in the target system needs to have this object in his or her authorization profile to be able to connect to the target system using RFC.
- The RFC function modules are divided into specific groups. When assigning the authorization profile, you specify which function groups the user is allowed to call.
- Use trace functions to determine which function groups are necessary for a specific connection.
- Be restrictive when assigning these groups to users.

Trusted System Networks (RFC)

In a trusted system scenario, servers in one system 'trust' servers from another system. Users from the first system (System A) that access the second system (System B) are not authenticated over passwords with every access request. System B trusts System A, and because of this trusting relationship, System B accepts the user from System A without further authentication. The user must have accounts in both systems, and he or she receives the authorizations from the target system, in this case, System B.

The advantage to this system is that users do not have to continually authenticate themselves when communicating with trusted systems. You save on the transmission of logon information over the network.

However, in order for trusted systems to securely operate, you need to maintain the following requirements, which involve higher administration costs:

- The systems need to have the same security-level requirements. (They consequently form a 'virtual' single R/3 System.)
- The systems need to have the same user administration. (All users need to exist in both systems and with the same rights in both systems.)

If you can meet these requirements, then you might consider establishing a trusted system scenario.

Authorizations for External Server Programs (RFC and CPI-C)

The authorizations for external server programs are controlled by the SAP gateway. Either you can allow external server programs to be started over the gateway, or you can allow them to register themselves on the gateway. The security information that the gateway needs to allow the starting or registration of the external server programs is stored in a file called `secinfo`. You can find this file in the path designated in the profile parameter `gw/sec_info`; the standard value is `/usr/sap/<SID>/<instance>/data/secinfo`.



Note

If this file does not exist, then there are **no** restrictions applied to the starting or registration of external server programs. We recommend that you use and maintain this file!

To define the authorizations for starting or registering external programs, modify the `secinfo` file by entering the information indicated in the following:

- **Authorizations for Starting External Server Programs:**

Enter the following line to allow a particular R/3 user `<R/3_user>` to start a particular external server program `<ext_program>` on a particular computer `<server_host>`.

```
USER=<R/3_user>, [PWD=<CPIC_pwd>], [USER-HOST=<client_host>], HOST=<server_host>,
TP=<ext_program>;
```

The parameter `<client_host>` is an optional parameter where you can specify from which client the user must log on to the gateway to start the external server program.

The parameter `<CPIC_pwd>` is an optional parameter for CPI-C calls only, where you can specify a password for the connection. (To set passwords in your own CPI-C developments, use the function module `CMSCSP`.)

- **Authorizations for Registering External Programs on the SAP Gateway:**

Enter the following line to allow a particular server program on the server host `<server_host>` to register itself on the SAP gateway under the program ID `<program_ID>`:

```
USER=*, HOST=<server_host>, TP=<program_ID>;
```

You must always specify `USER=*`, although this parameter is not further used.

With this method, you specify which server programs can register themselves on a SAP gateway.

- If you want to allow external operating system commands or the execution of external programs within batch jobsteps over the gateway, then include an entry for the program `sapxpg` in the `secinfo` file.

You can find more information on configuring the gateway in the following online documentation: *BC SAP Communication: Configuration Guide* → *SAP Gateway* [A.9].

As previously mentioned, as of Release 4.0, you can apply Secure Network Communications (SNC) protection to RFC calls and CPI-C connections. This also applies to the starting or registration of external server programs.

Secure Network Communications for Remote Communications

Secure Network Communication (SNC) uses an external security product to apply additional protection to the communication paths between distributed R/3 components. As of Release 4.0, you can apply SNC protection, which can include encryption, to both RFC and CPI-C connections. For more information, see *Chapter 2-3 : Network Infrastructure* in the section titled *Secure Network Communications (SNC)*.

Additional Information on Remote Communications

For more information, refer to the following documentation:

- [R/3 Online Documentation: Remote Communications](#) [A.33]
- [R/3 Online Documentation: BC SAP Communication: Configuration Guide → SAP Gateway](#) [A.9]
- [R/3 Online Documentation: BC SAP Communication: CPI-C Programmer's Guide](#) [A.10]
- [OSS Note 43417](#): RFC security loophole in 3.0C and 3.0D [C.16]
- [OSS Note 63930](#): Gateway registration of RFC server program [C.22]
- [OSS Note 64016](#): Use of the SAP gateway monitor GWMON [C.23]
- [SAP Documentation: SNC User's Guide](#) [E.6]

Chapter 2-8 : Secure Store & Forward Mechanisms (SSF) and Digital Signatures

As of Release 4.0, R/3 offers the Secure Store & Forward Mechanisms (SSF) as internal means to protect arbitrary data in the R/3 System. R/3 applications can use the SSF mechanisms to secure data integrity, authenticity and confidentiality. The data is protected even if it leaves the R/3 System. The first applications that use SSF include:

- Production Planing - Process Industry
- Product Data Management
- ArchiveLink II

With time, more and more applications will use SSF for their security purposes.

In the following, we will discuss the global aspect of SSF. This background will help you understand the use of SSF in the application context. For further details, refer to the documentation pertaining to the application.

SSF uses **digital signatures** and **digital envelopes** to secure the data. The digital signature uniquely identifies the signer, is not forgeable, and protects the integrity of the data. (Any changes in the data after being signed result in an invalid digital signature for the altered data.) The digital envelope ensures that the contents of the data are only visible to the intended recipient.

SSF requires the use of a security product to perform its functions. As of Release 4.5, R/3 is shipped with SAPSECULIB (SAP Security Library) as the default SSF service provider. SAPSECULIB is a software solution with functionality that is limited to digital signatures. For support of crypto hardware (for example, smart cards, crypto boxes, etc.) or digital envelopes, you need a SAP-certified external security product.

In the following discussion, we refer to SSF in the general context, followed by the description of the special aspects of the SAPSECULIB.

Digital signatures are based on public-key technology. To successfully use digital signatures, a public-key infrastructure (PKI) must be established. Because there is not yet a worldwide PKI available, you have to either establish your own or rely on a Trust Center as a PKI service provider. Establishing your own local PKI for a very limited number of users only may or may not be easy, depending on the external security product that you use. Even if establishing a local PKI is relatively easy, the process of linking the PKI to your customers and business partners may involve a much greater effort. For you and your partners to agree on a common Trust Center, you can solve many of the PKI problems.

Regardless of your infrastructure, you need to take precautions in protecting the private keys. Each participant that uses the digital signatures and envelopes needs to own a key pair (public and private key). This includes system components such as the R/3 application servers, if they act as signers. There are certain measures that you need to take to protect these keys pairs. We describe these measures in the following sections:

- **Protecting Private Keys**
- **Protecting Public Keys**
- **SAP Security Library (SAPSECULIB)**
- **Additional Information for SSF and Digital Signatures**

**Note**

There are also laws in various countries that regulate the use of cryptography and digital signatures. These laws are currently controversial and may change. You need keep yourself informed on the impact these laws may have on your applications, and make sure that you are aware of any further developments.

Protecting Private Keys

There are two methods of storing the private keys. They are:

- Hardware solutions (for example, smart cards or crypto boxes)
- Software solutions (for example, PSE or PKCS#12)

Hardware Solutions

The best protection of the R/3 users' private keys is a smart card that you issue to each individual user. There is no way to reveal the private key from the smart card. The user has to authenticate him or herself to his or her smart card, either using biometrics (for example, a fingerprint) or knowledge (for example, a PIN, password or passphrase entry). Nevertheless, each user needs to protect his or her smart card from theft or loss.

**Caution**

Do not allow your users to share smart cards or give them to others to use!

On the server side, you can use a crypto box instead of a smart card for higher performance.

Software Solutions

As an alternative, you can also use a software solution to store the users' private keys. You should be aware that the software solution is not as safe as the use of crypto hardware, however, less expensive to implement. If you use a file to store the user's information and private key, then you need to take extra care in ensuring that the file is protected from any access by an attacker.

Protecting Public Keys

If the security product uses an address book to store the public keys instead of certificates, then you need to protect the address book from unauthorized modifications.

As an alternative, you can use certificates that are signed by a trusted Certification Authority (CA) to ensure the authenticity of the public keys.

SAP Security Library (SAPSECULIB)

As of Release 4.5, R/3 offers the SAPSECULIB as the default security service provider for the SSF API. The functionality of the SAPSECULIB is limited to digital signatures and certificate management. Confidentiality (encryption / decryption) and the use of crypto hardware are not supported. For those purposes, you need to use an external security product.

The SAPSECULIB is a part of each R/3 application server. At startup, the application server looks for its own (personal) security environment (PSE) . If no PSE is found (for example, at the first startup), the application server generates its own PSE.

This automated generation process is responsible for protecting the application server's PSE. The following sections provide you with details to verify the correctness of that process.

Protection of the R/3 Application Servers' Private Keys

Each R/3 application server owns a public/private key pair. The private key is contained in the file `SAPSECU.pse` in the subdirectory `sec` of the directory specified by the profile parameter `DIR-INSTANCE`. Only the user running the application server process (for example, `<sid>adm`) is allowed to access the files in the `sec` directory.



Caution

It is very important to protect this file from being read or copied by unauthorized persons! An attacker who manages to copy this file has access to the R/3 application server's private key can proceed to use it to produce digital signatures that belong to the application server.

If you have reasons to believe that the application server's private key has been compromised, you should delete the files in the `sec` directory (do not forget to backup). During the next startup, the application server will generate a new PSE with a new key pair.



Caution

If any other application (for example, the archive using the ArchiveLink II interface) is using the R/3 application server's public key, and you replace it with a new one, then you have to publish the new application server's public key to that application. For details, refer to the application's documentation.

If you want to disable SAPSECULIB support for a R/3 application server, you can place an arbitrary file with the name `SAPSECU.pse` in the `sec` directory. This will prevent the automatic PSE generation during startup of the application server. To re-enable SAPSECULIB support, delete the file and the application server will generate a new PSE during next startup.



Caution

If you disable SAPSECULIB support for a R/3 application server and an application (for example, the ArchiveLink II interface) tries to use it, it will fail.

Protecting the R/3 Application Servers' Public Keys

The R/3 application servers are featured with an automatic PSE generation. A public-key certificate is generated, but it is self-signed (signed with the application server's private key) instead of being signed by a Certification Authority (CA).

Self-Signed Certificates

If you use self-signed certificates (for example, the application server signs its own certificate, as with archive requests with ArchiveLink II), then the receiver of the certificate should explicitly validate it before accepting it for the first time.

CA Signed Certificates

As an alternative, you can use certificates that have been signed by a CA. If the receiver trusts the CA, then the system can automatically verify the certificate. This automated verification process depends on the external security product that you use and can also require many preconditions. For more information, see the documentation provided by the product vendor.

Additional Information on SSF and Digital Signatures

- [SAP Documentation: Secure Network Communications and Secure Store & Forward Mechanisms with the SAP R/3 System](#); Material Number: 50014335 [E.7]
- [OSS Note 86927](#): Use of the digital signature in the R/3 System [C.30]
- [OSS Note 66687](#): Use of network security products [C.25]
- [OSS Note 110600](#): SAP Security Library (SAPSECULIB) [C.32]

Chapter 2-9 : Logging and Auditing

R/3 keeps a variety of logs for system administration, monitoring, problem solving, and auditing purposes. Logs and audits are important for monitoring the security of your system and to track events in case of problems.

In this guide, we discuss the importance and uses of the following auditing tools and logs. Sources of additional information are also included.

- **The Audit Info System (AIS)**
- **The Security Audit Log**
- **The System Log**
- **Statistic Records in CCMS**
- **Logging of Specific Activities**
 - Application Logging
 - Workflow Execution Logging
 - Logging Changes to Business Objects
 - Logging Changes to Tables
 - Logging Changes to User Master Records, Profiles, and Authorizations
- **Additional Information for Logging and Auditing**

The Audit Info System (AIS)

The Audit Info System (AIS) is an auditing tool that you can use to analyze security aspects of your R/3 System in detail. AIS presents its information in the Audit Info Structure (similar to IMG) so that you can easily determine which activities you need to perform and which you have accomplished. The following functions are available:

- Auditing procedures and documentation
- Auditing evaluations
- Audit data downloads

An auditor (or system administrator) can use AIS to check the security of your R/3 System. AIS is useful for the following types of audits:

- Ongoing controlling
- Interim audits
- Preparation of year-end closing statements

AIS is designed for business audits and systems audits. The Audit Info Structure is designed with these types of audits in mind and we deliver pre-defined views based on these auditing types. You can modify these views or develop your own, as you wish.

You access AIS with the Transaction SECR.

AIS is available as a standard component as of Releases 3.1I. We do support the import of AIS into other releases (as of 3.0D). For more information on AIS and its availability, see the OSS Notes 77503 [C.28] and 100609 [C.33].

The Security Audit Log

As of Release 4.0, you can use the Security Audit Log to record security-related system information such as changes to user master records or unsuccessful log-on attempts. This log is a tool designed for auditors who need to take a detailed look at what occurs in the SAP R/3 System. By activating the audit log, you keep a record of those activities that you specify for your audit. You can then access this information for evaluation in the form of an audit analysis report.

The security audit log provides for long-term data access. The audit files are retained until you explicitly delete them. Currently, the security audit log does not support the automatic archiving of the log files; however, you can manually archive them at any time.

You can record the following information in the Security Audit Log:

- successful and unsuccessful dialog log-on attempts
- successful and unsuccessful RFC log-on attempts
- RFC calls to function modules
- changes to User Master Records
- successful and unsuccessful transaction starts
- changes to the audit configuration

The audit files are located on the individual application servers. You specify the location of the files and their maximum size in the following profile parameters:

Table 2-9-1 : Profile Parameters for the Security Audit Log

Profile Parameter	Definition	Standard or Default Value
rsau/enable	Activates the audit log on an application server.	Default Value: 0 (audit log is not activated)
rsau/local/file	Specifies the location of the audit log on the application server.	Standard Value: /usr/sap/<SID>/<instno>/log/ audit_<SAP_instance_number>
rsau/max_diskspace_local	Specifies the maximum length of the audit log.	Default Value: 1,000,000 bytes
rsau/selection_slots	Specifies the number of selection slots for the audit.	Default Value: 2

You specify the activities that you want to log in the Transaction SM19. You can read the log with Transaction SM20. You can delete old logs with the Transaction SM18.

For more information on the Security Audit Log, see the online documentation *BC System Services → The Security Audit Log* [A.21].

System Log

The R/3 System logs all system errors, warnings, user locks due to failed log-on attempts from known users, and process messages in the system log (SysLog). The SysLog writes to two different types of logs:

- **Local Logs**
- **Central Logs**

Use the Transaction SM21 to access the system log output screen. With this transaction, you can read any of the messages that are contained in the system logs. You can modify the view to meet your needs.

Local Logs

Each R/3 Application Server has a local log that receives all the messages output by this server. SysLog records these messages in a circular file on the server. When this log file reaches the maximum permissible length, SysLog overwrites it, starting over from the beginning. (The location of the local log is specified in the `rslg/local/file` profile parameter.)

Central Logs

We recommend that you also maintain a central log file on a selected application server. Each individual application server then sends its local log messages to this server. The server that you designate to maintain the central log collects the messages from the other application servers and writes these messages to the central log.

The central log consists of two files: the active file and the old file. (The location of the active file is specified in the `rslg/central/file` profile parameter; the location of the old file is specified in the `rslg/central/old_file`.)

The active file contains the current log. When it reaches the maximum size, the system performs a "log file switch". It deletes the old log file, makes the previously active file the 'old' file, and creates a new active file. The switch occurs when the size of the active log file is half the value as specified in the `rslg/max_diskspace/central` parameter. (Note: R/3 does not support the saving of old system log files. If you want to save old logs, then you must archive them yourself.)

**Note**

If you use Windows NT or AS/400, then note the following:

- Central logging is not available on the Windows NT and AS/400 platforms.
- Per default, the profile parameter `rslg/collect_daemon/host` should be set correctly. However, if you receive warnings, then make sure that this parameter is set to NONE.
- For these platforms, you can use the *All remote syslogs* function from Transaction SM21 to read the data of all the instances in your R/3 System. In the alert monitor, if you receive an alert, you can use the *Remote syslog* function to analyze the affected instance.

Profile Parameters and File Locations

Table 2-9-2 shows some of the profile parameters for the system log along with their standard values:

Table 2-9-2 : Profile Parameters and File Locations for the System Log

Profile Parameter	Definition	Standard or Default Value
<code>rslg/local/file</code>	Specifies the location of the local log on the application server.	Standard Value: <code>/usr/sap/<SID>/D20/log/SLOG<SAP-instance_number></code>
<code>rslg/collect_daemon/host</code>	Specifies the application server that maintains the central log.	Default Value: <code><hostname of main instance></code>
<code>rslg/central/file</code>	Specifies the location of the active file for the central log on the application server.	Standard Value: <code>/usr/sap/<SID>/SYS/global/SLOGJ</code>
<code>rslg/central/old_file</code>	Specifies the location of the old file for the central log on the application server.	Standard Value: <code>/usr/sap/<SID>/SYS/global/SLOGJO</code>
<code>rslg/max_diskspace_local</code>	Specifies the maximum length of the local log.	Default Value: 500,000 bytes
<code>rslg/max_diskspace_central</code>	Specifies the maximum length of the central log.	Default Value: 2,000,000 bytes

**Note**

This is not a complete list. There are additional profile parameters that refer to the system logs; they all begin with `rslg*`. However, we do not discuss them all here. You can use the Transaction RZ11 to access the rest of the parameters.

For more information, see the online documentation *BC System Services* → *The System Log* [A.22].

Statistic Records in CCMS

The R/3 System logs R/3 activities, categorized by transaction and user, in statistical records. You can access these records with the Transaction STAT.

Statistic records logging is controlled by the following profile parameters described in Table 2-9-3:

Table 2-9-3 : Profile Parameters for Statistic Records in CCMS

Parameter	Description	Default	Permitted value
stat/level	Sets statistic record on or off	1	0 : off 1 : on
stat/version	Version of statistic record	2	1 : as in Release 2.2 2 : additional RFC statistics and memory usage statistics
stat/file	Location of the statistic records file	\usr\sap\ <sid>\<instance>\data\stat.DAT</sid>	path name

Users who access global statistic records need an authorization based on the object S_TOOLS_EX in their profiles. Without this authorization, a user can only access his or her statistic records.

For more information, see the online documentation: *BC Computing Center Management System → R/3 Accounting Interface → Available Statistics Data [A.5]*.

Logging of Specific Activities

R/3 logs other specific activities in various logs. We discuss the following specific logs below:

- **Application Logging**
- **Logging Workflow Execution**
- **Logging Using Change Documents (Changes to Business Data Objects)**
- **Logging Changes to Table Data**
- **Logging Changes to User Master Records, Profiles, and Authorizations**



Caution

A user with programming or debugging authorizations can evade these logs. Do not assign these authorizations in your productive system!

Application Logging

Application logging records the progress of the execution of an application so that you can reconstruct it later if necessary. Whereas the system log logs system events, you can use the application log to record application-specific events. Use the Transaction SLG0 to define entries for your own applications in the application log. Use the Transaction SLG1 to analyze the application log.

The application log is a table structure consisting of several tables. Applications write their entries to these tables over R/3 function modules. (These modules conform to the R/3 authorization concept.)

You can also find out who accessed these function modules over a where-used list by using the Report RSFKT100 (function group: SLG0).

For more information, see the online documentation *ABAP Development Workbench* → *Extended Applications Function Library* → *Create application log* [A.8].

Logging Workflow Execution

SAP Business Workflow is a cross-application tool that integrates transactions that span various applications.

The technology and tools needed to automate the control and processing of cross-application processes are included in the SAP Business Workflow functions, to include logging and analysis functions. These activities are not included in application logging.

The SAP Business Workflow analysis functions (such as the transactions SWI2 or SWI5) are also protected by the R/3 authorization concept.

For more information, see the online documentation *BC Business Engineering Workbench* → *SAP Business Workflow* [A.34].

Logging Using Change Documents

Business data objects are changed frequently. We recommend that you log these changes for objects that are critical or susceptible to audits. You may find it helpful, and sometimes necessary, to be able to trace or reconstruct such changes later, for example for investigating or auditing purposes. R/3 logs changes to business data objects in **change documents**.

R/3 does not automatically use change documents for business objects. You must activate the process yourself.

To activate a change document for an object, you have to perform the following steps:

1. Create the change document. (Use the Transaction SCD0.)
2. Activate the change document for the object. (Use data element maintenance: Transaction SE11.)
3. Generate an update for the object. (Again, use the Transaction SCD0.)
4. Insert the appropriate calls in the corresponding programs.

To view change documents for an object, also use the Transaction SCD0.

For more information, see *BC Extended Applications Function Library* → *Change documents* [A.7] and *BC ABAP Dictionary (Maintaining ABAP Dictionary Objects)* [A.1].

Logging Changes to Table Data

As with business objects, we recommend that you activate the logging of table data for those tables that are critical or susceptible to audits. Again, you must explicitly activate this logging. Note the following:

- You must start the R/3 System with the `rec/client` profile parameter set. This parameter specifies whether R/3 logs for all clients or only specific clients. We recommend setting this parameter to log all clients in your productive system.
- Set the *Log data changes* flag for those tables that you want to have logged.

If both of these conditions are met, the database logs table changes in the table DBTABPRT. (Setting the *Log data changes* flag only does not suffice in recording table changes; you must also set the `rec/client` parameter.)

You can view these logs with the Transaction SCU3.

For more information, see the OSS Note 1916 [C.1].

Logging Changes to User Master Records, Profiles and Authorizations

R/3 logs changes made by a user administrator in non-transparent tables in the database. Access to these tables is protected by the R/3 authorization concept. Once these logs have been archived, they are deleted. (Use R/3 archiving tools to archive these logs.)

Depending on your release, use either the Authorization Infosystem or Transaction SU01 to access these logs. You can view the following changes:

- Changes made directly to a user's authorization.
These are changes made to the profile list in the user's master record. This does not include indirect changes that occur when authorizations or profiles are changed. View the change documents for the profiles and authorizations to check those changes.
- Changes to:
 - the user password (hashed representation only)
 - the user type
 - the user group
 - the validity period
 - the account number
- Changes made directly to profiles or authorizations.

For more information, see *BC Users and Authorizations* → *Creating and Maintaining User Master Records* → *Displaying Change Documents* [A.30].

Additional Information for Logging and Auditing

For more information, refer to the following documentation:

Audit Info System

- [OSS Note 77503](#): Audit Information System (AIS) Version 1.5 [C.28]
- [OSS Note 100609](#): Audit Information System (AIS) - installation [C.33]

Security Audit Log

- [R/3 Online Documentation](#): *BC System Services* → *The Security Audit Log (as of 4.0B)* [A.21]

System Log

- [R/3 Online Documentation](#): *BC System Services* → *The System Log* [A.22]

Statistical Records

- [R/3 Online Documentation](#): *BC Computing Center Management System* → *R/3 System Administration* → *R/3 Accounting Interface* → *Available Statistics Data* [A.5]

Application Logging

- [R/3 Online Documentation](#): *BC Extended Applications Function Library* → *Create application log* [A.8]

Logging Workflow Execution

- [R/3 Online Documentation](#): *SAP Business Workflow* [A.34]

Logging Using Change Documents

- [R/3 Online Documentation](#): *BC Extended Applications Function Library* → *Change documents* [A.7]
- [R/3 Online Documentation](#): *BC ABAP Dictionary (Maintaining the ABAP Dictionary Objects)* [A.1]

Logging Changes to Table Data

- [OSS Note 1916](#): Logging table changes in R/3 [C.1]

Logging Changes to User Master Records, Profiles and Authorizations

- [R/3 Online Documentation](#): *BC Users and Authorizations* → *Creating and Maintaining User Master Records* → *Displaying Change Documents* [A.30]

Chapter 2-10 : Special Topics

In this chapter, we describe security measures that you can or need to take for the following special topics:

- **Protecting R/3 Internet Application Components (IAC)**
- **Protecting Application Link Enabling (ALE) Applications**
- **Security when Using R/3 Online Services**
- **Virus Protection and SAPgui Integrity Checks**
- **Synchronized Data Access With Locking**
- **Protecting Specific Tables, Authorization Objects, and other Specific Objects**

R/3 Internet Application Components (IAC)

R/3 Internet Application Components (IAC) enable users to perform business functions in R/3 using a World Wide Web browser as the user interface instead of SAPgui.

We supply a number of IACs that you can use as they are, or you can modify them to meet your own needs. (For example, you can configure the Web user interface to suit your corporate identity.) In addition, you can also develop your own Internet Application Components.

The Internet Transaction Server (ITS) serves as the link between the R/3 System and the Web. It allows for effective communication between the two systems, in spite of their technical differences.

The Internet Transaction Server is an intermediate server between the Web server and the R/3 Application Server. It controls the data flow between the R/3 System and the Internet and provides access to the Internet Application Components. This basic set-up is shown in Figure 2-10-1:

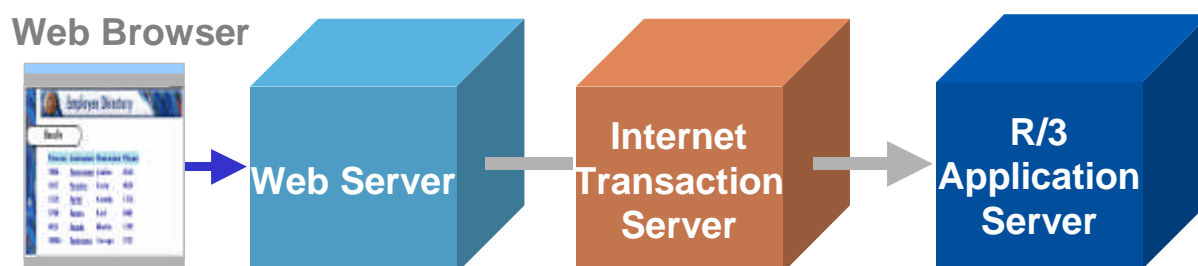


Figure 2-10-1 : The Internet Transaction Server

When connecting to the **Internet**, it is essential to protect your system from undesired access and attacks against your computers. We describe how the ITS is designed as well as the measures and concepts necessary for providing security with Internet applications in the following sections:

- **The Overall Architecture of the ITS**
- **A Secure Network Infrastructure for the ITS**
- **Configuring the Server and Network Components**
- **An Example Network Setup**
- **Using Security Services / Providing Privacy**
- **Authenticating Users**
- **Protecting Session Integrity**
- **Setting Security Levels**
- **Declaring Allowed Applications**
- **Additional Information for Internet Applications**

Although we refer to the Internet throughout the discussion, **Intranet** applications may also require a certain degree of protection, depending on your security policy. The following descriptions apply to Intranets as well.

The OSS Note 60058 [C.21] also contains information pertaining to security for R/3 on the Internet.

**Note**

In the following discussion, we describe the ITS Release 2.0, except for those points where a notable difference to earlier releases exists. In these cases, we explicitly mention the necessary information pertaining to the earlier releases.

The Overall Architecture of the ITS

The overall architecture of the ITS is shown in Figure 2-10-2:

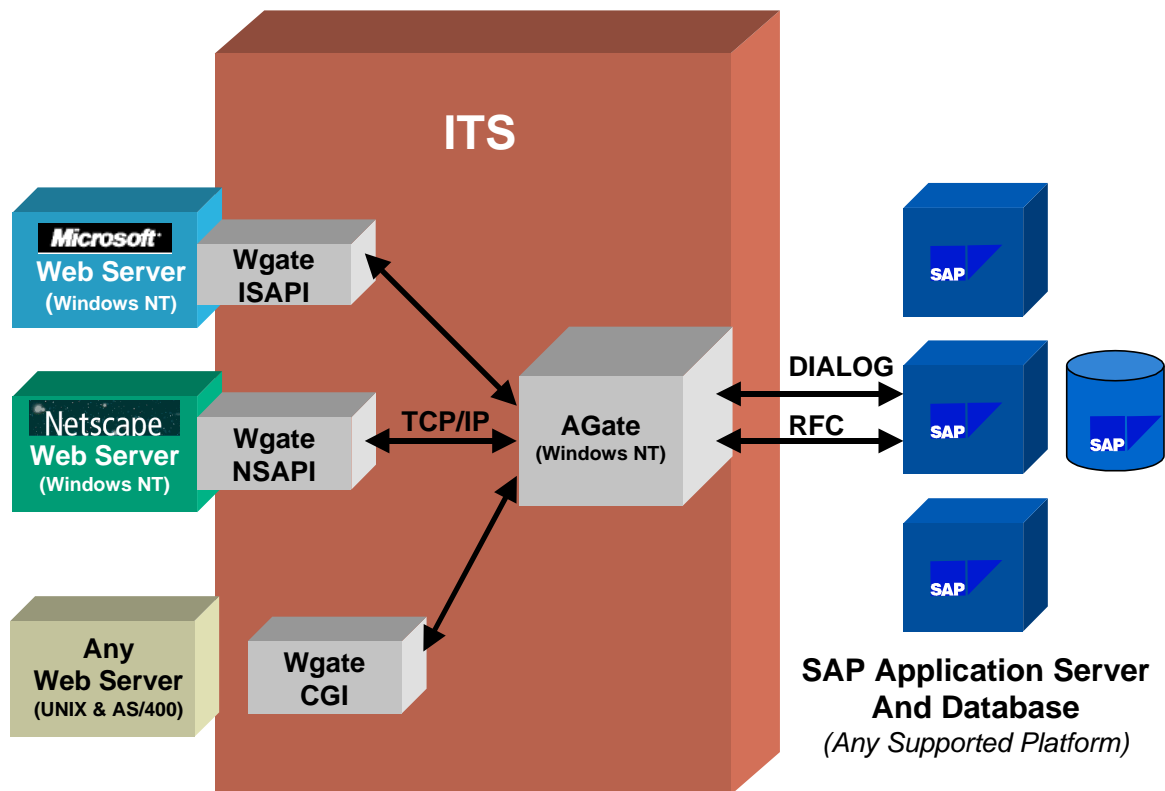


Figure 2-10-2 : The Internet Transaction Server Architecture

Components and Data Flow

WGate

The WGate component connects the ITS to the Web server. The WGate is always located on the same computer as the Web server. The following standard Web server interfaces are supported:

- **Microsoft's Information Server API (ISAPI)** on Windows NT.

The Microsoft Information Server API loads the WGate into the Web server process as a dynamic link library (DLL).

- **Netscape Server API (NSAPI)** on Windows NT.

The Netscape Server API also loads the WGate into the Web server process as a DLL.

- **Common Gateway Interface (CGI)** on UNIX and AS/400 (as of Release 4.5A).

On the UNIX and AS/400 platforms, the Common Gateway Interface starts the WGate as an external executable program.

AGate

The AGate program is implemented as a Windows NT service. Although the AGate can be located on the same machine as the WGate, we recommend that you keep the two components on two separate machines.

The AGate is responsible for managing the communication to and from R/3, including:

- Establishing the R/3 connection using DIAG (SAPgui) or RFC protocols
- Generating the HTML documents for the R/3 applications
- Managing user login data
- Managing session context and time-outs
- Code page conversions and national language support

Data Flow

The WGate establishes the connection and forwards requests to the AGate. The components communicate using the SAP Network Interface (NI), which in turn uses a TCP connection.

The AGate receives Web requests from the WGate and communicates with the R/3 application server (using DIAG or RFC). It processes the HTTP request, sends the appropriate data (including login information) to the R/3 System, retrieves information from R/3, processes it, and sends the response back to the WGate.

A Secure Network Infrastructure for the ITS

The R/3 Internet architecture has many built-in security features, such as the possibility to run the WGate and AGate on separate hosts. We strongly recommend that you set up a network infrastructure that makes use of these features to control access from the Internet to internal networks. We also recommend you use other security components, such as firewalls, packet filters and SAProuters to separate the individual parts of the network from another. Thereby, you can ensure that unauthorized access, if it does occur, is restricted to a small part of the system and can not harm your internal network and the R/3 System. Figure 2-10-3 shows some of the components that you can use to build a secure network architecture when using ITS:

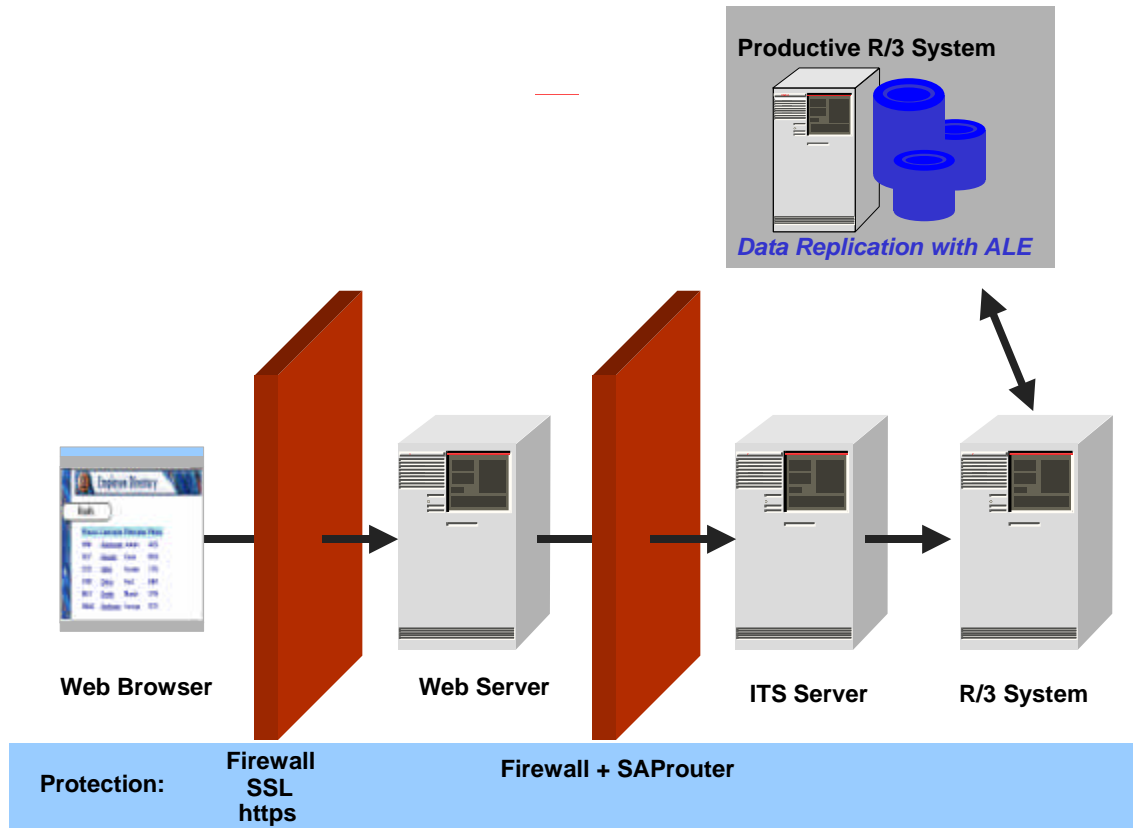


Figure 2-10-3 : Providing ITS Security

You may decide to implement some or all of these components depending on your security policy. You can find details about the components and a concrete example network setup in the sections below.

Note

To improve performance and reduce the amount of data available to your Internet applications, we recommend that you use a separate system (replicated using Application Link Enabling) for your "Internet" system, instead of your productive system.

Configuring the Server and Network Components

Our recommended network topology consists of three separate network segments that are connected by two firewall systems. Note that we use the term "firewall" in a very broad sense here. Some of the described firewall systems may only consist of a usual network router with packet filtering capabilities. Refer to *Chapter 2-3 : Network Infrastructure* for details on our networking topology and an introduction on TCP ports. Here we cover only the specific aspects pertaining to Internet applications with R/3.

Protecting the Web Server

You should protect your Web server against any kind of network packets that are not needed for the HTTP communication. To accomplish this, configure the router to pass packets to the corresponding TCP port only.

Usually a Web server requires one TCP service. Port number 80 is reserved for HTTP and used by default by all servers and browsers. Web servers that support HTTPS (HTTP plus the Secure Sockets Layer protocol), use port number 443 by default.

You should configure the Web server operating system as closed and restrictive as possible. You should disable all unnecessary network services. Refer to *Chapter 2-4 : Operating System Protection* for more details.

Protecting the AGate Server

We strongly recommend that you take additional measures to isolate the Web server from your internal corporate network. This prevents additional damage if, for example, an intruder would manage to gain control of the Web server. We also recommend that you impose very strict control over any connection between the external network, where the Web server and the WGate are located, and your internal corporate network, which contains the AGate.

We recommend that you keep the AGate in your internal network, which should be protected with a firewall and SAProuter. We explain how to protect your internal network with these components in *Chapter 2-3 : Network Infrastructure*. The following description provides specific information that applies to the ITS. It is valid for ITS Release 1.1 or higher. We no longer advise using Release 1.0 productively.



Note

It is possible to install multiple "virtual" AGates on a single computer. Each virtual AGate then has a unique name and a separate NT service. The executable files are shared with all of the AGates on a single computer. Each WGate is then configured to connect to exactly one virtual AGate on one computer.

TCP Ports

The WGate and AGate communicate using one TCP socket connection. The WGate initiates the connection to the TCP port of the AGate service. The connection is opened for each new incoming request and closed once the connection is finished.

The AGate service's port is `sapavw00_<INST>`, where `<INST>` is the name of the virtual ITS instance. The file `\WINNT\System32\Drivers\etc\Services (/etc/services on UNIX)` defines which port number corresponds to this port name; normally 3900 for the first virtual AGate installed. Multiple virtual AGates use separate ports.

Chapter 2 : The R/3 Security Toolbox

When installing the ITS, ten TCP ports are automatically added to the file `etc\services`, for example:

```

sapavw00_<INST>    tcp/3900
sapavw01_<INST>    tcp/3901
...
sapavw08_<INST>    tcp/3908
sapavwmm_<INST>    tcp/3909

```

ITS versions prior to 2.0 allocate 100 ports in a similar fashion. However, because these versions do not support virtual ITS instances, the `<INST>` string is empty.

**Note**

For normal ITS installations only the port `sapavw00_<INST>` is required for the firewall. The other ITS ports are not used and may be deleted from `etc\services`.

During installation, the ITS setup program tries to find a sequence of 10 unused ports on the installation machine starting with port number 3900. As a result, the port number associated with port name `sapavw00_<INST>` may vary for different installations. You need to check your installation to find out which port number is actually used. Each virtual ITS instance uses separate ports.

**Note**

Make sure that the port numbers associated with port name `sapavw00_<INST>` are identical on the WGate and the AGate host. This is not automatically ensured.

Using SAProuter

For a detailed description of the SAProuter functionality and administration, see the online documentation, *BC SAProuter*. Configure the SAProuter to relay only one specific WGate–AGate connection and deny all other connection attempts.

Configure the WGate to connect to the AGate via a SAProuter. Enter the route string in the NT registry on the WGate host in the following location where `<INST>` is the name of the virtual ITS installation:

```
HKEY_LOCAL_MACHINE\Software\SAP\ITS\2.0\<INST>\Connects\Host
```

The key may contain a route string of the type:

```
/H/<SAProuterhost>/S/<routerservice>/H/<host>
```

Do not specify the AGate port in the route string.

The SAProuter host must be able to map the port that is entered in the following key to a port number:

```
HKEY_LOCAL_MACHINE\Software\SAP\ITS\2.0\<INST>\Connects\PortAGate
```

The default entry is `sapavw00_<INST>`. If this port is not mapped in the SAProuter's `etc\services` file, enter the port number directly in this key.

Using other Firewall Products

You can use other firewall products (such as plug gateways) to relay the TCP connection from the WGate to the AGate.

For example, you can use a plug gateway to transparently forward an incoming TCP connection to the AGate port on the AGate host. In this case, enter the name of IP address of the plug gateway host in the following WGate registry key:

```
HKEY_LOCAL_MACHINE\Software\SAP\ITS\2.0\<<INST>\Connects\Host
```

Enter the import port of the plug gateway in the following key:

```
HKEY_LOCAL_MACHINE\Software\SAP\ITS\2.0\<<INST>\Connects\PortAGate
```

Refer to the documentation for your firewall for further information.

Protecting the R/3 Servers

You should always protect your server LAN with a firewall and SAProuter as described in *Chapter 2-3 : Network Infrastructure*. These measures also apply to networks that include the ITS.

To protect the AGate from unauthorized access, we recommend that you place the AGate in the server LAN with the R/3 application server. In this way, the AGate is protected with the same mechanisms that protect your server LAN.

Because the AGate communicates with the R/3 application server in the same way as the typical SAPgui (using DIAG or RFC), you may also want to protect this connection. For this purpose, you can include an additional packet filter (either with or without a SAProuter) between the AGate and the R/3 application server. See the OSS Note 104576 [C.34] for more information on this set-up.

Example Network Setup

Figure 2-10-4 shows an example network security infrastructure suitable for Internet access to R/3 using the SAP Internet Transaction Server:

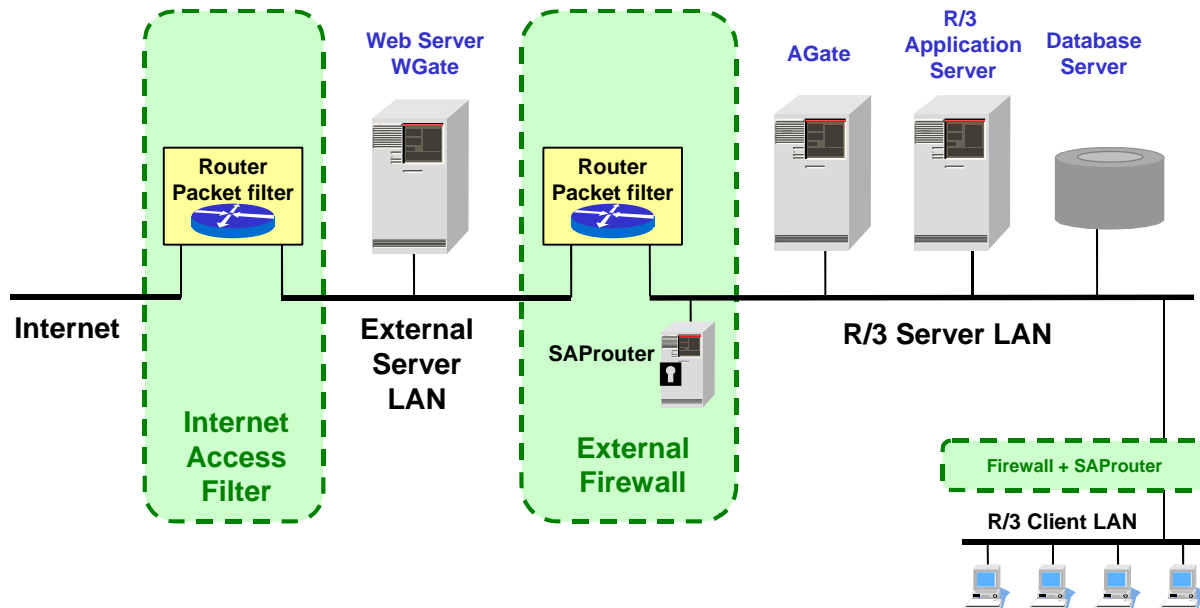


Figure 2-10-4 : Example ITS Network Topology

The "security" of the network zones increases from left to right. The first router/packet filter (the "Internet Access Filter") allows direct access from the Internet to the Web server's TCP ports only. The second router/packet filter (the "External Firewall") is configured to deny any direct access from the external server LAN to any host in the corporate LAN except for the SAProuter's TCP port on the SAProuter host. Therefore, the connection from the WGate to the AGate can only be transmitted via the SAProuter. In the example, the AGate exists in the R/3 server LAN, which is also protected from the client LAN with a firewall and SAProuter.

If desired, and as mentioned in the previous section, you can also place a router/packet filter between the AGate and the R/3 application server. This provides additional protection for the case that an intruder would manage to gain control of the Web server host. He or she could then only connect to the AGate port on the AGate computer, and not to any other computer in the corporate LAN (see OSS Note 104576 [C.34]).

Again, see *Chapter 2-3 : Network Infrastructure* for details on the configuration of the routers and SAProuters.

In the above example, we have chosen to show a setup using standard network and computer components. Many vendors offer specialized firewall products for these tasks. You may use such products; however, we do not describe them in more detail here in this guide.

Using Security Services / Providing Privacy

You can use our additional security services to increase the security of the following connections.

- **Between Web Browser and Web Server**
- **Between WGate and AGate**
- **Between AGate and R/3**

Between Web Browser and Web Server

All data (including passwords) is usually transmitted through the Internet in plain text. To maintain confidentiality for this data, you can apply encryption to the connection between the Web server and browser. The SAP-supported Web servers and all modern browsers support the encryption of the HTTP data stream by means of the Secure Sockets Layer protocol (SSL), also known as HTTPS. HTTPS data streams are completely transparent to the ITS. For more details regarding encryption techniques, see the documentation supplied by the Web server manufacturer.

In order to use SSL encryption, the Web server must obtain an X.509 certificate. We refer to this certificate in this section as the **server certificate**. The server certificate is used to authenticate the server. It is issued by a Certification Authority (CA). If the browser receives a server certificate issued by a trusted CA, then the browser can verify that it is connected to the intended server.

If you want to offer a service for all Internet users, this server certificate should have been issued by an official CA that is trusted by most browsers used in the Internet. For internal users, you can set up a corporate CA and configure the browsers to trust this CA.

The Web server uses **browser certificates** to authenticate the user. To restrict access to R/3, configure the Web server to accept only connection requests that present valid browser certificates. The browser certificates are again issued by a CA.

Between WGate and AGate

- **ITS 1.0 and ITS 1.1**

Data sent between the WGate and the AGate is encrypted using a static key. This key is easily accessible; therefore, the protection that this encryption provides is minimal.

- **ITS 2.0**

For better protection, as of ITS Release 2.0, you can use SNC (Secure Network Communications) to protect the link between the WGate and AGate. SNC uses an external security product to apply encryption to communication links between components of an R/3 System. See *Chapter 2-3 : Network Infrastructure* in the section titled *Secure Network Communications (SNC)* for details. Refer to the documentation provided with the security product itself for instructions on the necessary configuration.

Between AGate and R/3

For current releases, we do not offer any security services for the connection between the AGate and the R/3 application server. However, as of ITS 2.2 (available with R/3 Release 4.5), you will also be able to use SNC for this communication link.

Authenticating Users

In the **Internet** scenario, you do not necessarily know which users want to access the application data within R/3. In addition, for the large number of Internet users, you normally cannot set up a separate account for each user. Therefore, if you want to make certain Internet Application Components available to anonymous Internet users, you normally set up service users with pre-defined passwords in R/3. These users should have only the permissions necessary to access the application (for example, a product catalog). The corresponding ITS service is configured with this logon information, to include the password. If you need to further authenticate the Internet user (for example, when he or she places an order), the application itself must perform the additional authentication. (For example, the application verifies the customer number and password using corresponding function calls.)

For each application that is accessible over the Internet, you must create a service file, which is located on the AGate. This file contains information that is specific to the application (for example, the R/3 transaction to start, the R/3 client, the service user name and password to use). The ITS needs this information to run the application. The password does not appear as clear text in the service file, but is encrypted using a static key. Therefore, if you have service users with authorizations that are worth protecting, then take special care to protect the AGate from unauthorized access.

ITS does not store any security-relevant information on the WGate.

In an **Intranet** scenario, users can log on to R/3 over the ITS using their R/3 user name and password. User names and passwords are not stored permanently in the ITS in this case. User authentication takes place entirely within the R/3 System. Internet Application Components are subject to the usual R/3 authorization concept, just like any other R/3 transactions.

Protecting Session Integrity

To maintain the integrity of the multi-step transactions when using IACs, the ITS issues a unique session identification number when the user makes his or her first request. This session ID is sent to the browser with the first HTML page. It must be passed back to the ITS with every successive request. The session ID ensures that another user cannot easily take over a current session. (With HTTPS, a session cannot be taken over by another user.)

ITS 1.0 and 1.1 use HTTP-Cookies to store the session ID. As of ITS version 1.11, you can disable cookies. In these versions the session ID is stored directly inside the HTML pages.

As an additional security feature, the ITS stores the client IP address along with the session ID. A possible eavesdropper, who listens on the network connection and thus acquires the current session ID, cannot easily issue a fake reply. (His or her IP address does not match that of the original user.)

It is possible to configure the number of significant bytes used for the network address comparison. On the AGate, the following registry key specifies a mask of the significant network address bits:

```
HKEY_LOCAL_MACHINE\SOFTWARE\SAP\ITS\2.0\<INST>\Connects\IPChecking
```

The default value is 255.255.255.255, which specifies that the entire address should be compared. For an **Intranet** solution, this value should be enabled. For **Internet** applications, it is advisable to enter a value of 255.255.0.0. In this case, only the leading figures of a network address are compared. This allows clients who use Web Proxy servers with load balancing to access the ITS.

Setting Security Levels

The access permissions for ITS specific files on the WGate and AGate servers should be set according to your security needs. For example, you will probably want to set a high level of security (Level 3) for your productive system, and level 2 for your development system (see below).

ITS supports three levels of security (by default):

1. Full Access for everyone

At this level, everyone can access all files.

2. ITS Administrator and ITS Users

At this level, a single administrator account has access to all ITS related files and members of a given ITS users group have restricted access to certain files. You can use this level, for example, for a development scenario. Thereby, you can allow a group of users to make changes in certain files (for example, HTML templates and service files). Only the ITS Administrator can access the rest of the files. Other users cannot access any files.

3. ITS Administrator

At this level, only the ITS Administrator has access to ITS related files. Apply this level to your productive site.

You set the security level during the installation process; however, you can change the level at any time with the command-line utility `itsvprotect`.

Declaring Allowed R/3 Internet Applications

Only those R/3 applications that are explicitly written for Internet use are accessible from the Internet. This applies to both transactions, as well as for function modules and reports. You must configure the ITS so that it knows applications, reports, and function modules are to be accessible over the Internet. We describe how you declare these applications below.

Transactions (IACs)

When you call IAC transactions, the ITS acts as a regular SAPgui accessing R/3 over transaction screens. The ITS finds the information it needs to run the desired transaction in the service file that is defined for the transaction. You define the transaction to start in the `~transaction` parameter in the service file.



Example

The Transaction VW01 needs to have a service file; we suggest naming it `vw01.srvc`. In this example, the parameter `~transaction` in the file `vw01.srvc` has the value `VW01`.

If a service file does not exist for a transaction, then an Internet user cannot call the transaction over the ITS.

WebRFC

ITS also supports RFC-based access to R/3 with WebRFC or WebReporting. (WebReporting is based on WebRFC.)

In the same way as with dialog transactions, you can only call those function modules that have been specifically written for ITS.

Additionally, as of Release 4.5, you must explicitly release all Reports and Function Modules that are accessible over the Internet (use Transaction SMW0).

To disable the use of WebRFC altogether, delete the file `SAPXGWFC.dll`.



Note

For Release 3.1H, there is a patch that you should run to prevent the starting of reports that contain an empty authorization group (see OSS Note 92725 [C.31]).

Additional Information for Internet Applications

For more information, refer to the following documentation:

- [R/3 Online Documentation: R/3 Internet Application Components](#) [A.32]
- [R/3 Online Documentation: BC SAProuter](#) [A.20]
- [OSS Note 92725](#): WebReporting and Authorisation group [C.31]
- [OSS Note 60058](#): Security for R/3 Release 3.1 on the Internet [C.21]
- [OSS Note 104576](#): Package filter (firewall) between ITS and R/3 [C.34]

Protecting Application Link Enabling (ALE) Applications

Application Link Enabling (ALE) business processes are integrated processes across distributed systems.

In Releases 3.0 and 3.1, ALE uses IDocs (intermediate documents) as the data transfer format between the systems. IDocs act as data containers for transferring messages asynchronously to the receiving system.

As of Release 3.1G, ALE can also use BAPIs (Business Application Programming Interface) for the interface between systems. BAPIs are interfaces based on object-oriented technology. BAPIs can be called synchronously or asynchronously. Asynchronous BAPIs also use IDocs as data containers.

Newer ALE business processes use BAPIs; however, ALE will continue to support existing IDocs. With time, BAPIs will be created with functionality similar to existing IDoc interfaces.

Security Measures

Because ALE relies heavily on transactional RFC, all security issues that apply to RFC also apply automatically to ALE (see *Chapter 2-7 : Remote Communications (RFC & CPI-C)*). You also need a well-established network infrastructure (see *Chapter 2-3 : Network Infrastructure*). Additional measures that apply to ALE are described in the following sections:

- **ALE Users and Authorizations**
- **Useful Procedures for ALE**
- **Additional Information on ALE**

ALE Users and Authorizations

You need to take the following measures when assigning the users and authorizations for ALE use:

General

- The authorization profile B_ALE_ALL contains the following authorization objects that are needed for ALE:
 - B_ALE_LSYS ALE/EDI: Maintaining logical systems
 - B_ALE_MAST ALE/EDI: Distributing master data
 - B_ALE_MODL ALE/EDI: Maintaining customer distribution model
 - B_ALE_RECV ALE/EDI: Receiving IDocs via RFC
 - B_ALE_REDU ALE/EDI: Generating messages (ex. reduction)
 - S_TABU_DIS Table Maintenance (via standard tools such as SM31)
- Use the Transaction SALE to maintain the ALE configuration, to include setting up the distribution model and setting up ALE user authorizations and profiles.

Chapter 2 : The R/3 Security Toolbox

- Protect external users and passwords.

For example, for a non-SAP system to send IDocs to an R/3 System using transactional RFC, it must also send an R/3 user and password. In most cases, the user and password are stored outside of the R/3 System. Ensure that this information is not accessible to external systems or programs. (How you can do this is dependent on the system that you have; therefore, you need to refer to the documentation for the system where the information is stored.)

Distribution Model

- Protect the ALE distribution model from unauthorized access. The corresponding authorization object is B_ALE_MODL.

Source System

- To make sure that users communicating over RFC in ALE are known to the sending system, you need to enter them and their logon information in the RFC destination. (Use Transaction SM59). Therefore, set up these ALE users in the target system so that improper use is held to a minimum. (Keep all authorizations to a minimum.)

Target System

- Set up special users for using ALE. Give only these users the authorizations for using ALE. Do not give the standard users authorizations for using ALE.
- The RFC users in the target system authorized to communicate in ALE with transactional RFC, must be made known to the sender system. To prevent remote logons, assign the ALE users in the target system the type CPIC. (Use Transaction SU01). Do not assign them type DIALOG. There are two reasons for this:
 - CPIC users cannot execute dialog transactions.
 - DIALOG users can remotely logon to an RFC destination from the maintenance transaction for RFC destinations (SM59).
- Restrict application authorization in the target system. You only need application authorizations in the target system if IDocs have to be processed immediately. IDocs should be processed as background jobs and not immediately, unless absolutely necessary.

Background Processing

- ALE users only require authorization for creating IDocs; they do not need authorization for the receiving application.
- The authorization object for receiving an IDoc is B_ALE_RECV. It contains the field EDI_MES, which enables you to specify the message type that the user is authorized to receive.

Immediate Processing

- If inbound IDocs have to be transferred immediately to the application, the ALE user should only be assigned those application authorizations required to post the application document from the IDoc.
- To determine which authorizations are needed, perform a trace (see UP 2-10-1).

Give the ALE user the highest level of authorization in the trace. Restrict authorizations to those specific function groups (authorization object S_RFC) that are accessed during the trace.

Useful Procedures for ALE

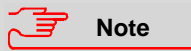
UP 2-10-1 : Verifying Required Authorizations using Trace

To verify required authorizations using the Trace function, perform the following procedure.

Prerequisites

The following objects in the test system are required:

- ALE user with the required authorizations (for example, full authorizations).
- IDoc with the status 64 (ready for transfer to the application), which corresponds to the IDocs expected in the production operation.



The authorization trace is a component of the trace function in the R/3 System (Transaction ST01).

Procedure

Execute Trace

Proceed as follows:

1. Start Transaction BD87.
2. Call Transaction ST01.
3. Choose *Standard options*.
4. Choose *None* to switch off all the trace options.
5. Choose *Trace for authorization checks*.
6. In the group box *Restrictions*, enter the ALE user in the *Users* field.
7. Choose *Accept*.
8. Choose *Switch, edit*.
9. In the group box *General management*, set the *write options* to *Trace: write to disk*.
10. In the group box *Status of active system* choose the symbol, *Activate trace*.
11. Process the IDoc in Transaction BD87.

Stop Trace

Stop the trace by choosing *No trace*.

Display Trace

To display the trace perform the following:

1. Choose *Trace files* → *Standard*.
2. Double click on file.

Additional Information on ALE

For more information, refer to the following documentation:

- [R/3 Online Documentation: CA ALE \[A.31\]](#)

R/3 Online Services

When using the R/3 Online Services for assistance and advice, you want to be sure that the information being transferred and processed is securely handled. We discuss the necessary security measures in the following sections:

- **Measures That We Take at SAP**
- **Measures That You Should Take**
- **Additional Information for R/3 Online Services**

Measures That We Take at SAP

To ensure the security of the remote connection, at SAP we take the following measures:

- We use only designated communication connections (VPNs) or direct connections (ISPN).
- We restrict the access authorizations of the hardware router.
- We use the SAProuter program.
- We log all usage and maintenance activities of the remote connection.
- We divide the available services into different categories, each with its own access authorizations.
- We restrict the access authorizations accordingly.
- Our employees and our partner's employees must oblige to regulations pertaining to secrecy when accessing personal data or company secrets. This applies to data belonging to SAP itself as well as to our customers (see OSS Note: 35493 [C.11]).
- Following our policy, you must open the remote connection. We do not initiate remote connections.

Measures That You Should Take

We recommend that you take the following measures:

- Restrict the access authorizations for the hardware router. (We recommend you use a hardware router.)
- Use the SAProuter program.
 - The SAProuter logs connection activities.
- Increase protection by enforcing password protected connections.
- Tailor your R/3 user profiles to the type of service required. Set these users up in test clients, unless otherwise necessary.
- After a session, you can analyze the activities that occurred using the Transaction STAT.
- Monitor consultants with the echo mode.

- Do not disclose any of your users' passwords over the remote connection.

If you have a problem that can only be solved by an SAP service person accessing your system as <SID>adm, you should log the session on at the operating system level (for example, using the UNIX `script` command). As soon as the problem has been fixed, change the password.

- We suggest you disclose the remote user's logon information over a separate channel. Either write the information in a separate document, or request a return telephone call. Do not send the information in the remote request.
- Deactivate the R/3 remote user's name and password as soon as the service session is terminated.
- Deactivate the remote connection as soon as the task is completed.
- Close the OSS connections upon completion.
- Set time limits for OSS connections.

For more information on service connections, see the OSS Note 35010 [C.10].

Additional Information on R/3 Online Services

For more information, refer to the following documentation:

- R/3 Online Documentation: SAP Network Security [A.35]
- SAP Documentation: Remote Connections to the R/3 Online Services; Material Number 50017380 [E.5]
- OSS Note 46902: Security Aspects in Remote Access [C.17]
- OSS Note 35010: Service connections: Composite note (overview) [C.10]
- OSS Note 35493: Secrecy and Data Security Obligations [C.11]

Virus Protection and Integrity Checks

General Recommendations

The spreading of software viruses is not a new topic of discussion. Viruses have infected thousands of systems over the past several years and they should not be taken lightly. A successful virus infection can destroy data or block systems within moments. The spreading of viruses has been harmful enough on isolated machines where a single hard drive has been the storage medium. With the use of networks, the damage incurred by a virus infection increases enormously. An infected network can be rendered useless, costing a company money, time, and assets to re-establish itself. There are numerous virus-checking software packages on the market that you should use to check your software and you should update these regularly. Additionally, you need to educate your employees on the importance of being wary of unchecked software.

R/3 Software

We check the R/3 software and data media for viruses before delivery. Additionally, as of Release 3.0 (on Windows NT platforms only), the SAPgui presentation software performs an integrity check on itself, which detects and reports any changes that may indicate a virus infection.

Protecting Specific Tables, Authorizations Objects, etc.

We recommend that you decide which individual tables, authorizations, etc. you consider sensitive and take the appropriate measures to protect them.

There may be many objects that you consider sensitive. We are not going to discuss them all in detail here. However, we do want to draw your attention to the following objects in R/3 that we consider especially sensitive:

- **SAP_ALL Authorization**
- **SAP_NEW Authorization**
- **Table T000**
- **HR Tables**
- **HR Authorization Profile P_BAS_ALL**
- **System Parameter Profile File**

We describe the measures that you can take to protect these objects in detail below:

SAP ALL Authorization

This composite profile contains all of the SAP authorizations. A user with this authorization can perform all R/3 tasks. You should not assign any of your users this authorization profile. We recommend that you maintain one single user with this profile; you should keep this password secret (lock it in a safe) and use it only in emergencies.

We recommend that you distribute the authorizations from SAP_ALL on the appropriate positions. For example, instead of assigning your system administrator (or superuser) the authorization SAP_ALL, assign him or her only those that apply to system administration, namely the S_* authorizations. These authorizations give him or her enough rights to administer the entire R/3 System, without allowing him or her to perform tasks in other areas such as Personnel.

SAP NEW

This composite profile contains those profiles that are new to each release. After an upgrade, you need this profile so that certain tasks can run smoothly. However, we do not recommend that you keep this profile active for a longer period.

We recommend the following steps:

1. After the upgrade, delete the SAP_NEW_* profiles for releases prior to the establishment (or re-establishment) of your authorization concept.
2. Delete those SAP_NEW_* profiles for releases in which you have already distributed the profiles.
3. Distribute the rest of the profiles contained in the SAP_NEW_* profiles to their appropriate places and maintain their values.
4. Then, delete the profile SAP_NEW.

A long list of SAP_NEW profiles (for example, after several upgrades) is an indicator that it is time to review your authorization concept and re-establish it.

Table T000

Table T000 is a fundamental table in your R/3 System. You create and maintain your R/3 clients in this table. Therefore, you should protect this table in your productive system from unauthorized access.

To protect T000, take the following precautions:

- Give maintenance access to system administrators only. The corresponding authorization object is S_ADMI_FCD.
- Define a process for creating and maintaining clients.
- Ensure that the S_TCODE authorization object contains the table maintenance and client maintenance transactions SCC4, SM30 and SM31.
- Set the following fields to the following values for the authorization object S_TABU_DIS.
 - **Field:** *Activity*; Values: 02, 03
 - **Field:** *Authorization group*; Value: SS
- Set the indicator for client-independent maintenance field for the authorization object S_TABU_CLI to the value X.

HR Tables

In Releases 3.0A-C, the PA<nnnn> (employee data) and PB<nnnn> (applicant data) tables for the infotypes nnnn were delivered without having the authorization group PA assigned to them. Consequently, they could be read using SE16. (This problem has been solved in 3.0D.)

Therefore, to protect your HR tables in the Releases 3.0A-C, you must explicitly assign them to the authorization group PA. In addition, exclude the group PA from the authorization object S_TABU_DIS.

HR Authorization Profile P_BAS_ALL

The P_BAS_ALL authorization profile allows users to display the contents of tables from other applications using general table display transactions. This authorization is intended for HR end users only.

The P_BAS_ALL authorization profile contains the P_TABU_DIS authorization (based on the S_TABU_DIS object). As default, the P_TABU_DIS contains the authorization groups A - O* and PB - XXXX. This allows PA users to display table contents that do not belong to the PA group (using general table viewing tools).

To restrict this function to HR tables only (PA users can then thereby view HR tables):

1. Make sure that you assign all HR tables one of the classes PC or PS.
2. Restrict the *Authorization group* field in P_BAS_ALL to PC and PS.

For more information, see OSS Note 11796 [C.5].

System Profile Parameter Files

Certain security-relevant configurations are contained in the following system profile files (for example, the profile parameters `login/no_automatic_user_sap*` or `login/fails_to_user_lock`):

- <SID>_<Instance> system profile for the application server
- START_<Instance> start script
- DEFAULT.PFL global profile file

You should protect these files from unauthorized access. If an intruder manages to access and change these files, he or she can change the configuration for the next time that the system is started.

Ensure that as few people as possible are given access to these files. Regularly make sure that these files are authentic.

Maintain these files with the Transaction RZ11.

Additional Information for Specific Objects

For more information, refer to the following documentation:

- OSS Note 11796: Authorization profile P_BAS_ALL and table display [C.5]

Chapter 3 : Summary

As previously mentioned, there are numerous areas in R/3 that are relevant to R/3 security. In Chapter 2, we explained the details of these issues that apply in each of these various areas. There is a lot to consider regarding R/3 security, and in this chapter, we summarize some of the more relevant information. The following information is available:

- **Tools, Transactions, and Reports**
- **Profile Parameters**
- **Authorization Objects**

Chapter 3-1 : Tools, Transactions, and Reports

Table 3-1-1 shows the available tools, transactions, and reports for each of the areas in R/3 (where applicable):

Table 3-1-1 : Tools, Transactions, and Reports in R/3

Area	Tool, Transaction or Report	Comment
User Authentication	Customer exit: SUSR0001	Customer exit for additional authentication checks after logon
	Report: RSUSR003	Check that SAP* has been created in all clients and that standard passwords for the standard users have been changed.
	Report: RSUSR006	Lists users that are locked due to incorrect logon attempts or explicitly locked from the system administrator.
	Security Audit Log Transactions SM18, SM19, SM20	Records all successful and unsuccessful logon attempts.
R/3 Authorization Concept	System Log Transaction SM21	Records all locks.
	The Profile Generator Transaction PFCG	Tool for maintaining profiles and authorizations.
	The Authorization Infosystem Transaction SUIM	Infosystem containing a variety of reports on authorizations and profiles.
	Report: RSCSAUTH	Assign reports to authorization classes.

Table 3-1-1 : Tools, Transactions, and Reports in R/3 (continued)

Area	Tool, Transaction or Report	Comment
Database Access	SAPDBA	Tool for database maintenance tasks. Available for ORACLE and INFORMIX.
	Note: There are also tools available from the various database vendors. See the documentation on your database for more details.	
Change and Transport System	Workbench and Customizing Organizer Transactions SE09 and SE10	Tool for managing imports and exports
	Transport Management System Transaction STMS	Tool for managing the change and transport system. (Available as of Release 3.1H.)
	Programs: <code>tp</code> , <code>R3trans</code>	Programs at the operating system level for executing transports.
Logging and Auditing	Audit Info System Transaction SECR	Tool for running business or security audits.
	The Security Audit Log Transactions SM18, SM19, SM20	Tool for auditing security-relevant information in R/3 such as unsuccessful transaction starts or changes to user master records.
	The System Log Transaction SM21	Tool for logging system-relevant information such as user locks.
	Statistic Records Transaction STAT	Tool for obtaining statistical records, categorized by transaction and user.
	Application Logging Transactions SLG1 and SLG0	Tool for logging application-level activities.
	SAP Business Workflow analysis tools. (Transactions SWI2, SWI5, ...)	Tools for logging and analyzing workflow activities.
	Change Documents for business objects Transaction: SCD0	Set up change documents for dictionary objects.
	Changes to Table Data Transaction: SCU3	View changes to table data.
	Change Documents for User Master Records Transaction: SU01	View change documents for user master records.

Chapter 3-2 : Profile Parameters

Table 3-2-1 shows the R/3 profile parameters that are relevant to security.



Note

Note that for the following values, there may be slight variations between releases. The values shown below were taken from a 4.0A Release (unless indicated otherwise). To find the exact description that applies to your release, refer to the documentation in the Transaction RZ11.

Also, note that not all of the parameters were mentioned elsewhere in the guide. They are listed here for your information only. For a more detailed description, see the documentation in the Transaction RZ11.

Table 3-2-1 : Profile Parameters

Profile Parameter	Definition	Default	Comment	Reference on Page:
User Authentication				
login/....				
failed_user_auto_unlock	Enable automatic unlock of locked user at midnight	1		2-7
fails_to_session_end	Number of invalid logon attempts until session end	3		2-7
fails_to_user_lock	Number of invalid logon attempts allowed until user lock	12		2-7
min_password_lng	Minimum password length	3		2-4
no_automatic_user_sap* (prior to 3.1H)	Control of the automatic login user SAP*	0	0=automatic user SAP* is permitted	2-5
no_automatic_user_sapstar (as of 3.1H)			1=automatic user SAP* is deactivated	
			Set in all instances; setting in the main instance does not affect all servers.	
password_expiration_time	Number of days until password must be changed	0	0=no time limit	2-4

Chapter 3 : Summary

Table 3-2-1 : Profile Parameters (continued)

Profile Parameter	Definition	Default	Comment	Reference on Page:
User Authentication (continued)				
rdisp/....				
gui_auto_logout	Number of seconds that a user can be idle before being logged off	0	0=no time limit	2-7
rfc_max_login	Maximum number of users that can be logged on to the R/3 System.	90	% value. The total number of users allowed is specified in the parameter rdisp/tm_max_no.	not referenced
rfc_max_own_login	Maximum number of own logons in the R/3 System.	25	see above	not referenced
tm_max_no	Maximum number of entries in the array tm_adm. (Limits maximum number of users per instance.)	200		not referenced
R/3 Authorization Concept				
auth/....				
auth_number_in_userbuffer	Maximum number of authorizations allowed in user buffer	1000		not referenced
authorization_trace	The combination of transaction and authorization object is written to table USOBX upon authorization check, if it does not exist.	N	Affects performance!	not referenced
no_check_in_some_cases	Special authorization checks switched off by customer.	N	May be relevant if you use the profile generator. Adhere to the cautions when setting this parameter!	2-22
no_check_on_tcode	Disable authority check against authorization object S_TCODE	N	Do not change unless absolute necessary!	not referenced

Table 3-2-1 : Profile Parameters (continued)

Profile Parameter	Definition	Default	Comment	Reference on Page:
R/3 Authorization Concept (continued)				
auth/....				
rfc_authority_check	Execute RFC authority check against the object S_RFC	1	0=No authorization check 1 or 2=Authorization check active (see documentation in RZ11) Set to at least 1	not referenced
system_access_check_off	Deactivate authorization checks for certain ABAP language elements (file operations, CPIC calls)	0		not referenced
test_mode	Run Report RSUSR400 when authorization checks are performed.	N (off)	Used for tracing purposes. Reduced performance!	not referenced
Network Infrastructure (SNC)				
snc/....				
accept_insecure_cplic	Accept unprotected incoming CPIC-connections when using SNC.	0	0=only accept SNC-protected connections As of 4.0	not referenced
accept_insecure_gui (4.0) or permit_insecure_gui (3.1)	Allow non-protected SAPgui connections when using SNC.	0	0=accept secure logons only	not referenced
accept_insecure_r3int_rfc	Accept unprotected internal RFC-connections when using SNC.	1	1=accept unprotected RFC connections As of 4.0	not referenced
accept_insecure_rfc	Accept unprotected incoming RFC connections when using SNC.	0	0=only accept SNC-protected connections As of 4.0	not referenced
data_protection/max	Use this level of security when snc/data_protection_use = 9	3	1=authentication 2=integrity 3=privacy	not referenced
data_protection/min	Minimum level of security for incoming connections	2	1=authentication 2=integrity 3=privacy	not referenced
data_protection/use	User-defined level of security for data transfers	9	same as above plus 9=use value from snc/data_protection/max	not referenced

Chapter 3 : Summary

Table 3-2-1 : Profile Parameters (continued)

Profile Parameter	Definition	Default	Comment	Reference on Page:
Network Infrastructure (continued)				
snc/....				
enable	Activate SNC	0	0=off 1=on	not referenced
gssapi_lib	Location of the gssapi library	none		not referenced
identity/as	Security name of the application server	none		not referenced
permit_insecure_start	Permit the starting of unprotected external programs when using SNC.	0	0=do not start unprotected programs As of 4.0	not referenced
r3int_rfc_gop	Quality of protection for internal RFCs with SNC protection	8	8=use value from snc/data_protection/use As of 4.0	not referenced
r3int_rfc_secure	Use SNC for initiating internal RFC communications	0	0=do not use SNC As of 4.0	not referenced
Change and Transport System				
transport/....				
systemtype	System class of transport (SAP or CUSTOMER)	CUSTOMER		not referenced
tp_logging	Log use of transport program	ON		not referenced
Remote Communications				
gw/....				
max_conn	Maximum number of active connections allowed	100		not referenced
monitor	Allow monitor commands	2	0: not allowed 1: only from GW monitors allowed 2: from local and remote gateways allowed	2-108
sec_info	Directory path for the configuration file secinfo	/usr/<SID>/<instance>/data/secinfo		2-110
stat	Activate gateway statistics	0	0=off 1=on	not referenced

Table 3-2-1 : Profile Parameters (continued)

Profile Parameter	Definition	Default	Comment	Reference on Page:
Secure Store and Forward Mechanisms				
DIR-INSTANCE	Instance's main directory	/usr/sap/ <SID>/ <instance>		2-114
Logging and Auditing				
rsau/...				
enable	Activates the audit log on an application server.	0	as of Release 4.0B	2-117
local/file	Specifies the location of the audit log on the application server.	/usr/sap /<SID> /<instno> /log /audit_ <instno>	as of Release 4.0B	2-117
max_diskspace_local	Specifies the maximum length of the audit log.	1,000,000 bytes	as of Release 4.0B	2-117
selection_slots	Specifies the number of selection slots for the audit.	2	as of Release 4.0B	2-117
rslg/...				
local/file	Specifies the location of the local log on the application server.			2-119
collect_daemon/host	Specifies the application server that maintains the central log.	<hostname of main instance>		2-119
central/file	Specifies the location of the active file for the central log on the application server.			2-119
central/old_file	Specifies the location of the old file for the central log on the application server.			2-119
max_diskspace_local	Specifies the maximum length of the local log.	500,000 bytes		2-119
max_diskspace_central	Specifies the maximum length of the central log.	2,000,000 bytes		2-119

Chapter 3 : Summary

Table 3-2-1 : Profile Parameters (continued)

Profile Parameter	Definition	Default	Comment	Reference on Page:
Logging and Auditing (continued)				
rec/....				
client	Record SM30 table changes	OFF	Tables must also be specified for recording changes	2-122
stat/....				
file	Location of the statistic records file	/usr/sap/ <SID>/ <instance>/ data/ stat.DAT		2-120
level	Set logging of system activities, changes in profile parameters, changes in UNIX kernel parameters, and changes in DB parameters for CCMS	1		2-120
version	Set logging version	2 (Vers. 2)	Version 1: as in Rel. 2.0 Version 2: as with 1, but additionally records RFC and memory statistics	2-120

Chapter 3-3 : Authorization Objects

Table 3-3-1 shows those authorization objects that we have referenced throughout the guide. For a more detailed description, see the documentation provided in the Authorization Infosystem (Transaction SUIM).

Table 3-3-1 : Authorization Objects

Authorization Object	Description	Reference on Page(s):
B_ALE_LSYS	ALE/EDI: Maintaining logical systems	2-137
B_ALE_MAST	ALE/EDI: Distributing master data	2-137
B_ALE_MODL	ALE/EDI: Maintaining customer distribution model	2-137 2-138
B_ALE_RECV	ALE/EDI: Receiving IDocs via RFC	2-137 2-138
B_ALE_REDU	ALE/EDI: Generating messages (ex. reduction)	2-137
S_ADMI_FCD	System Authorizations	2-15 2-105 2-108 2-143
S_CTS_ADMI	Administration functions in Change and Transport System	2-105
S_DEVELOP	ABAP Workbench	2-15 2-105
S_LOG_COM	Authorization to execute logical operating system commands	2-53
S_RFC	Auth. check for RFC access	2-109 2-138 3-5
S_RZL_ADM	CC control center: System administration	2-54
S_TABU_CLI	Maintenance of client-independent tables	2-15 2-143
S_TABU_DIS	Table Maintenance (via standard tools such as SM31)	2-15 2-21 2-137 2-143 2-144
S_TCODE	Authorization check for transaction start	2-20 2-21 2-108 2-143 3-4
S_TOOLS_EX	Tools Performance Monitor	2-120

Chapter 3 : Summary

Table 3-3-1 : Authorization Objects (continued)

Authorization Object	Description	Reference on Page(s):
S_TRANSPRT	Change and Transport Organizer	2-15 2-105 2-105
S_USER_AUT	User Master Maintenance: Authorizations	2-15 2-18 2-19
S_USER_GRP	User Master Maintenance: User Groups	2-18 2-19
S_USER_PRO	User master maintenance: Authorization profile	2-18 2-19

Appendix A : List of References

The following sources of documentation are provided in this appendix:

- **R/3 Online Documentation and their Locations**
- **IMG**
- **OSS Notes**
- **Internet Sites**
- **Miscellaneous**



Note

R/3 Online Documentation: For the online documentation, we have provided the locations for the Releases 3.1H and 4.0B. The menu paths may vary slightly in other releases.

Internet sites: Note that we do not guarantee the availability or correctness of the Internet sites.

A: R/3 Online Documentation and their Locations

Ref.No.	Name and Location
[A.1]	<p><u>BC ABAP Dictionary (Maintaining the ABAP Dictionary Objects)</u></p> <p>Release 3.1H: <i>Basis Components</i> → <i>ABAP/4 Development Workbench</i> → <i>ABAP/4 Dictionary</i></p> <p>Release 4.0B: <i>BC Basis Components</i> → <i>ABAP Workbench</i> → <i>BC ABAP Dictionary</i></p>
[A.2]	<p><u>BC Basis Programming Interfaces → Programming with External Operating System Commands</u></p> <p>Release 3.1H: <i>Basis Components</i> → <i>ABAP/4 Development Workbench</i> → <i>Basis Programming Interfaces</i> → <i>Programming with External Operating System Commands</i></p> <p>Release 4.0B: <i>BC - Basis Components</i> → <i>ABAP Workbench</i> → <i>BC Basis Programming Interfaces</i> → <i>Programming with External Operating System Commands</i></p>
[A.3]	<p><u>BC Change and Transport Organizer</u></p> <p>Release 3.1H: see <i>BC Transport System</i> [A.25]</p> <p>Release 4.0B: <i>BC Basis Components</i> → <i>Change and Transport System</i> → <i>BC Change and Transport Organizer</i></p>
[A.4]	<p><u>BC Computing Center Management System</u></p> <p>Release 3.1H: <i>Basis Components</i> → <i>System Administration</i> → <i>Computing Center Management System</i></p> <p>Release 4.0B: <i>BC - Basis Components</i> → <i>Computing Center Management System</i> → <i>BC Computing Center Management System</i></p>

A: R/3 Online Documentation and their Locations (continued)

Ref.No.	Name and Location
[A.5]	<p><u><i>BC Computing Center Management System → R/3 Accounting Interface → Available Statistics Data</i></u></p> <p>Release 3.1H: <i>Basis Components → System Administration → Computing Center Management System → R/3 System Administration → R/3 Accounting Interface → Available Statistics Data</i></p> <p>Release 4.0B: <i>BC - Basis Components → Computing Center Management System → BC Computing Center Management System → R/3 System Administration → R/3 Accounting Interface → Available Statistics Data</i></p>
[A.6]	<p><u><i>BC Computing Center Management System → R/3 System Administration → External Operating System Commands</i></u></p> <p>Release 3.1H: <i>Basis Components → System Administration → Computing Center Management System → R/3 System Administration → External Operating System Commands</i></p> <p>Release 4.0B: <i>BC - Basis Components → Computing Center Management System → BC Computing Center Management System → R/3 System Administration → External Operating System Commands</i></p>
[A.7]	<p><u><i>BC Extended Applications Function Library → Change documents</i></u></p> <p>Release 3.1H: <i>Basis Components → ABAP/4 Development Workbench → Extended Applications Function Library → Change documents</i></p> <p>Release 4.0B: <i>BC - Basis Components → ABAP Workbench → BC Extended applications functions library → Change documents</i></p>
[A.8]	<p><u><i>BC Extended Applications Function Library → Create application log</i></u></p> <p>Release 3.1H: <i>Basis Components → ABAP/4 Development Workbench → Extended Applications Function Library → Create application log</i></p> <p>Release 4.0B: <i>BC - Basis Components → ABAP Workbench → BC Extended applications functions library → Create application log</i></p>
[A.9]	<p><u><i>BC SAP Communication: Configuration Guide → SAP Gateway</i></u></p> <p>Release 3.1H: <i>Basis Components → System Administration → R/3 Network Configuration → SAP Communication: Configuration → SAP Gateway</i></p> <p>Release 4.0B: <i>BC - Basis Components → Basis Services / Communication Interfaces → BC - SAP Communication: Configuration → BC - SAP Communication: Configuration → SAP Gateway</i></p>
[A.10]	<p><u><i>BC SAP Communication: CPI-C Programmer's Guide</i></u></p> <p>Release 3.1H: <i>Basis Components → ABAP/4 Development Workbench → CPI-C Programming</i></p> <p>Release 4.0B: <i>BC - Basis Components → Basis Services / Communication Interfaces → BC SAP Communication: CPI-C Programmer's Guide</i></p>
[A.11]	<p><u><i>BC SAP Database Administration</i></u></p> <p>Release 3.1H: <i>Basis Components → Database Administration</i></p> <p>Release 4.0B: <i>BC - Basis Components → Database Interface, Database Platforms</i></p>
[A.12]	<p><u><i>BC SAP Database Administration: ADABAS (Software AG)</i></u></p> <p>Release 3.1H: <i>Basis Components → Database Administration → ADABAS</i></p> <p>Release 4.0B: <i>see ADABAS Documentation</i></p>

A: R/3 Online Documentation and their Locations (continued)

Ref.No.	Name and Location
[A.13]	<p><u>BC SAP Database Administration: DB2 common server</u></p> <p>Release 3.1H: <i>Basis Components → Database Administration → SAP Database Administration: DB2 Common Server</i></p> <p>Release 4.0B: <i>BC - Basis Components → Database Interface, Database Platforms → BC SAP Database Administration: DB2</i></p>
[A.14]	<p><u>BC SAP Database Administration: DB2 common server → Managing Passwords of R/3 Admin Users</u></p> <p>Release 3.1H: <i>Basis Components → Database Administration → SAP Database Administration: DB2 Common Server → Managing Passwords of R/3 Admin Users</i></p> <p>Release 4.0B: <i>BC - Basis Components → Database Interface, Database Platforms → BC SAP Database Administration: DB2 → Users → Managing Passwords</i></p>
[A.15]	<p><u>BC SAP Database Administration: DB2/400</u></p> <p>Release 3.1H: <i>Basis Components → Database Administration → SAP Database Administration: DB2/400</i></p> <p>Release 4.0B: <i>BC - Basis Components → Database Interface, Database Platforms → BC SAP Database Administration: DB2/400</i></p>
[A.16]	<p><u>BC SAP Database Administration: INFORMIX</u></p> <p>Release 3.1H: <i>Basis Components → Database Administration → SAP Database Administration: INFORMIX</i></p> <p>Release 4.0B: <i>BC - Basis Components → Database Interface, Database Platforms → BC SAP Database Administration: INFORMIX</i></p>
[A.17]	<p><u>BC SAP Database Administration: Oracle</u></p> <p>Release 3.1H: <i>Basis Components → Database Administration → SAP Database Administration: ORACLE</i></p> <p>Release 4.0B: <i>BC - Basis Components → Database Interface, Database Platforms → BC SAP Database Administration: Oracle</i></p>
[A.18]	<p><u>BC Database Administration: ORACLE → Starting and Using the SAPDBA Program → SAPDBA: Expert Mode → Defining the Password</u></p> <p>Release 3.1H: <i>Basis Components → Database Administration → SAP Database Administration: ORACLE</i></p> <p>Release 4.0B: <i>BC - Basis Components → Database Interface, Database Platforms → BC SAP Database Administration: Oracle → Starting and Using the SAPDBA Program → Configuring SAPDBA → SAPDBA: Expert Mode → Defining the Password</i></p>
[A.19]	<p><u>BC SAP High Availability</u></p> <p>Release 3.1H: <i>Basis Components → System Administration → SAP High Availability</i></p> <p>Release 4.0B: <i>BC - Basis Components → Computing Center Management System → BC SAP High Availability</i></p>
[A.20]	<p><u>BC SAProuter</u></p> <p>Release 3.1H: <i>R/3 Service and Support → SAProuter</i></p> <p>Release 4.0B: <i>BC Kernel Components → BC SAProuter</i></p>

List of References

A: R/3 Online Documentation and their Locations (continued)

Ref.No.	Name and Location
[A.21]	<u><i>BC System Services → The Security Audit Log</i></u> Release 3.1H: not available Release 4.0B: <i>BC - Basis Components → Kernel Components → BC System Service → The Security Audit Log</i>
[A.22]	<u><i>BC System Services → The System Log</i></u> Release 3.1H: <i>Basis Components → System Administration → System Services → The System Log</i> Release 4.0B: <i>BC - Basis Components → Kernel Components → BC System Service → The System Log</i>
[A.23]	<u><i>BC Transport Control</i></u> Release 3.1H: <i>Basis Components → System Administration → Transport Control</i> Release 4.0B: <i>BC - Basis Components → Change and Transport System → BC Transport Control</i>
[A.24]	<u><i>BC Transport Management System</i></u> Release 4.0B: <i>Basis Components → System Administration → BC - Transport Management System</i>
[A.25]	<u><i>BC Transport System</i></u> Release 3.1H: <i>Basis Components → System Administration → Transport System</i> Release 4.0B: see → <i>BC Change and Transport Organizer</i> [A.3]
[A.26]	<u><i>BC Transport System → Setting up the Workbench Organizer and the Transport System → Setting the System Change Option</i></u> Release 3.1H: <i>Basis Components → System Administration → Transport System → Setting up the Workbench Organizer and the Transport System → Setting the System Change Option</i> Release 4.0B: <i>BC - Basis Components → Change and Transport System → BC Change and Transport Organizer → Requirements for Working with the Change and Transport System (CTS) → Setting Up the System Group → Setting the System Change Option</i>
[A.27]	<u><i>BC Users and Authorizations</i></u> Release 3.1H: <i>Basis Components → System Administration → Users and Authorizations</i> Release 4.0B: <i>BC - Basis Components → Computing Center Management System → BC Users and Authorizations</i>
[A.28]	<u><i>BC Users and Authorizations → Access Security: Logon Customizing and Protecting Standard Users</i></u> Release 3.1H: <i>Basis Components → System Administration → Users and Authorizations → Access Security: Logon Customizing and Protecting Standard Users</i> Release 4.0B: <i>BC - Basis Components → Computing Center Management System → BC Users and Authorizations → Access Security Logon Customizing and Protecting Standard Users</i>

A: R/3 Online Documentation and their Locations (continued)

Ref.No.	Name and Location
[A.29]	<u><i>BC Users and Authorizations → Transporting User Master Records, Authorizations and Profiles</i></u> Release 3.1H: <i>Basis Components → System Administration → Users and Authorizations → Transporting User Master Records, Authorizations and Profiles</i> Release 4.0B: <i>BC - Basis Components → Computing Center Management System → BC Users and Authorizations → Transporting User Master Records, Authorizations and Profiles</i>
[A.30]	<u><i>BC Users and Authorizations → Creating and Maintaining User Master Records → Displaying Change Documents</i></u> Release 3.1H: <i>Basis Components → System Administration → Users and Authorizations → Creating and Maintaining User Master Records → Displaying Change Documents</i> Release 4.0B: <i>BC - Basis Components → Computing Center Management System → BC Users and Authorizations → Overview: Creating and Maintaining User Master Records → Displaying Change Documents</i>
[A.31]	<u><i>CA ALE</i></u> Release 3.1H: <i>Cross Application → ALE - Application Link Enabling</i> Release 4.0B: <i>CA - Cross-Application Components → Business Framework Architecture → ALE Integration Technology</i>
[A.32]	<u><i>R/3 Internet Application Components</i></u> Release 3.1H: <i>Cross Application → SAP@WEB → R/3 Internet Application Components</i> Release 4.0B: <i>CA - Cross-Application Components → Business Framework Architecture → Web Basis → R/3 Internet Application Components</i>
[A.33]	<u><i>Remote Communications</i></u> Release 3.1H: <i>Basis Components → ABAP/4 Development Workbench → Remote Communications</i> Release 4.0B: <i>BC - Basis Components → Remote Communications → Remote Communications</i>
[A.34]	<u><i>SAP Business Workflow</i></u> Release 3.1H: <i>Basis Components → Business Engineering Workbench → SAP Business Workflow</i> Release 4.0B: <i>BC - Basis Components → Business Management → SAP Business Workflow</i>
[A.35]	<u><i>SAP Network Security</i></u> Release 3.1H: <i>R/3 Service and Support → SAP Network Security</i> Release 4.0B: not available

B: IMG Path

Ref.No.	Path
[B.1]	<u><i>Implementation Guide</i></u> <i>Basis Components → System Administration → Users and Authorizations → Maintain authorizations and profiles using profile generator</i>

List of References

C: OSS Notes

Ref.No.	OSS Note Number and Title
[C.1]	OSS Note 1916 : Logging table changes in R/3
[C.2]	OSS Note 2467 : Answers on the topic of "Security"
[C.3]	OSS Note 4326 : No user exists with superuser privileges
[C.4]	OSS Note 7642 : Authorization protection of ABAP programs
[C.5]	OSS Note 11796 : Authorization profile P_BAS_ALL and table display
[C.6]	OSS Note 13202 : Security Aspects in ABAP Programming
[C.7]	OSS Note 27928 : Consequences in transport during password change
[C.8]	OSS Note 29276 : SAPCPIC: At which points are passwords visible
[C.9]	OSS Note 30289 : SAProuter documentation
[C.10]	OSS Note 35010 : Service connections: Composite note (overview)
[C.11]	OSS Note 35493 : Secrecy and Data Security Obligations
[C.12]	OSS Note 37724 : Customer exits in SAP logon
[C.13]	OSS Note 40689 : New reports for the User Information System
[C.14]	OSS Note 41731 : Deletion of data in transport directory (2.1/2.2)
[C.15]	OSS Note 41732 : Deletion of data in transport directory (3.0)
[C.16]	OSS Note 43417 : RFC security loophole in 3.0C and 3.0D
[C.17]	OSS Note 46902 : Security Aspects in Remote Access
[C.18]	OSS Note 48736 : Set up ORACLE SQL*Net V2 under Windows NT
[C.19]	OSS Note 50088 : Creating OPS\$ users on Windows NT/Oracle
[C.20]	OSS Note 52937 : Debugging Authorizations (Releases 3.0A to 3.0F!)
[C.21]	OSS Note 60058 : Security for R/3 Release 3.1 on the Internet
[C.22]	OSS Note 63930 : Gateway registration of RFC server program
[C.23]	OSS Note 64016 : Use of the SAP gateway monitor GWMON
[C.24]	OSS Note 65968 : ABAP debugging authorizations as of Release 3.1G
[C.25]	OSS Note 66687 : Network security products SECUDE and Kerberos
[C.26]	OSS Note 67766 : S_TCODE: Authorization check on start transaction
[C.27]	OSS Note 68048 : Deactivating the automatic user SAP*
[C.28]	OSS Note 77503 : Audit Information System (AIS) Version 1.5
[C.29]	OSS Note 80723 : AUTOlogin Shared Library correction
[C.30]	OSS Note 86927 : Use of the digital signature in the R/3 System
[C.31]	OSS Note 92725 : WebReporting and Authorisation group
[C.32]	OSS Note 110600 : SAP Security Library (SAPSECULIB)
[C.33]	OSS Note 100609 : Audit Information System (AIS) - installation
[C.34]	OSS Note 104576 : Package filter (firewall) between ITS and R/3

D: Internet Sites

Ref.No.	Name and Internet Address
General Information	
[D.1]	Computer Emergency Response Team http://www.cert.org
[D.2]	Computer Incident Advisory Capability http://CIAC.llnl.gov
[D.3]	Australian Computer Emergency Response Team http://www.AUSCERT.org.au
[D.4]	Forum of Incident Response and Security Teams http://www.FIRST.org
[D.5]	Cipher: Electronic Newsletter of the Technical Committee on Security & Privacy http://www.itd.nrl.navy.mil/ITD/5540/ieee/cipher
Information Specific for Windows NT	
[D.6]	Microsoft Security Advisor Program http://www.microsoft.com/security
[D.7]	NT Bug Traq http://NtbugTraq.ntadvice.com

E: Other Documentation

Ref.No.	Description
[E.1]	<u>R/3 Report Documentation</u> : RCSCAUTH
[E.2]	<u>SAP Documentation: Authorizations Made Easy Guide</u> : Material Number 50020475 (Release 3.0F) Material Number 50021412 (Release 3.1G/3.1H) Material Number 50023994 (Release 4.0A/4.0B)
[E.3]	<u>SAP Documentation: BC SAP High Availability Guide</u> , Material Number 50018071
[E.4]	<u>SAP Documentation: Leitfaden Datenschutz für SAP R/3</u> . Material Number 50024598 (Germany only)
[E.5]	<u>SAP Documentation: Remote Connections to the R/3 Online Services</u> ; Material Number 50017380
[E.6]	<u>SAP Documentation: The SNC User's Guide</u> , Presentations ITS CD in the directory Docu→ SNC
[E.7]	<u>SAP Documentation: Secure Network Communications and Secure Store & Forward Mechanisms with R/3</u> , Material Number 50014335
[E.8]	<u>SAP ASAP Implementation Roadmap: Work-package 3.11 Establish Authorization Concept; Phase 3: Realization</u>
[E.9]	<u>IBM Documentation: IBM DB2 Universal Database Administration Guide, IBM DB2 Universal Database Troubleshooting Guide</u>
[E.10]	<u>IBM Documentation: OS/400 Security - Basic</u>
[E.11]	<u>IBM Documentation: OS/400 Security - Reference</u>
[E.12]	<u>IBM Documentation: Installing R/3 on IBM AS/400</u>
[E.13]	<u>IBM Documentation: SAP R/3 Implementation for AS/400</u> , Material Number SG24-4672

Index

- A**
- activation administrator 2-18
 - ADABAS 2-73
 - CONTROL operations 2-74
 - passwords 2-73, 2-77, 2-78
 - ADABAS / UNIX 2-74
 - files and directories 2-75, 2-80
 - passwords 2-75, 2-79
 - ADABAS / Windows NT 2-76
 - files and directories 2-76
 - passwords 2-76
 - additional information 2-2, A-1
 - ADABAS 2-80
 - Application Link Enabling (ALE) 2-139
 - authorization concept 2-22
 - Change & Transport System 2-106
 - DB2/400 2-98
 - DB2/CS / UNIX 2-86
 - DB2/CS / Windows NT 2-93
 - INFORMIX/UNIX 2-72
 - logging and auditing 2-123
 - network security 2-36
 - operating system commands in R/3 2-54
 - ORACLE/UNIX 2-63
 - ORACLE/Windows NT 2-69
 - R/3 Online Services 2-141
 - remote communications (RFC & CPI-C) 2-111
 - specific objects 2-144
 - SSF and digital signatures 2-115
 - UNIX 2-42
 - user authentication 2-10
 - Windows NT 2-52
 - AGate 2-127, 2-129, 2-133
 - Application Link Enabling (ALE) 2-128, 2-137
 - authorization trace 2-138, 2-139
 - background processing 2-138
 - distribution model 2-138
 - IDocs 2-137, 2-138, 2-139
 - passwords 2-138
 - users and authorizations 2-137
 - application logging 3-2
 - Audit Info System (AIS) 2-116, 3-2
 - auditing 2-116
 - Audit Info System (AIS) 2-116
 - Security Audit Log 2-117
 - See also logging
 - authority checks 2-11, 2-20, 2-108
 - reducing the scope of 2-21
 - authorization administrator 2-18
 - authorization data administrator 2-17
 - Authorization Infosystem 2-11, 2-15, 2-122, 3-9
 - authorization objects
 - B_ALE_LSYS 2-137, 3-9
 - B_ALE_MAST 2-137, 3-9
 - B_ALE_MODL 2-137, 2-138, 3-9
 - B_ALE_RECV 2-137, 2-138, 3-9
 - B_ALE_REDU 2-137, 3-9
 - S_ADMI_FCD 2-105, 2-108, 2-143, 3-9
 - S_CTS_ADMI 2-105, 3-9
 - S_DEVELOP 2-105, 3-9
 - S_LOG_COM 2-53, 3-9
 - S_RFC 2-109, 2-138, 3-5, 3-9
 - S_RZL_ADM 2-54, 3-9
 - S_TABU_CLI 2-143, 3-9
 - S_TABU_DIS 2-21, 2-137, 2-143, 2-144, 3-9
 - S_TCODE 2-20, 2-21, 2-108, 2-143, 3-4, 3-9
 - S_TOOLS_EX 2-120, 3-9
 - S_TRANSPRT 2-105, 3-10
 - S_USER_AUT 2-19, 3-10
 - S_USER_GRP 2-19, 3-10
 - S_USER_PRO 2-19, 3-10
 - summary 3-9
 - authorization profile administrator 2-17
 - authorization trace 2-138, 2-139
 - authorizations
 - administration tasks 2-16
 - manually 2-18
 - with profile generator 2-17
 - authorizations 2-14
 - changes to 2-122
 - fields 2-14
 - object classes 2-14
 - objects 2-14, 2-15
 - profiles 2-14
 - R/3 authorization concept 2-11
 - S_LOGCOM_ALL 2-53
 - SAP_ALL 2-143
 - SAP_NEW 2-143
 - user master records 2-15
- B**
- BRBACKUP 2-61, 2-66
 - browser certificates 2-133
 - Business Application Programming Interface (BAPI) 2-137
- C**
- CCMS
 - statistic records 2-120
 - certificates
 - See also public-key certificates
 - Certification Authority (CA) 2-113, 2-115, 2-133
 - Change & Transport System 2-99
 - change documents for business objects 3-2
 - change documents for user profiles 3-2

Index

- change options 2-101, 2-102
chdbpass 2-58, 2-62
checklists 1-3
Common Gateway Interface (CGI) 2-126
common transport directory 2-101
consulting services 1-7
CPI-C 2-34, 2-107, 2-108, 2-138
 external server programs 2-110
crypto boxes 2-112, 2-113
cryptography 2-112
- D**
- database access 2-55
 SAPDBA 2-56
 see also the specific database
 using external tools 2-56
DB2/400 2-94
 passwords 2-97, 2-98
 security concept 2-95
 security levels 2-97
DB2/CS / UNIX 2-81
 DB2DB6EKEY 2-81, 2-83
 files and directories 2-84, 2-85
 passwords 2-81, 2-82, 2-85
 SAP-DB2admin operations 2-83
DB2/CS / Windows NT 2-87
 DB2DB6EKEY 2-87, 2-90, 2-92, 2-93
 environment variables 2-90, 2-92, 2-93
 files and directories 2-91
 passwords 2-87, 2-90, 2-92
 users and groups 2-88
DB2DB6EKEY 2-81, 2-83, 2-87, 2-90, 2-93
digital envelopes 2-112
digital signatures 2-112, 2-114
- E**
- emergency changes in productive system 2-105
encryption 2-33, 2-112
- F**
- feedback 1-7
firewall 2-28, 2-34
firewalls 2-127, 2-128, 2-131
- G**
- gateway 2-108, 2-110
GSS-API V2 2-35
- H**
- HR Tables 2-144
HTTP/HTTPS 2-129, 2-133, 2-134
- I**
- IDocs 2-137, 2-138, 2-139
INFORMIX / UNIX 2-70
 files and directories 2-71, 2-72
 passwords 2-70, 2-71
 SAPDBA 2-56
integrity checks on SAPgui 2-142
Internet 2-124
Internet Application Components (IAC) 2-124
 WebReporting 2-136
 WebRFC 2-136
Internet Transaction Server (ITS) 2-124, 2-126, 2-131
 AGate 2-127, 2-129, 2-133
 declaring applications 2-135
 encryption 2-133
 firewalls 2-132
 HTTP 2-133
 HTTPS 2-133
 network infrastructure 2-127, 2-132
 privacy 2-133
 SAProuter 2-130
 security levels 2-135
 session integrity 2-134
 TCP ports 2-129, 2-130
 user authentication 2-134
 WGate 2-126, 2-129, 2-133
- L**
- logging 2-116
 application logging 2-121
 Audit Info System (AIS) 2-116
 change documents for business objects 2-121
 changes to table data 2-122
 changes to user master records 2-122
 Security Audit Log 2-117
 See also auditing
 statistic records 2-120
 System Log 2-118
 workflow execution 2-121
logons 2-7, 2-8, 2-117
- M**
- message server 2-26
Microsoft Information Server API (ISAPI) 2-126
- N**
- Netscape Server API (NSAPI) 2-126
network
 routers and packet filters 2-27
 TCP ports 2-26, 2-27
Network File System (NFS) 2-38
network infrastructure 2-23, 2-127, 2-132
network services 2-25
new topics 1-6
NFS 2-38
NIS 2-38
notations 1-5
- O**
- Online Service System 2-29

Open Database Connectivity (ODBC)	2-56	login/failed_user_auto_unlock	2-7, 2-8, 3-3
operating system	2-37	login/fails_to_session_end	2-7, 2-8, 3-3
Operating System Commands in R/3	2-53	login/fails_to_user_lock	2-7, 2-8, 2-144, 3-3
OPSS\$ connect mechanism	2-57	login/min_password_lng	2-4, 3-3
ORACLE / UNIX	2-57	login/no_automatic_user_sap*	2-5, 2-144, 3-3
chdbpass	2-58, 2-62	login/no_automatic_user_sapstar	3-3
files and directories	2-60, 2-63	login/password_expiration_time	3-3
OPSS\$ connect mechanism	2-57	login/passwords_expiration_time	2-4
passwords	2-57, 2-61, 2-62	rdisp/gui_auto_logout	2-7, 2-8, 3-4
SAPDBA	2-56, 2-61	rdisp/rfc_max_login	3-4
SAPDBA expert mode	2-59	rdisp/rfc_max_own_login	3-4
ORACLE / Windows NT	2-64	rdisp/tm_max_no	3-4
files and directories	2-65	rec/client	2-122, 3-8
OPSS\$ connect mechanism	2-64, 2-67, 2-68	rsau/enable	2-117
passwords	2-64, 2-68	rsau/local/file	2-117
SAPDBA	2-56, 2-66	rsau/max_diskspace_local	2-117
P		rsau/selection_slots	2-117
packet filters	2-27, 2-31, 2-127, 2-128, 2-131, 2-132	rslg/central/file	2-118, 2-119
passwords		rslg/central/old_file	2-118, 2-119
ADABAS	2-73, 2-77, 2-78	rslg/collect_daemon/host	2-119
ADABAS / UNIX	2-75, 2-79	rslg/local/file	2-118, 2-119
ADABAS / Windows NT	2-76	rslg/max_diskspace/central	2-118
ALE users	2-138	rslg/max_diskspace_central	2-119
CPI-C external server programs	2-110	rslg/max_diskspace_local	2-119
database user SAPR3	2-55	snc/accept_insecure_gui	3-5
DB2/ CS / UNIX	2-85	snc/accept_insecure_r3int_rfc	3-5
DB2/400	2-97, 2-98	snc/accept_insecure_rfc	3-5
DB2/CS / UNIX	2-81, 2-82	snc/accept_insecure_spic	3-5
DB2/CS / Windows NT	2-87, 2-90, 2-92	snc/data_protection/min	3-5
INFORMIX / UNIX	2-70, 2-71	snc/data_protection/use	3-5
ORACLE / UNIX	2-57, 2-61, 2-62	snc/data_protection_max	3-5
ORACLE / Windows NT	2-64, 2-68	snc/enable	3-6
R/3 Online Services	2-140, 2-141	snc/gssapi_lib	3-6
R/3 standard user SAPCPIC	2-6	snc/identity/as	3-6
R/3 users	2-3, 2-8, 2-9	snc/permit_insecure_gui	3-5
profile parameters	2-4	snc/permit_insecure_start	3-6
rules	2-3	snc/r3int_rfc_qop	3-6
storage and transport	2-4	snc/r3int_rfc_secure	3-6
UNIX users	2-38	stat/file	2-120, 3-8
personal security environment (PSE)	2-114	stat/level	2-120, 3-8
private keys	2-112, 2-113, 2-114	stat/version	2-120, 3-8
Profile Generator	2-11, 2-12, 2-17	summary	3-3
profile parameters		transport/systemtype	3-6
auth/auth_number_in_userbuffer	3-4	transport/tp_logging	3-6
auth/authorization_trace	3-4	profiles	2-14
auth/no_check_in_some_cases	2-22, 3-4	B_ALE_ALL	2-137
auth/no_check_on_tcode	3-4	changes to	2-122
auth/rfc_authority_check	3-5	P_BAS_ALL	2-144
auth/system_access_check_off	3-5	S_A.ADMIN	2-53
auth/test_mode	3-5	S_A.SYSTEM	2-17, 2-18, 2-53
DIR-INSTANCE	2-114, 3-7	S_CTS_ALL	2-105
gw/max_conn	3-6	S_CTS_DEVELO	2-105
gw/monitor	3-6	S_CTS_PROJEC	2-105
gw/sec_info	2-110, 3-6	S_CTS_SHOW	2-105
gw/stat	3-6	S_USER*	2-18
		SAP_ALL	2-9
		public keys	2-112, 2-113, 2-115

Index

- public-key certificates 2-113, 2-115
public-key infrastructure (PKI) 2-112
- R**
- R/3 Online Services 2-140
passwords 2-140, 2-141
SAProuter 2-140
- R/3 resources
UNIX 2-40
Windows NT 2-50
- releases, valid 1-5
- remote communications 2-107
- remsh/rsh 2-39
- report classes 2-20
- reports
RSCSAUTH 2-20, 3-1
RSFKT100 2-121
RSUSR003 3-1
RSUSR006 2-7, 3-1
RSUSR400 3-5
summary 3-1
- RFC 2-34, 2-107, 2-108, 2-117, 2-137
external server programs 2-26, 2-110
- RFC authorizations 2-109
- RFC Software Development Kit 2-108
- RFC trusted systems 2-109
- RFC-API 2-107
- rlogin 2-39, 2-58
- routers 2-27, 2-31, 2-128, 2-132
- S**
- SAP Business Workflow 3-2
- SAP Logon Pad 2-8
- SAP Network Interface (NI) 2-127
- SAP Security Library (SAPSECULIB) 2-112, 2-114
- SAP Shortcuts 2-8
- SAP_ALL 2-143
- SAP_NEW 2-143
- SAPDBA 2-56, 3-2
expert mode 2-59
ORACLE 2-61
- SAPgui 2-26, 2-34
integrity checks 2-142
- SAPlpd 2-26, 2-34
- SAProuter 2-27, 2-29, 2-34, 2-127, 2-130, 2-140
- secinfo 2-110
- Secure Network Communications (SNC) 2-32, 2-108, 2-111, 2-133
- Secure Sockets Layer protocol (SSL) 2-133
- Secure Store & Forward (SSF) 2-112
- Security Audit Log 2-7, 2-117, 2-118
- security policy 1-1, 1-3
- security toolbox 2-1
- server certificates 2-133
- Session Manager 2-8
- smart cards 2-112, 2-113
- standard users 2-5
DDIC 2-6, 2-9
EARLYWATCH 2-7, 2-9
SAP* 2-5, 2-9
SAPCPIC 2-6, 2-9
- statistic records 2-120, 3-2
- support 1-7
- System Log 2-8, 2-118, 3-2
- system profiles 2-144
- T**
- table classes 2-21
- table recording 2-122, 3-2
- tables
DBTABPRT 2-122
RFCDES 2-55, 2-108
SAPUSER 2-55, 2-57, 2-70, 2-71
T000 2-9, 2-55, 2-143
TDDAT 2-21
USOBT 2-22
USOBX 2-22
USR* 2-55
USR40 2-9
- TCP ports 2-128, 2-129, 2-130
- third-party products 2-35, 2-112
- threats 1-1
- tools
summary 3-1
- transactions
BD87 2-139
PFCG 2-12, 3-1
RZ11 2-119, 2-144, 3-3
SALE 2-137
SCC4 2-143
SCD0 2-121, 3-2
SCU3 2-122, 3-2
SE03 2-101
SE06 2-101, 2-102
SE09 2-103, 3-2
SE10 2-103, 3-2
SE11 2-121
SE16 2-144
SE38 2-105
SE93 2-20
SECR 2-117, 3-2
SLG0 2-121, 3-2
SLG1 2-121, 3-2
SM18 2-7, 2-118, 3-1, 3-2
SM19 2-7, 2-118, 3-1, 3-2
SM20 2-7, 2-118, 3-1, 3-2
SM21 2-118, 2-119, 3-1, 3-2
SM30 2-9, 2-143
SM31 2-143
SM49 2-53
SM52 2-105
SM59 2-108, 2-138

SM69	2-54	DB2/400	2-98
SMW0	2-136	DB2/CS / UNIX	2-85
ST01	2-139	DB2/CS / Windows NT	2-92
STAT	2-120, 2-140, 3-2	INFORMIX/UNIX	2-71
STMS	2-99, 3-2	ORACLE/UNIX	2-61
SU01	2-122, 2-138, 3-2	ORACLE/Windows NT	2-67
SU24	2-21, 2-22	user authentication	2-9
SU25	2-22	user administrator	2-17, 2-18
SUIM	2-15, 2-17, 2-18, 3-1, 3-9	user authentication	2-3, 2-134
summary	3-1	user master records	2-15, 2-117
SUPC	2-18	changes to	2-122
SWI1	3-2	V	
SWI2	2-121	virus protection	2-142
SWI5	2-121, 3-2	W	
Transport Management System	2-99, 3-2	WebReporting	2-136
transport path	2-103	WebRFC	2-136
transporting		WGate	2-126, 2-129, 2-133
responsibilities and authorizations	2-104	Windows NT	2-43
U		domain concept	2-48
UMASK	2-41	groups	2-43
UNIX	2-37	R/3 resources	2-50
Network File System (NFS)	2-38	trusted domain	2-49
passwords	2-38	users	2-45
R/3 resources	2-40, 2-41	Workbench Organizer	2-103, 3-2
remsh/rsh	2-39	X	
rlogin	2-39, 2-58	X.509 certificates	2-133
SUID/SGID	2-38	Y	
UMASK	2-41	Yellow Pages (NIS)	2-38, 2-61, 2-71
Yellow Pages (NIS)	2-38, 2-61, 2-71		
useful procedures			
ADABAS	2-77		
Application Link Enabling (ALE)	2-139		

