



SAP NetWeaver '04  
Security Guide

Database Access  
Protection: IBM DB2  
Universal Database  
for iSeries

Document Version 1.00 – April 29, 2004



SAP AG  
Neurottstraße 16  
69190 Walldorf  
Germany  
T +49/18 05/34 34 24  
F +49/18 05/34 34 20  
[www.sap.com](http://www.sap.com)

© Copyright 2004 SAP AG. All rights reserved.

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

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

Microsoft, Windows, Outlook, and PowerPoint are registered trademarks of Microsoft Corporation.

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

Oracle is a registered trademark of Oracle Corporation.

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

Citrix, ICA, Program Neighborhood, MetaFrame, WinFrame, VideoFrame, and MultiWin are trademarks or registered trademarks of Citrix Systems, Inc.

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

Java is a registered trademark of Sun Microsystems, Inc.

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

MaxDB is a trademark of MySQL AB, Sweden.

SAP, R/3, mySAP, mySAP.com, xApps, xApp, SAP NetWeaver, and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world. All other product and service names mentioned are the trademarks of their respective companies. Data contained in this document serves informational purposes only. National product specifications may vary.

These materials are subject to change without notice. These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

#### **Disclaimer**

Some components of this product are based on Java™. Any code change in these components may cause unpredictable and severe malfunctions and is therefore expressly prohibited, as is any decompilation of these components.

Any Java™ Source Code delivered with this product is only to be used by SAP's Support Services and may not be modified or altered in any way.






#### **Documentation in the SAP Service Marketplace**

You can find this documentation at the following Internet address:  
[service.sap.com/securityguide](http://service.sap.com/securityguide)

## Typographic Conventions

| Type Style          | Description  |
|---------------------|--|
| <i>Example Text</i> | Words or characters quoted from the screen. These include field names, screen titles, pushbuttons labels, menu names, menu paths, and menu options.<br><br>Cross-references to other documentation                               |
| <b>Example text</b> | Emphasized words or phrases in body text, graphic titles, and table titles   |
| EXAMPLE TEXT        | Technical names of system objects. These include report names, program names, transaction codes, table names, and key concepts of a programming language when they are surrounded by body text, for example, SELECT and INCLUDE. |
| Example text        | Output on the screen. This includes file and directory names and their paths, messages, names of variables and parameters, source text, and names of installation, upgrade and database tools.                                   |
| <b>Example text</b> | Exact user entry. These are words or characters that you enter in the system exactly as they appear in the documentation.  |
| <Example text>      | Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system.   |
| EXAMPLE TEXT        | Keys on the keyboard, for example, F2 or ENTER.  |

## Icons

| Icon   | Meaning        |
|--|----------------|
|  | Caution        |
|  | Example        |
|  | Note           |
|  | Recommendation |
|  | Syntax         |

Additional icons are used in SAP Library documentation to help you identify different types of information at a glance. For more information, see *Help on Help* → *General Information Classes and Information Classes for Business Information Warehouse* on the first page of any version of *SAP Library*.

## Contents

|  |           |
|--|-----------|
| <b>IBM DB2 Universal Database for iSeries .....</b>                | <b>5</b>  |
| <b>1 General Description of the DB2 UDB for iSeries Security</b>   |           |
| <b>Concept .....</b>   | <b>6</b>  |
| <b>1.1 User and Group Profiles .....</b>                           | <b>7</b>  |
| <b>1.2 Properties of Objects Created During Installation .....</b> | <b>8</b>  |
| <b>1.3 Security Levels .....</b>                                   | <b>9</b>  |
| <b>2 Changing Passwords of the Database Standard Users .....</b>   | <b>9</b>  |
| <b>3 Additional Information on DB2 UDB for iSeries.....</b>        | <b>10</b> |

# IBM DB2 Universal Database for iSeries

The following list describes an overview of the sections that describe the measures that you take for IBM DB2 Universal Database for iSeries:

- [General Description of the DB2 UDB for iSeries Security Concept \[Page 5\]](#)
- [User and Group Profiles \[Page 7\]](#)
- [Properties of Objects Created During Installation \[Page 8\]](#)
- [Security Levels \[Page 9\]](#)
- [Changing Passwords of the Database Standard Users \[Page 9\]](#)
- [Additional Information on DB2 UDB for iSeries \[Page 10\]](#)

## Naming Conventions

In this documentation, the following naming conventions apply.

### **IBM eServer iSeries**

*IBM eServer iSeries* is referred to as *iSeries*.

*IBM eServer iSeries* was formerly called *IBM AS/400*.

### **IBM DB2 Universal Database for iSeries**

*IBM DB2 Universal Database for iSeries* is referred to as *DB2 UDB for iSeries*.

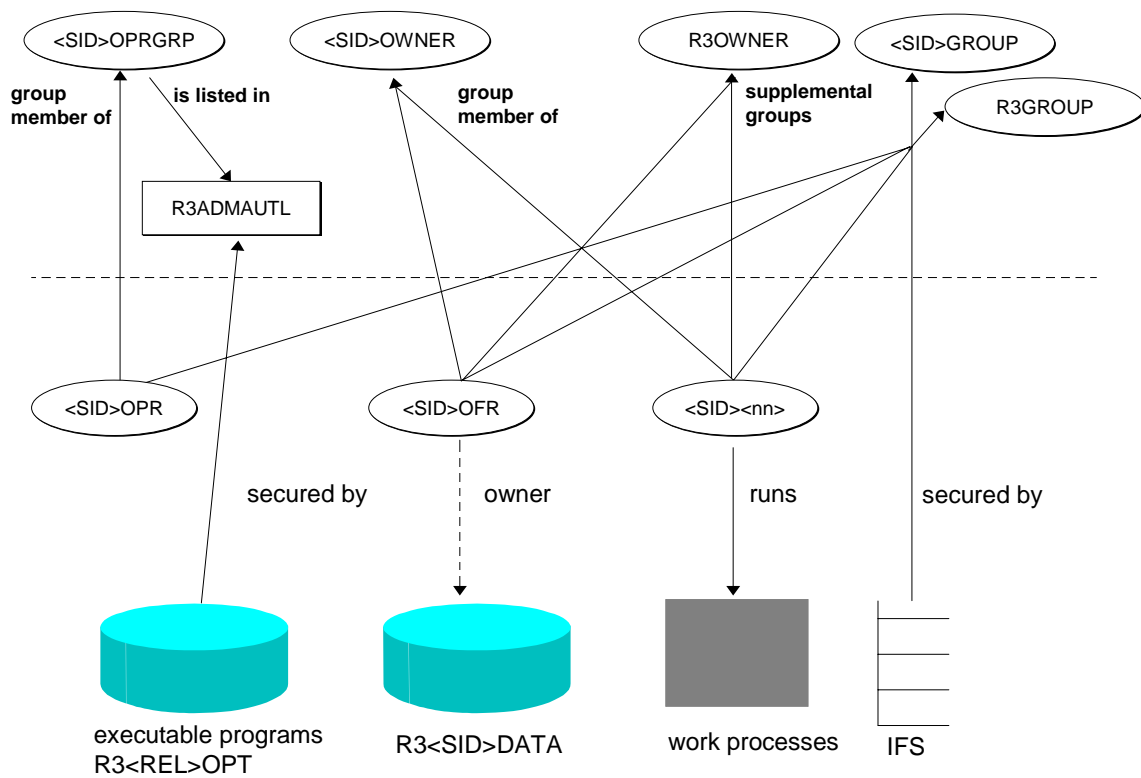
*IBM DB2 Universal Database for iSeries* was formerly called *IBM Universal Database for AS/400*.

1 General Description of the DB2 UDB for iSeries Security Concept

# 1 General Description of the DB2 UDB for iSeries Security Concept

The graphic below shows the user security concept for SAP systems on iSeries at the operating-system level.

**IBM DB2 Universal Database for iSeries User Security Concept**



For compatibility reasons, the group profiles  $\text{R3OWNER}$  and  $\text{R3GROUP}$  continue to exist. These profiles are primary group profiles in Release 3.x and 4.0.

**1 General Description of the DB2 UDB for iSeries Security Concept**

Depending on the users and groups in the DB2 UDB for iSeries security concept, the following supplemental groups apply:

| User      | Group Member of | Supplemental Groups  |
|-----------|-----------------|--|
| SID>OPR   | <SID>OPRGRP     | <ul style="list-style-type: none"> <li>• &lt;SID&gt;GROUP</li> <li>• R3GROUP</li> </ul>                    |
| <SID>OFR  | <SID>OWNER      | <ul style="list-style-type: none"> <li>• &lt;SID&gt;GROUP</li> <li>• R3GROUP</li> <li>• R3OWNER</li> </ul> |
| <SID><nn> | <SID>OWNER      | <ul style="list-style-type: none"> <li>• &lt;SID&gt;GROUP</li> <li>• R3GROUP</li> <li>• R3OWNER</li> </ul> |

For additional information regarding the individual user and group profiles, see the following sections:

- [User and Group Profiles \[Page 7\]](#)
- [Properties of Objects Created During Installation \[Page 8\]](#)
- [Security Levels \[Page 9\]](#)

## 1.1 User and Group Profiles

### User Profiles

#### <SID>OPR

<SID>OPR (system operator) is the SAP system administrator's user profile. This user is only allowed to do administrative tasks such as starting and stopping SAP system 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 SAP system superuser's profile. This user has all authorizations for the SAP system and its database R3<SID>DATA. <SID>OFR can perform all the tasks that it is authorized to perform and it has certain additional authorizations. However, <SID>OFR has no special authorizations outside the SAP system environment. It also has no special authorizations to other SAP systems (with different SAP system IDs) that may run on the same iSeries. Note that <SID>OFR is not the same as QSECOFR, which is the superuser for the iSeries system.

## 1 General Description of the DB2 UDB for iSeries Security Concept

### <SID><nn> / SAP<nn>

<SID><nn> is the user that runs the work processes for the SAP system. In Releases 3.x and 4.0, the processes are run by user SAP<nn> (<nn> represents the instance number). The objects created by this user belong to the corresponding group <SID>OWNER or R3OWNER.

### Group Profiles

#### <SID>OPRGRP

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

#### <SID>OWNER / R3OWNER

<SID>OWNER is the default owner of the SAP system libraries and all SAP system objects. You cannot sign on as user <SID>OWNER. It is the group profile for <SID><nn> and <SID>OPR.

#### <SID>GROUP / R3GROUP

<SID>GROUP is the primary group for the SAP System Integrated File System (IFS) objects. This group is the supplemental group for all other user profiles generated by the SAP system. Its only purpose is to authorize SAP system users access to IFS objects.

### Superuser for iSeries

#### QSECOFR

QSECOFR is the superuser for iSeries. This user is not necessary to run and maintain the SAP system.

### Additional Information

For more information on the user and group concept for DB2 UDB for iSeries, see **SAP Note 46063** (lower than 4.0) and **SAP Note 173579** (higher than 4.5).

## 1.2 Properties of Objects Created During Installation

The following applies to the objects created during the SAP system installation:

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



## 1.3 Security Levels

The security level system value (`QSECURITY`) specifies the level of security to be enforced on the iSeries system. Changes to this value take effect at the 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 iSeries system is shipped at security level 40, which provides sign-on and resource security as well as integrity protection.

If you want to change the security level, use the Work with System Values (`WRKSYSVAL`) command. Although you can use level 30 for operating SAP systems, we recommend using level 40. For more information on SAP installation documentation, see SAP Marketplace at [service.sap.com/instguides](http://service.sap.com/instguides).

## 2 Changing Passwords of the Database Standard Users

The following section provides information on the database standard users, whose passwords you need to change. The users are as follows:

### Database Standard Users

| User      | Function                          | Command Used to Change Password or Profile                                      |
|-----------|-----------------------------------|---|
| <SID>OPR  | SAP system administrator          | <ul style="list-style-type: none"> <li>• CHGPWD</li> <li>• CHGUSRPRF</li> </ul> |
| <SID>OFR  | SAP system superuser              | <ul style="list-style-type: none"> <li>• CHGPWD</li> <li>• CHGUSRPRF</li> </ul> |
| <SID><nn> | User that runs the work processes | <ul style="list-style-type: none"> <li>• CHGUSRPRF</li> </ul>                   |

### 3 Additional Information on DB2 UDB for iSeries

#### Procedure



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

To change the passwords for <SID>OFR and <SID>OPR, proceed as follows:

1. Sign on to the database server as user <SID>OFR or <SID>OPR.
2. In the command line, enter the following command:  
**CHGPWD**
3. Enter the old and new passwords.
4. If you want to change the user profile, enter the following command:

**CHGUSRPRF**

If you are using distributed directories on multiple iSeries systems using /QFileSvr.400, you must use the same passwords on all iSeries systems for each of the users <SID>OPR, <SID>OFR, and <SID><nn>.

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

## 3 Additional Information on DB2 UDB for iSeries

You can find additional information on iSeries in the table below:

| Type                           | Number             | Title  |
|--------------------------------|--------------------|--|
| SAP Library                    | —                  | <a href="#">SAP Database Guide: IBM DB2 Universal Database for iSeries</a>   |
| SAP Notes                      | 46063              | AS/400: Authorization problems with R/3 on   |
|                                | 173579             | AS/400: Authorization concept for R/3 on AS/400  |
| SAP Installation Documentation | —                  | For more information on SAP installation documentation, see <i>SAP Marketplace</i> at <a href="http://service.sap.com/instguides">service.sap.com/instguides</a> → SAP Web Application Server → <Release>. |
| SAP Press                      | ISBN<br>3934358225 | Sicherheit und Datenschutz mit SAP-Systemen (in German only)   |

**Other Documentation**

| Type                              | Number    | Description  |
|-----------------------------------|-----------|--|
| IBM Documentation                 | SG24-4672 | <i>SAP R/3 Implementation for AS/400</i>   |
|                                   | —         | OS/400 Security – Basic  |
|                                   | —         | OS/400 Security – Reference  |
| IT Governance Institute           | —         | Control Objectives for Information and Related Technology (COBIT). For more information, see the following Internet address:<br><br><a href="http://isaca.org/cobit.htm">isaca.org/cobit.htm</a> |
| Microsoft SQL Server Books Online | —         | Download from the following Internet address:<br><a href="http://microsoft.com/SQL/productinfo/70books.htm">microsoft.com/SQL/productinfo/70books.htm</a>  |