



SAP NetWeaver 2004s SPS 4
Security Guide

SAP Knowledge Warehouse Security Guide

Document Version 1.00 – October 24, 2005



SAP AG
Neurottstraße 16
69190 Walldorf
Germany
T +49/18 05/34 34 24
F +49/18 05/34 34 20
www.sap.com

© Copyright 2005 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

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. Cross-references to other documentation
Example text	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.
Example text	Exact user entry. These are words or characters that you enter in the system exactly as they appear in the documentation.
<Example text>	Variable user entry. 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

SAP Knowledge Warehouse Security Guide	5
1 Introduction	5
2 Technical System Landscape	7
3 User Administration and Authentication	8
3.1 User Management	8
3.2 Integration Into Single Sign-On Environments.....	9
4 Authorizations	9
5 Network and Communication Security	10
5.1 Communication Channel Security	10
5.2 Network Security	10
5.3 Communication Destinations.....	11
6 Data Storage Security	11
7 Minimal Installation	12
8 Other Security-Relevant Information	12
9 Trace and Log Files	13
10 Appendix	13

SAP Knowledge Warehouse Security Guide

1 Introduction



This guide does not replace the daily operations handbook that we recommend customers to create for their specific productive operations.

About this Guide

This guide provides an overview of the security issues you need to keep in mind if you intend to run your SAP Knowledge Warehouse scenarios in a secure environment.

To run SAP Knowledge Warehouse in a secure environment, you need to refer to the security guides of all the components that you are using for your SAP KW scenarios.

The following components are part of the solution SAP Knowledge Warehouse 7.0:

- SAP Web Application Server
- SAP J2EE Engine
- SAP Content Server
- SAP Enterprise Portal
- SAP Content Management with Search & Classification (TREX)
- SAP Internet Transaction Server

Related Security Guides

Application / Component	Guide
SAP Web Application Server	SAP Web Application Server Security Guide [SAP Library]
SAP J2EE Engine	SAP Web AS Security Guide for J2EE Technology [SAP Library]
SAP Content Server	SAP Content Server Security Guide [SAP Library]
SAP Enterprise Portal	Portal Platform Security Guide [SAP Library]
SAP Content Management with Search & Classification (TREX)	Knowledge Management Security Guide [SAP Library]
SAP Internet Transaction Server	Internet Transaction Server Security [SAP Library]

1 Introduction

Why Is Security Necessary?

If you are using your SAP Knowledge Warehouse system to store productive data, you need to ensure that this data is stored securely and can be recovered in case of a system crash or other events that might lead to data loss without preventive measures.

In addition, you need to take into account access restrictions for the information stored in your system – not every system user should have (read / write / administrative) access to all information. Such access restrictions can also be a legal requirement that you need to fulfill.

Target Groups

- Technical consultants
- System administrators

This document is not included as part of the Installation Guides, Configuration Guides, Technical Operation Manuals, or Upgrade Guides. Such guides are only relevant for a certain phase of the software life cycle, whereby the Security Guides provide information that is relevant for all time frames.

Important SAP Notes

Consider the following SAP Notes if you plan to run your SAP Knowledge Warehouse system in a secure environment.



Check regularly which SAP Notes are available about the security of the application.

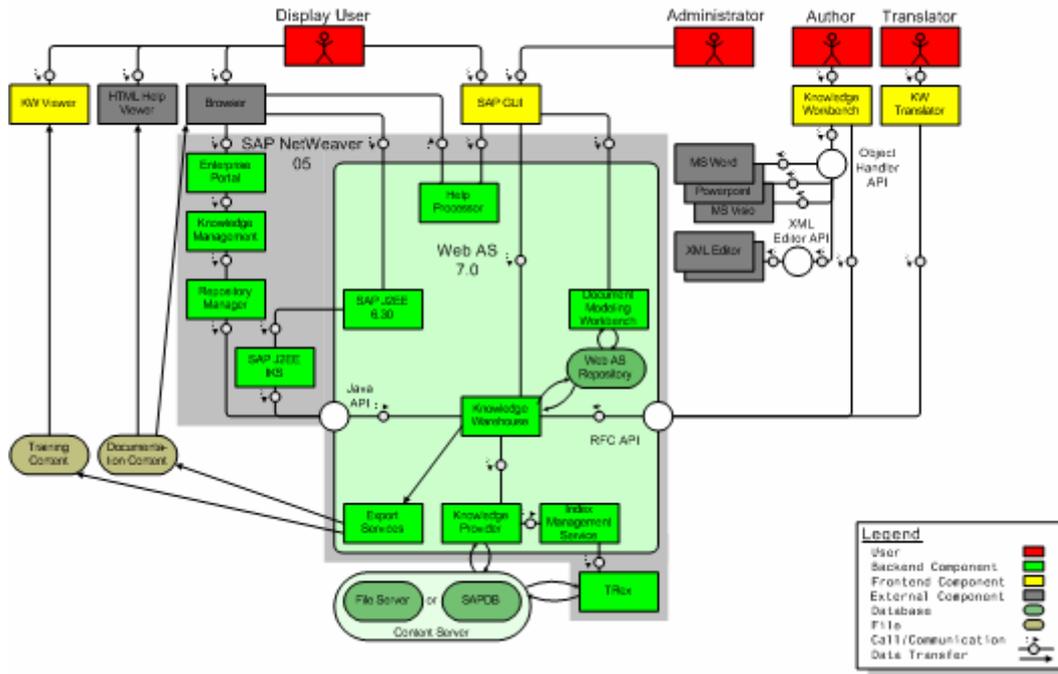
Important SAP Notes

SAP Note Number	Title	Comment
670108	SAP KW 7.0 Security Overview	A collection of security issues that are not (yet) taken over into this security guide.

2 Technical System Landscape

The following diagram gives an overview of the technical SAP KW landscape.

Knowledge Warehouse Components



The following table shows where you can find more information about the technical system landscape of SAP systems:

More Information About the Technical System Landscape

Topic	Guide/Tool	Quick Link to the SAP Service Marketplace (service.sap.com)
Application and industry-specific components such as SAP Financials and SAP Retail, Technology components such as SAP Web Application Server	Master Guide	instguides
Technical configuration, High availability	Technical Infrastructure Guide	ti
Security	Security Guide	security

3 User Administration and Authentication

For basic information about user administration and authorizations, refer to the SAP Web Application Server and the SAP User Management Engine documentation.

3.1 User Management

The following tools are used for user administration and management in SAP KW:

User Management Tools

Tool	Detailed Description	Prerequisites
SAP Web Application Server 6.40: Transaction PFCG (Role Maintenance)	For a detailed description, refer to the SAP Web Application Server 6.40 documentation.	The technical roles of the users within the scenarios should be adapted to the roles of the users in your company.
SAP User Management Engine 4.0	For a detailed description, refer to the SAP User Management Engine 4.0 documentation.	The roles and users in the SAP Web Application Server 6.40 must be defined.

The following user types are used in the SAP Knowledge Warehouse:

- Technical users: Service users, Communication users, Background users
- Individual users: Dialog users, Internet users

SAP KW does not deliver any users in addition to the standard users delivered with SAP Web AS 6.40. The same users needed for a standard SAP Web AS 6.40 installation are needed for a SAP KW 7.0 installation. For further information (such as how to provide users with their passwords and / or certificates), refer to the SAP Web AS 6.40 documentation.

The system administrator should create technical and administrative users during and after the installation.

If you use the SAP KW system to create your own info objects, the creation and maintenance of users is an ongoing process, as new authorizations are often needed when a new project is started or a completed project is “closed”. In this case, you should assign a user administrator who has an overview of the different tasks of different users and can adjust the authorizations as needed.

In a typical SAP KW scenario, the following dialog users typically are needed:

- KW administrators: These users are not technical system administrators. Instead, they administer the status of the documents (such as ‘Released’ or ‘In progress’) and create new folders when new projects are started.
- KW authors: These users have the authorization to create and maintain documents (restricted to specific areas) in folders for which they have the authorization to do so.
- KW translators: These users have the authorization to translate objects that were released by KW administrators.

- KW display users: These are users that have the authorization to display KW content. The authorization can be restricted to areas and folder groups.
- Technical users: These are users created for enabling the connection between the different components (such as the SAP J2EE Internet Knowledge Servlet). The users are created in the SAP Web AS 6.40. The SAP User Management Engine must get the authorization data from the corresponding SAP Web AS. The user is stored in the configuration file `web.xml` in the SAP J2EE services directories.

If you call the documentation from an application system, the technical user used for the connection is stored in the RFC destination.

3.2 Integration Into Single Sign-On Environments

For information about the integration into single sign-on environments, refer to the SAP Web Application Server 6.40 documentation.

4 Authorizations

The authorizations in SAP KW are assigned using transaction PFCG (Role Maintenance) within the SAP Web Application Server 6.40 or the SAP User Management Engine 4.0 (as part of the SAP J2EE Engine). All roles and authorization objects available within SAP Web AS are also available in SAP KW 7.0 and can be used for authentication.

The following roles are delivered with SAP KW 7.0:

User Roles in SAP KW

Technical name	Description
SAP_KM_KW_ADMINISTRATOR	SAP KW Administrator
SAP_KM_KW_ALL_AREAS_DISPLAY	Display all existing documents
SAP_KM_KW_ALL_AREAS_EDIT	Display and change documents in all areas
SAP_KM_KW_ALL_AREAS_TRANSLATE	Translate documents from all areas
SAP_KM_KW_CREATE_OFFLINE	Create offline presentation
SAP_KM_KW_EXPORT_SERVICES	Export HTML
SAP_KM_KW_IWBHELP_EDIT	Change and display in documentation area
SAP_KM_KW_IWBMISC_EDIT	Change and display in management area
SAP_KM_KW_IWBTRAIN_EDIT	Change and display in training area
SAP_KM_KW_KWNET_EDIT	Change and display in HTML-based documents
SAP_KM_KW_MODEL_ALL	Administrator of SAP KW document models (has all authorizations)
SAP_KM_KW_MODEL_DSP	Administrator of KW document models (has display authorization)
SAP_KM_KW_QM_ADMINISTRATOR	Administrator for QM documents
SAP_KM_KW_QM_DISPLAY_EXTERN	Display QM documents (external employee or customer)

5 Network and Communication Security

Technical name	Description
SAP_KM_KW_QM_DISPLAY_INTERN	Display QM documents (internal employee or auditor)
SAP_KM_KW_QM_EDITOR	Display and change QM documents
SAP_KM_KW_QM_TRANSLATE	Translate QM documents
SAP_KM_KW_QUALITY_CONTROL	Quality control
SAP_KM_KW_REMOTE_SUPPORT	Remote support for SAP KW
SAP_KM_KW_RFC_CPIC_USER	Infrep-User for KPro Web server
SAP_KM_KW_XML_TRAIN_EDIT	Change and display in XML training area

Whether or not you use any of the roles listed above, depends on the relevance of each for the scenarios or areas you use.

5 Network and Communication Security

In general, the network and communication security for the SAP KW 7.0 is provided by the components that are part of the solution. For an overview of the SAP KW system landscape and information about network connections, see [Technical System Landscape \[Page 7\]](#).

For further information about ports and protocols, refer to the corresponding component documentation.

5.1 Communication Channel Security

Communication channel security is generally provided by the individual components. For more information, refer to the documentation of the individual components.

5.2 Network Security

Network security is generally provided by the individual components. For more information, refer to the documentation of the individual components.

5.3 Communication Destinations

Connection Destinations

Destination	Delivered?	Type	User, Authorizations	Description
IMSDEFAULT	No	RFC	No user needed	For additional information, see the <i>SAP KW Business Scenario Configuration Guide</i> .

If you want to use SAP KW to supply your application help using the dynamic help option, you need to configure SAP connections between the relevant application systems and the SAP KW system. Refer to the SAP Web Application Server documentation for a description of how to create such connections.

You need to configure the connection between the SAP Web Application Server and the SAP J2EE Engines you are using. For further information, refer to the SAP Web AS and the SAP J2EE Engine documentation.

6 Data Storage Security

Info object data

SAP Knowledge Warehouse data is stored in two places:

- The meta data of info objects is stored in the SAP Web Application Server database. This includes data typically stored in the SAP Web AS, such as user data.
- The physical info objects (in, for example, Microsoft Word or PowerPoint format) are stored on the SAP Content Server – either in a SAP DB or on file system level.

For relevant information concerning the security of this data, see the security guides for SAP Web Application Server 6.40, the SAP Content Server, or the SAP DB.

To have a consistent backup of your SAP KW system, adjust the backup cycles for the SAP Web AS system and the SAP Content Server. To be able to do a point-in-time recovery of the system, both backups need to have the same time stamp.



If you store productive data in your SAP KW system and create your own info objects, SAP strongly recommends to run the SAP Content Server with a SAP DB and not to store the data on a file system. In the latter case, it is not possible to write logs and to execute a time-in-point recovery.

Index data

Index data is stored in Search and Classification (TREX) 6.0, the search engine used for full text search in SAP KW. If you need the full text search for productive use of your SAP KW installation, we recommend that you back up the index categories as described in the TREX administration guide.

7 Minimal Installation

Configuration data

Configuration data is stored on the SAP Internet Knowledge Servlet (IKS). We recommend that you secure this data according to SAP J2EE Engine security standards.



If you customized the layout of the SAP IKS framesets or stylesheets, we recommend that you make a file system backup of the folders where this data is stored. For information on a backup strategy for the SAP J2EE Engine and its services, see the SAP J2EE Engine documentation.

Frontend storage

If you are an author working with the Knowledge Workbench, info objects you edit are stored on your local PC (or a shared drive) in the so-called local repository. You can edit these objects without maintaining a connection with the SAP KW system. For updating the info object in the SAP KW system, the data is checked into SAP KW from the local repository. To ensure that such data is not lost during the time you have the objects checked out, follow your general procedure for securing data stored on a user's frontends.

7 Minimal Installation

SAP KW does not deliver any functions or programs that can be deactivated or removed.

For information on removing or deactivating functions and programs (if available), refer to the security guides of the relevant components.

8 Other Security-Relevant Information

Active code

Active code is used in the SAP KW frontend in the following components:

Knowledge Workbench:

- Microsoft Word VBA Macros (signed)
- Microsoft PowerPoint VBA Macros (signed)
- Arbortext Epic Editor ACL Scripts (unsigned)
- Altova Authentic (unsigned)

Online editing:

- Microsoft Word VBA Macros (signed)
- Microsoft PowerPoint VBA Macros (signed)

Printing:

- Microsoft Word VBA Macros (signed)

Translation with Microsoft Word / Trados:

- Microsoft Word VBA Macros (signed)
- Microsoft PowerPoint VBA Macros (signed)

The signed macros need to be installed on the user's frontend according to the procedure described in SAP Note 368963. For additional information, see SAP Note 368861.

9 Trace and Log Files

Trace or log files are written by the individual SAP KW components.

For further information on trace and log files, see the individual components' guides and documentation.

10 Appendix

Related Security Guides

You can find more information about the security of SAP applications on the SAP Service Marketplace, quick link [security](#). Security guides are available using the quick link [securityguide](#).

Related Information

For more information about topics related to security, see the links shown in the table below.

Quick Links to Related Information

Content	Quick Link on the SAP Service Marketplace (service.sap.com)
Master Guides, Installation Guides, Upgrade Guides, Solution Management Guides	instguides ibc
Related SAP Notes	notes
Released platforms	platforms
Network security	network securityguide
Technical infrastructure	ti
SAP Knowledge Warehouse 7.0	kw70