SAP NetWeaver 2004s SPS 4

Security Guide

Knowledge Management 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

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 expressively 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
Example Text	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

Knowledge Management Security Guide 5
1 User Administration and Authentication 6
2 Permissions 7
3 Communication Channel Security 9
4 Data Storage Security 11
5 Overview of KM Services 13
6 Minimal Configuration 17
7 Further Security-Relevant Information 18
8 Trace and Log Files 19

Knowledge Management Security Guide

About this Guide

This section describes the topics relevant to the security of Knowledge Management (KM) in the *Enterprise Portal* usage type.

The KM security aspects described here prevent illegal access to documents and settings and prevent them being manipulated illegally.

Validity

The information here is applies to all scenarios and scenario variants that implement the Enterprise Portal usage type.

In addition, the information also applies to the following scenarios and scenario variants:

- Enterprise Knowledge Management
- Content Integration and Management
- Content Creation, Publication, and Access

Related Security Guides

Because Knowledge Management is implemented in conjunction with the stand-alone engine *Search and Classification (TREX)*, you must also read the Search and Classification (TREX) Security Guide [SAP Library].

The table below contains links to further related security guides:

Application	Guide	Relevant Sections/Specific Constraints
SAP Web Application Server	SAP NetWeaver Application Server Security Guide [SAP Library]	SAP NetWeaver Application Server Java Security Guide [SAP Library]
Portal	Portal Security Guide [SAP Library]	
Collaboration	Collaboration Security Guide [SAP Library]	

Important SAP Notes

Check frequently to see which SAP notes for the security of your application are available.

Important SAP Notes

SAP Note Number	Title	Comments
864172	SAP NetWeaver 2004s Documentation	Contains information on corrections to the documentation after it has been delivered.
701097	SAP NetWeaver '04 Documentation	Contains information on corrections to the documentation after it has been delivered.
599425	EP6: Permissions for Knowledge Management	After the installation you have to restrict permissions for accessing folders and documents.

1 User Administration and Authentication

User Management

Knowledge Management (KM), like the portal, uses the user management of the J2EE Engine, since it does not have its own user management.

The following services users are used internally:

User	Delivered?	Type	Default Password	Description
cmadmin_service	Yes	Service user	-	Used for various tasks in KM. The service user has write permissions to create a personal folder for every user in the repository `/userhome` and to create configuration settings at start up.
ice_service	Yes	Service user	-	Used to access documents with the content exchange service.
index_service	Yes	Service user	-	Used for crawling and indexing documents with the index management service.

User	Delivered?	Type	Default Password	Description
notificator_service	Yes	Service user	-	Used by the inbox and notification services.
subscription_service	Yes	Service user	-	Used by the subscription service.
timebasedpublish_ service	Yes	Service user	-	Used by the time-dependent publishing service.
collaboration_service	Yes	Service user	-	Used by KM repository services such as the feedback and rating services.

Service users in KM have various system-wide permissions, including resource permissions such as read, write, and delete, and the permission for removing locks on documents. Service users are automatically created by the services in the user management of the J2EE Engine. However, no authentication is possible. For more information, see Service Users [SAP Library].

Also refer to User Administration and Authentication [SAP Library] in the SAP NetWeaver™ security guide.

2 Permissions

Roles

The following roles are used in Knowledge Management (KM):

Role	Description
Content Manager	The *Content Manager* role allows users to structure and manage content. This role must be assigned to relevant users after the installation. For more information, see Assigning the Content Manager Role [SAP Library].
System Administrator	The *System Administrator* role in the *portal* now contains KM-specific administration functions. A *system administrator* performs the KM configuration (see System Administration [SAP Library]).
Content Administrator	The *Content Administrator* role in the *portal* now contains KM-specific content administration functions. It allows direct access to all folders and documents that are stored in internal or external repositories (see the Content Manager Guide [SAP Library]).

You can delegate the task areas to other roles. For more information see Delegated Administration [SAP Library].

Restricting access permissions only by using the role concept or worksets is not sufficient. You should also use ACLs.

ACLs

In addition to the role concept, another authorization concept is used – *access control lists (ACLs).*

Do not confuse the Knowledge Management ACLs with the ACLs used in the portal catalog (PCD).

KM uses repository managers that use various types of data store, such as file systems and WebDAV servers. KM has a uniform way of managing content that is located in different repositories. Initially, all users have full access to this content. If you activate a security manager for a repository, you can protect the content of the repository in question using an access control list.

Subordinate folders inherit permissions (ACLs) from superordinate folders. However, if you change the permissions for a subordinate folder, the system creates a separate ACL for the folder in question. Changes to the superordinate folder are then no longer inherited by the subordinate folder, which now has its own ACL.

You should restrict access permissions on the root nodes of security-relevant repositories **immediately after the installation** or after configuring new repository managers in order to prevent documents being read illegally by users hacking or guessing document URLs (see SAP Note 599425). Change the ACLs for subordinate folders if different permissions apply for these folders.

The restrictions are particularly important for the repository `/etc`, because this is where system and configuration data is stored.

Implementing ACLs early on prevents users with standard permissions from changing permissions themselves.

If you activated the parameter `Preserve Version Histories` in the configuration of CM repository managers, in order to store versions of documents that have already been deleted, you should restrict the permissions for the directory `/-~system~` of the relevant CM repository. Versions of deleted documents are stored beneath the directory. Only allow system administrators to access this directory.

See also:

Permissions [SAP Library]

Security Manager [SAP Library]

ACL Security Manager [SAP Library]

Service ACLs

You can use service permissions to limit access to certain functions, such as subscriptions or management of the approval process, to specific users. Service permissions can only be defined for folders.

After the installation of SAP NetWeaver, all users have full access by default. Make sure you restrict these permissions (see SAP Note 599425).

The repository service *service ACL service* must be activated in the configuration of the repository manager in question so that you can use service ACLs.

See also:

Service Permissions [SAP Library]

Service ACL Service [SAP Library]

Security Zones

Security zones constitute a portal concept for restricting unauthorized direct access to iViews using their URLs (see Security Zones [SAP Library]).

For initial KM content, the required permissions in the security zones are already assigned during installation of SAP NetWeaver.

If you upgrade your system, you can find information about setting permissions in the how-to guide *Configuring Permissions for Initial Content in SAP EP 6.0*. You can find this guide on the *SAP Service Marketplace* at **`service.sap.com/nw-howtoguides`** → *SAP NetWeaver* → *Media Library* → *How-to Guides* → *Portal, KM and Collaboration* → *Portal*.

If you use PAR files to import your own portal content (portal components) to the portal, you must also set permissions in the security zones. If you create new iViews, you must also check or reset the permissions there, if they are not inherited.

See also:

Authorizations [SAP Library]

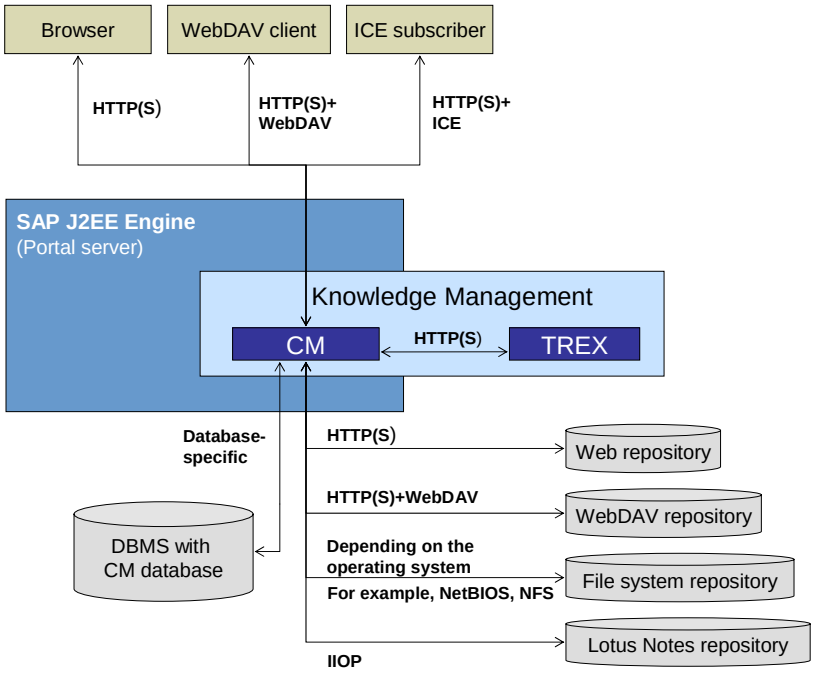
3 Communication Channel Security

Various channels of communication and technologies are used between the components and data sources in Knowledge Management.

Used Technologies

The following technologies are used for communication:

- HTTP/HTTPS
- WebDAV
- ICE
- JDBC on OpenSQL
- Operation-system-dependent and database-specific technologies



Components and Communication Channels

Communication Between…	Communication Channel/Log	Transmitted Data	Comments
CM and DBMS with CM database	Database-specific protocol	Documents, metadata	You can use database management systems such as ORACLE® and MICROSOFT®.
CM and TREX	HTTP or HTTPS	Search requests, search results, index data, classification data	
CM and repositories	Depends on the implementation (see table below).	Documents, metadata	
ICE subscriber und ICE provider (CM)	ICE using HTTP or HTTPS.	Documents, metadata	Use for exchanging content packages.
WebDAV client and WebDAV server (CM)	HTTP or HTTPS with WebDAV extension.	Documents, metadata	
Browser and portal with installed KM	HTTP or HTTPS	(HTML) documents	

Technologies for Repositories

External Repositories	Communication Technology	Type of Authentication
Web repository	HTTP, HTTPS	HTTP Basic Authentication, HTTP Digest Authentication, NTLM Authentication
WebDAV repository	HTTP, HTTPS with WebDAV extension	HTTP Basic Authentication, HTTP Digest Authentication, NTLM Authentication
File-system repository and CM repository (DBFS and FSDB modes)	Operating-system-dependent. WINDOWS® - Example: NetBIOS, TCP/IP UNIX – Example: NFS	Dependent on operating system and configuration. WINDOWS® – Example: SMB using TCP/IP
Lotus Notes repository	IIOP	IIOP-specific

In the case of Web and WebDAV repositories, the combination of HTTP and *Basic Authentication* is not seen as secure. This is because passwords are practically transmitted in plain text. However, the authentication type used is controlled by the remote server: If a remote server uses *Basic Authentication*, the server is not configured to be secure. If this is the case, change the type of authentication to another type, such as *Digest Authentication*.

See also:

Content Management Configuration [SAP Library]

Repositories and Repository Managers [SAP Library]

4 Data Storage Security

Data in KM

Various types of data are used in Knowledge Management. They are stored in different places.

Data in Knowledge Management

Type of Data	Storage Location	Protected By
Configuration data	Database (see Content Management Configuration [SAP Library]).	Security concepts of the DBMS. Access to the portal is controlled by the role concept.
KM portal content (worksets and iView templates)	Portal catalog (database)	Security concepts of the portal (roles), security concepts of DBMS.

Type of Data	Storage Location	Protected By
KM content (folders and files)	Internal repositories [SAP Library] (such as `/documents`) File system repository `/etc`	Security concepts of the portal (roles), security concepts of DBMS, permissions at operating system level.
Service data	Database, directory with configuration data in the file system.	Security concepts of the DBMS, permissions at operating system level.
Customer and system-external content (folders and files)	External repositories [SAP Library]	Security concepts of the remote server, ACLs, permissions.
Customer and system-external content (folders and files)	Internal repositories (database, file system)	Permissions at operating system level, ACLs.

Data in Repositories

Note that repository managers such as CM or file-system repository managers cannot be created in system directories.

The root directory of a repository manager cannot be located in the system directory of the J2EE Engine. This is because documents can be accessed not only from the portal, but also directly using HTTP.

Virus Check

There is a virus check option in KM for documents for which you have write or read access. You have to configure the virus scan interface of the SAP Web AS for this.

The following are examples of times when you can use a virus check with write access:

- Loading files to KM
- Storing changed data

The virus check can run in the background or be started by a content manager using a report.

For more information, see Virus Scanner Service [SAP Library].

Temporary Data on the Client PC

Note that KM-specific Internet files are stored on the client PC when the portal is called.

When you use the function *Edit Locally,* the content of the document in question is stored in a temporary directory on the client PC. When you upload the document to KM, it is deleted from the client PC when the program used to edit it is terminated. If you do not terminate the program, or if the document is locked, it is not deleted from the client PC.

If the client PC is also being used by another user, delete the content from the temporary directories and the browser cache when you have finished your work.

Digital Signatures and Document Encryption

At the moment, Knowledge Management does not contain any digital signatures or functions for document encryption. To digitally sign or encrypt documents, you need to use third-party solutions.

5 Overview of KM Services

The Knowledge Management capabilities of the portal use numerous services. SAP distinguishes between global services and repository services. The former are used system-wide; the latter can only be used in the repositories that they have been activated in.

For more information, see Global Services [SAP Library] and Repository Services [SAP Library].

Many services have other services as prerequisites, because they provide certain basic functions. The dependencies are listed in the tables below. If a service uses a service user, this is entered in the *Comments* column.

Global Services

Since global services can be used system-wide and also by other usage type in their own scenarios, you must not deactivate them.

The following table lists the global services and displays the dependencies to other services.

KM Services (Global Services)

Name	Used Internally (Hidden)	Required Services	Comments
Global Application Property Service		URI Mapper Service System Landscape Service Cache Service	
Audit Log Service			
Crawler Service		Application Log Service Resource Filter Service URL Generator Service	The applications or services that call the crawler service (for example, index administration, subscription service, or content exchange service) provide the user.
Legacy Crawler Service			This service is now used only in upgrade or migration scenarios.
Content Exchange Service		Scheduler Service Task Queue Service System Landscape Service Crawler Service	Uses the service user *ice_service*

Name	Used Internally (Hidden)	Required Services	Comments
Inbox Service	X		Uses the service user *notificator_service*
Index Management Service		Application Log Service Crawler Service Property Metadata Service Scheduler Service System Landscape Service Task Queue Service URI Mapper Service URL Generator Service Application Property Service	Uses the service user *index_service*
System Landscape Service			
Mime Handler Service		URL Generator Service	
Notificator Service			
Object Type Handler Service			
Publishing pipeline service	X		
Property Metadata Service			
Property Structure Service		Property Metadata Service	
Reporting Service			
Service for Registering Resource Types			
Scheduler Service	X	System Landscape Service	
Task Queue Service			
Template Service			
URL Generator Service			

Name	Used Internally (Hidden)	Required Services	Comments
URI Mapper Service			
Virus Scanner Service			
Application Log Service	X		
Cache Service	X		
Checkout Service			
Global Attachments Service	X		Used by Collaboration
File System Mount Service	X		
Service for Form-Based Publishing	X	Property Metadata Service URL Generator Service XSLT Pipeline Service	
Service for Registering Properties	X		
Quick Poll Service	X		Used by Collaboration
Relation Service	X		
Scheduler Service	X		
Filter Service for Resource Lists	X	XSLT Pipeline Service Service for Form-Based Publishing	
Resource Filter Service	X		
Resource Type Registry Service			

Repository Services

In principle, all repository services are optional. You can activate them for each repository that you want to use the service in. If you do not want to use a service, you deactivate it in the configuration of the repository manager in question.

In the portal, choose *System Administration* → *System Configuration* → *Knowledge Management* → *Content Management* → *Repository Managers* to do this. Open the configuration of the repository manager in question and deactivate the service affected.

When creating a repository manager, choose only those repository services that you really intend to implement (see Minimal Configuration [Page 17]).

The following table lists the repository services and displays the dependencies to other services.

KM Services (Repository Services)

Name	Required Services	Optional	Comments
Application Property Service (properties)	URI Mapper Service System Landscape Service Cache Service	x	
Service ACL Service (svc_acl)		x	If this is not activated, other services cannot ensure protection of resources using this service's special permissions.
Access Statistics Service (accessstatistic)	Application Property Service (properties)	x	
Subscription Service (subscription; subscription_collaboration)	URL Generator Service Pipeline Service Notificator Service Application Log Service Crawler Service Scheduler Service Optional: Inbox Service	x	Uses the service user *subscription_service*
Time-Dependent Publishing Service (tbp)	Global Application Property Service	x	Uses the service user *timebasedpublish_service*

Name	Required Services	Optional	Comments
Status Management Service (statemngt)	Global Application Property Service Notificator Service Optional: Feedback Service	x	
Layout Service (layout)	Global Application Property Service	x	
Collaboration Services [SAP Library] (discussion, feedback, personalnote, comment, rating)		x	Use the service user *collaboration_service* If you want to prevent discussion posts, comments, or feedback from being created in HTML format for security reasons, activate the appropriate `Secure` parameter in the configuration of the services.

6 Minimal Configuration

Functional Restrictions

Depending on the users of your system, you may want to restrict functions as well as access permissions.

Deactivating Repository Services

By default, the CM repository *documents* is delivered for storing documents and metadata. For a minimal configuration, you deactivate the repository services that you do not need (for example, the discussion service for creating discussions) in the configuration of this repository manager. If you integrate your own repositories, you should also reduce the number of repository services to a minimum. However, you should not change the configuration of repository managers that are used system-internally.

For more information, see Repositories and Repository Managers [SAP Library] and Repository Services [SAP Library].

Deactivating Interface Commands

The KM flexible user interface provides you with interface commands for carrying out operations. For a minimal configuration, you should deactivate interface commands that cause changes, including commands for checking objects in (*Upload, Create New Text File. Create New HTML File),* commands for editing objects (*Edit Locally, Edit Online*) and commands for deleting objects.

Permissions dictate whether a command can be carried out. A user without write permission can not use the commands for creating a new file. Deactivation is therefore only necessary for a minimal configuration or for performance reasons.

For more information see User Interface Commands [SAP Library].

7 Further Security-Relevant Information

Active Code

Various types of active code are used in Knowledge Management (KM). This is executed on the client host in the Web browser.

Active Code	Usage	Comments
ActiveX	Used for the *Local Editing* function.	If your security policy rules out ActiveX, you can use a Java applet instead. For more information, see Online and Local Editing [SAP Library].
JavaScript	Used by the HTMLB software component (for example, for client-side check of entries and for generating popup menus).	JavaScript is used extensively in the portal.
Java	Java applets are used for *Local Editing* and for the *XML Forms Builder* application.	When launching the *XML Forms Builder* application and the *Local Editing* function, you must log on if the parameter `ume.logon.httponlycookie=true` is set in the *User Management Engine* configuration (see SAP Logon Ticket [SAP Library]). Basic authentication is used to log on. If this parameter is set to `false`, the current logon ticket is used. If you use this method, there is a risk that it could be read by malicious scripts. SAP therefore recommends setting this parameter to `true`. If your security policy rules out Java applets, you cannot use the *XML Forms Builder.* The *Local Editing* function can also be used with ActiveX.

Configuration on Secure Sockets Layer (SSL)

SAP recommends that you configure Knowledge Management in a portal that is secured with SSL encryption. Otherwise, communication could be overheard.

Anonymous Users and Creating Documents

Users can use Knowledge Management to create documents in the portal. Examples of document creation are uploading and editing document, sending feedback, taking part in discussions, and writing reviews. Users normally create these documents using the HTML Editor. In portals that grant access to anonymous users from the internet, we recommend that you do not give these users permission to create HTML documents, as the privilege could be abused

We therefore recommend that you only give anonymous users read permission for all documents and folders. You should not give them write permission. On the flexible UI, layout sets for anonymous users cannot contain menu items for creating documents.

The implementation of KM and Collaboration in scenarios that involve anonymous users accessing the portal is only supported with restrictions. These restrictions are described in SAP note 709354. You should also read SAP note 837898, which explains the required settings. If you are using Release SPS 11 or earlier, read SAP Note 728106.

It is also possible to configure discussions, reviews, and feedback so that they can be created using a text editor instead of an HTML editor. We recommend that you make this setting. You can do this by setting a parameter in the services in question.

For more information on setting this parameter, see Collaboration Services [SAP Library]. Use the same procedure for comments and feedback.

You can also configure the *XML Forms Builder* so that no HTML can appear in the forms created and no JavaScript can be executed. For more information, see Form-Based Publishing [SAP Library] and Project Options [SAP Library].

Deactivating Repository Services

If you later deactivate the repository services *time-dependent publishing (tbp)* and *status management (statemngt)* in the configuration of repository managers, all documents in folders of these repositories become visible for all users. If the services are active, some documents are not visible, because they have a status that restricts visibility to certain user groups or time periods.

8 Trace and Log Files

Log information pertaining to Knowledge Management is stored by the system in the file `defaultTrace.trc`. This file is stored in the directory `.../j2ee/cluster/server<n>/log`. You use the log viewer [SAP Library] to display and evaluate logged data.

You activate audit logging for ACLs by setting the required level of detail for the audit logging class `com.sapportals.wcm.repository.security.SecurityAudit$Log` in the visual administrator of the J2EE Engine.

`com.sapportals.wcm.repository.security.SecurityAudit$Log`

Severity = DEBUG