SAP NetWeaver 2004s SPS 4

Security Guide

Security Guides for the SAP NetWeaver Scenarios

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

Security Guides for the SAP NetWeaver Scenarios

Security Guides for the SAP NetWeaver Scenarios

Scenario	Variants	See
Running an Enterprise Portal	Providing Uniform Content Access	Portal Security Guide [SAP Library]
	Implementing a Global Portal	Portal Security Guide [SAP Library] Implementing a Global Portal (Federated Portal) [Page 8]
	Implementing a Multitenant Portal	Portal Security Guide [SAP Library] Implementing a Multitenant Portal [Page 8]
Enterprise Knowledge Management	All variants	Knowledge Management Security Guide [SAP Library]
Enabling User Collaboration	All variants	Collaboration Security Guide [SAP Library]
Business Planning and Analytical Services	All variants	Security Guide SAP NetWeaver BI [SAP Library]
Enterprise Reporting, Query and Analysis	All variants	Security Guide SAP NetWeaver BI [SAP Library] Scenario Enterprise Reporting, Query and Analysis [SAP Library]
Enterprise Data Warehousing	All variants	Security Guide SAP NetWeaver BI [SAP Library] Scenario Enterprise Data Warehousing [SAP Library]
Enabling Application-to-Application Processes	Application-to-Application Integration	SAP NetWeaver Application Server Security Guide [SAP Library] SAP NetWeaver Process Integration Security Guide [SAP Library]
Enabling Business-to-Business Processes	Business partner integration using industry standards Small-business partner and subsidiary integration	SAP NetWeaver Application Server Security Guide [SAP Library] SAP NetWeaver Process Integration Security Guide [SAP Library]

Scenario	Variants	See
Business Process Management	All variants	SAP NetWeaver Application Server Security Guide [SAP Library] SAP NetWeaver Process Integration Security Guide [SAP Library]
Business Task Management	Central Access to Tasks	Universal Worklist Security Guide [SAP Library]
	Support for Offline Processes	Guided Procedures Security Guide [SAP Library] Interactive Forms based on Adobe Software [SAP Library]
Enabling Enterprise Services	Point-to-point services-based integration	SAP NetWeaver Application Server Security Guide [SAP Library]
	Brokered services-based integration	SAP NetWeaver Application Server Security Guide [SAP Library] SAP NetWeaver Process Integration Security Guide [SAP Library]
Developing, Configuring, and Adapting Applications	Developing Java applications using Web Dynpro	SAP Web Application Server Security Guide [SAP Library] Security Aspects for Usage Type DI and Other Development Technologies [SAP Library] Security Aspects of Web Dynpro for Java [SAP Library]
	Developing ABAP applications using Web Dynpro	Security Aspects for Web Dynpro for ABAP [SAP Library]
	Creating composite applications using the CAF	Composite Application Framework Core Security Guide [SAP Library] Security Guide for Guided Procedures [SAP Library]
SAP NetWeaver Operations	Data archiving	Security Guide for ADK-Based Data Archiving [SAP Library] Security Guide for XML-Based Data Archiving [SAP Library]

Scenario	Variants	See
Software Life-Cycle Management	All variants	Security Guide for the SAP System Landscape Directory [SAP Library] SLM Security Roles [SAP Library]
	Implementation support	Protecting Your Productive System (Change & Transport System) [SAP Library] (AS-ABAP) Security of the SAP NetWeaver Development Infrastructure [SAP Library] (AS-Java)
Authentication and Single Sign-On	All variants	User Authentication and Single Sign-On [SAP Library] Portal Security Guide [SAP Library]
Integrated User and Access Management	All variants	User Management [SAP Library] Integration of User Management in Your System Landscape [SAP Library]

1 Running an Enterprise Portal: Security Aspects

The *Running an Enterprise Portal* IT scenario provides all the members of a company's value chain—with uniform, role-based, and secure access to their day-to-day work and information resources through a Web-based portal interface. These resources include SAP applications, third-party applications, databases, data warehouses, desktop documents, Web content, and services. The portal makes it possible to search internal and external sources, and to access both structured and unstructured information from any geographical location throughout the organization.

The following scenario variants are derived from this IT scenario:

- Providing Uniform Content Access
- Implementing a Global Portal (Federated Portal)
- Implementing a Multitenant Portal

To successfully deploy and run each scenario variant, you need to consider a number of security aspects. Some of these security aspects are generic to all scenario variants, while others are scenario-specific.

Refer to the subtopics in this section for an overview of the security aspects relevant to each scenario variant.

1.1 Providing Uniform Content Access

This *Running an Enterprise Portal* IT scenario variant lets organizations develop, configure, and operate a knowledge-based, Web-like user interface—an enterprise portal—that provides a consistent environment and single point of access to content to users can perform their daily tasks.

All security aspects necessary for this scenario variant are covered in the Portal Security Guide [SAP Library].

1.2 Implementing a Global Portal (Federated Portal)

Documentation for this feature will be available upon its release in a future version of SAP NetWeaver.

1.3 Implementing a Multitenant Portal

Implementing a multitenant portal is a scenario-variant whereby several independent customers (tenants) can run and coexist on the same single SAP NetWeaver Portal installation base, which is hosted by a dedicated service provider. Each customer's portal is customized and branded with their corporate identity, and its users and data are securely compartmentalized so that it is available only to the users of each tenant and the global administrators of the multitenant portal.

Security Related Tasks in a Multitenant Portal

First, you need to consider the security aspects for running a standard portal. All information about securing SAP NetWeaver Portal is available in the Portal Security Guide [SAP Library].

As a result of the inherent risks of hosting multiple customers on a single multitenant portal, you then need to consider the following security issues:

- Since all tenants access the same single portal infrastructure, any log and trace files generated can contain information about applications, users, and other portal objects of various tenants.

  For this reason, we recommend not to deliver such files to a specific tenant, as some applications save sensitive information in log files, such as the name of servers used by tenants, and user IDs and passwords.

  For information about the contents of these files, see Logging and Tracing [SAP Library].

  If you must provide a trace or log file to a specific tenant, carefully check it and then remove the details about other tenants.

- The multitenant portal scenario supports delegating user and content administration tasks to tenant administrators (see Delegated Administration [SAP Library]). For example, each tenant has a tenant-specific delegated content administrator who manages the content of that tenant.

  You cannot assign tenant administrators to a delegated system administration role, since the role contains tools that allow one to directly and indirectly access and manipulate data across multiple tenants.

  Delegating administration tasks to employees of the service provider, and not to employees of the tenant customers, ensures that under no circumstance is the information intended for a specific tenant exposed to an employee of another tenant.

- The portal provides tools for assigning, changing, and designating security zones.

  All operations relating to security zones in the multitenant portal must be performed by the super administrator rather than the delegated system administrator.

  For more information, see Security Zones [SAP Library].

- A set of default permissions for initial portal content is available on deploying the portal. The default permissions enable other delegated administration roles in addition to that of the super administrator.

  In all cases, the super administrator of the multitenant portal environment must make sure that no delegated administrator can change permissions for any portal object that has not been assigned to their tenant. For more information, see Portal Permissions [SAP Library].

  On the other hand, the super administrator can enable a tenant administrator (delegated administrator) to change permissions for objects within the specific tenant's folder.

- Portal applications are delivered as Portal Archive (PAR) files, which are uploaded and deployed in the portal. PAR files contain the Java classes and resources that are required to run the application.

  They can also contain code intended for hacking into other tenants. For this reason, we recommend that uploading and deploying of *par* files to the portal must be the task for only the super administrator of the portal. For more information, see Managing PAR and JAR Files in the Project [SAP Library].

See Also

Securing the Multitenant Portal Environment [SAP Library]