SAP NetWeaver 2004s SPS 4

Security Guide

Portal 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

Portal Security Guide

1 Introduction

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

Target Audience

- 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.

Why Is Security Necessary?

The portal offers users a single point of access to all applications, information, and services needed to accomplish their daily tasks. Links to back-end and legacy applications, self-service applications, company intranet services, and Internet services are all readily available in the user's portal. Because the borders between company intranets and the Internet are blurring, comprehensive security is vital to protect the company's business.

About this Guide

The Security Guide comprises the following main sections:

- Before You Start [Page 6]

  This section contains information about why security is necessary, how to use this document, and references to other Security Guides that build the foundation for this Security Guide.

- User Administration and Authentication [Page 7]

  This section provides an overview of the following user administration and authentication aspects:

  - Recommended tools to use for user management.
  - Standard users that are delivered with the portal.
  - Overview of the user synchronization strategy.
  - Overview of the authentication mechanisms available and related security recommendations.
  - Overview of Single Sign-On and recommendations for securing SAP logon tickets.

2 Before You Start

Fundamental Security Guides

The portal uses SAP Web Application Server Java as its underlying application server. Therefore you must read and apply the security recommendations in the *SAP Web AS Security Guide for Java Technology* for all productive portal installations. This guide only describes the security information that differs from it as well as additional security information.

If you set up a SAP Enterprise Portal scenario with Knowledge Management, you must also read the Knowledge Management security guide.

Related Security Guides

Application	Guide
SAP Web Application Server Java	SAP Web AS Security Guide for Java Technology [SAP Library]
Knowledge Management	Knowledge Management Security Guide [SAP Library]

Important SAP Notes

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

Important SAP Notes

SAP Note Number	Title	Comment
740328	NW04: Portal Security Guide	This note contains additional security information about the portal that is not available at the time of publishing this guide.
720590	User Management Engine (UME) on WAS 6.30 and higher	Central note for all UME issues in EP 6.0 SP3 and higher.

3 User Administration and Authentication

This section covers:

3.1 User Management

The portal uses the User Management Engine (UME) for user management. The UME can be configured to work with user management data from multiple data sources, for example, an LDAP directory, database, or ABAP system. For more information on the UME, see User Management Engine [SAP Library] and Integration of User Management in Your System Landscape [SAP Library].

The UME is integrated as a service of the SAP Web Application Server Java (Web AS Java). Therefore you can use the user management tools of the Web AS Java to manage users. In addition, the portal provides additional tools for user management which are available in the portal environment only.

User Management Tools

Tool	Detailed Description
User management functions in the Visual Administrator of SAP J2EE Engine	For more information, see SAP J2EE Engine User Management Using the Visual Administrator [SAP Library].
User management administration console	Allows you to manage users, groups, roles, and user-related data. It is available either as a standalone Web-based tool or as a series of iViews integrated in the *User Administration* role in the portal. For more information, see User Management Administration Console [SAP Library].
Role Assignment function (only available in portal)	Allows you to assign users and groups to portal roles and to search for users, groups, or portal roles. For more information, see Role Assignment [SAP Library].
User Mapping function (only available in portal)	Allows you to map users' portal user IDs and passwords to the corresponding user ID in systems connected to the portal to enable Single Sign-On. For more information, see User Mapping [SAP Library].
Tool for distributing portal roles to ABAP systems (only available in portal)	For more information, see Role and User Distribution to the SAP System [SAP Library].
Tool for uploading objects such as roles and transactions from ABAP systems to the portal (only available in portal)	For more information, see Upload of Roles from ABAP-Based Systems [SAP Library].

Default Users

The portal uses the same administrator, guest, and emergency users as SAP Web Application Server Java (SAP Web AS Java). It also uses the same communication users. For details, see Standard Users [SAP Library].

After installation, the standard administrator user is by default assigned to the standard *Administrators* group, which is in turn assigned to the standard *Super Administrator* role. As the *Super Administrator* role has extensive permissions, users associated to this role should not be used in normal operation. For more information, see Portal Roles [Page 13].

In addition, the portal uses the following service users. They are all used internally in the portal and should not be deleted. However, if you do delete one of these users by mistake, it will automatically be created at the next startup of the portal.

User	Delivered?	Type	Default Password	Detailed Description
pcd_service	Created during startup.	Service user		User to authenticate against the Portal Content Directory (PCD) service, for example to create ACLs.
config_fwk_ service	Created during startup.	Service user		User that the configuration service (a portal core application) uses to perform any configuration operation such as deployment.
ume_service	Created during startup.	Service user		User with extensive permissions that the UME uses to request role data from the PCD.

3.2 User Data Synchronization

User Management Engine (UME) can use a Lightweight Directory Access Protocol (LDAP) directory, database, or the ABAP user management of a SAP Web Application Server as a data source. Therefore, in most cases, no user data synchronization is necessary. For recommendations on when to use which data source, see Integration of User Management in Your System Landscape [SAP Library].

SAP Enterprise Portal 6.0 customers are are entitled to a 250,000-user version of Novell eDirectory free of charge. For more information, see **`www.novell.com/products/edirectory/sap/`**.

UME provides a replication function to SAP systems for scenarios where it is not possible to integrate the user management of an SAP system with UME by any other means. The data is replicated in one direction only, from UME to the SAP System. Data cannot be replicated from the SAP System to UME. For more information, see Replication of User Data [SAP Library].

3.3 Authentication

The portal offers the same authentication mechanisms as the J2EE Engine. For an overview of the available mechanisms and how to configure them, see Authentication on the J2EE Engine [SAP Library] and Configuring Authentication Mechanisms [SAP Library].

Basic Authentication

This authentication mechanism is based on the Basic Authentication feature of the HTTP protocol. When you configure the portal to use HTTP Basic Authentication as authentication mechanism, authentication data is transported in clear text (base 64 encoded). This means that passwords can easily get sniffed by an attacker with physical access to the network path between the client and the Portal Server. The attacker can then impersonate portal users. This is not a weakness of the Enterprise Portal itself, but a weakness of the standardized HTTP Basic Authentication mechanism.

For this reason, we strongly recommend using Secure Sockets Layer (SSL) between the client and Portal Server, since this will encrypt all information exchanged between client and server including the authentication credentials.

3.4 Integration Into Single Sign-On Environments

Single Sign-On

Single Sign-On (SSO) is a key feature of the portal that eases user interaction with the many component systems available to the user in a portal environment. Once the user is authenticated to the portal, he or she can use the portal to access external applications. With SSO in the portal, the user can access different systems and applications without having to repeatedly enter his or her user information for authentication.

The portal SSO mechanism is available in two variants depending on security requirements and the supported external applications:

- SSO with SAP logon tickets
- SSO with user ID and password

Both variants eliminate the need for repeated logons to individual applications after the initial authentication at the enterprise portal. Whereas SSO with SAP logon tickets is based on a secure ticketing mechanism, SSO with user ID and password forwards the user's logon data (user ID and password) to the systems that a user wants to call.

In most system landscapes, the portal will be set up as the ticket-issuing system. This means that users log on to the portal using any of the supported authentication methods and the portal issues a SAP logon ticket to the user. In cases where the portal is not the ticket-issuing system, it is possible to set up the portal to accept tickets issued by other systems.

For more information on Single Sign-On in the portal, see:

- Single Sign-On [SAP Library]
- Single Sign-On in a Complex System Landscape [SAP Library]

Using SAP Logon Tickets

- When using SAP logon tickets for authentication with Web applications, the user's ticket is stored as a non-persistent cookie in the user's Web browser. This cookie contains the information necessary to log the user on to additional systems without having to provide an explicit password authentication. Therefore, you should protect the SAP logon ticket from being compromised or manipulated during transfer by using SSL between Internet-enabled components. See Communication Channel Security [Page 14].
- Optionally you can mark the logon ticket as a secure cookie, to enforce that the client browser only sends the cookie over SSL connections. We strongly recommend this setting. For this, you must set the user management property `ume.logon.security.enforce_secure_cookie` to `TRUE`.
- To reduce the risk of SAP logon tickets being reused in replay attacks, we recommend that you reduce the validity period of the logon ticket. The default validity period is eight hours. To change the validity period, use the user management configuration tool [SAP Library] in the portal.

Using SAP Logon Tickets with User Mapping

If users have different IDs in the portal and in ABAP-based SAP systems, users and administrators can map users' portal user ID to their ABAP user ID in a SAP reference system. By default the mapped user IDs are stored encrypted in the User Management Engine (UME) database. It is also possible to store the mapped user IDs in an LDAP directory. In this case they are not encrypted. To prevent these IDs from being manipulated, you must make sure that no unauthorized users have write-access to the LDAP directory, in particular to the attribute containing the ABAP user ID. See also Using an LDAP Directory Attribute as the ABAP User ID [SAP Library].

Using User ID and Password with User Mapping

When Single Sign-On with user ID and password is used, the user ID and password are sent across the network. We strongly recommend that you protect the connections to the backend systems using HTTPS or SNC to prevent the user ID and password being eavesdropped by an external party.

We strongly recommend that you install the full version of the SAP Java Cryptographic Library if you use user mapping. This toolkit is required so that user mapping data can be stored in encrypted form. If the toolkit is not deployed, user mapping data is stored with weak encryption (base 64 encoding), which is not recommended for production systems.

4 Authorizations

Authorizations define which objects users can access and which actions they can perform. The portal has an authorization concept that is implemented using permissions, security zones, UME actions, and the *AuthRequirement* property. These are described in more detail below.

We recommend that before you deploy a production portal, you check that the authorizations assigned in the portal do not allow unauthorized users to access sensitive content such as administrative tools or confidential data.

- **Permissions**: permissions for all Portal Content Directory (PCD) objects. Portal permissions define portal user access rights to portal objects in the PCD and are based on access control list (ACL) methodology. Essentially, every portal object can be assigned directly to an individual user or collectively to groups of users through user groups and roles. Portal content objects for which you can set permissions are folders (Portal Catalog folders, not role folders), iViews, pages, layouts, roles, worksets, packages, and systems. When any portal user accesses a portal tool that displays portal objects stored in the PCD, those objects are filtered according to the user's access permissions. If a user is permitted to access a portal object, the permission level set for the user defines which actions and operations the user can perform on that object. Permissions also define which objects are available to end users in a runtime portal environment.

  In EP 6.0 SP9 and higher, the default permissions assigned to portal objects after installation are set in a manner that permits only the Super Admin role full access to the entire portal and its initial content. The remaining pre-configured administration and business user roles shipped with the portal are permitted access to the out-of-the-box tools and user interfaces relevant to each role; however, access to objects within these tools is not permitted.
  After installation, you can configure the permissions to enable the preconfigured portal roles to access initial content objects relevant to their role. To help you with this task, see the guide *Configuring Permissions for Initial Content in SAP EP 6.0* which you can find on SAP Service Marketplace at **`service.sap.com/nw-howtoguides`** → *Portal, KM and Collaboration* → *Portal* → *Configuring Permissions for Initial Content in SAP EP 6.0*.
  We recommend that if you change the permissions, you provide users with the minimum set of permissions that they require to fulfill their tasks. You should check the permissions carefully before deploying a test or production portal.

  For more information on permissions, see Portal Permissions [SAP Library] and Default Permissions [SAP Library].

- **Security Zones**: Control which portal components and portal services users can launch and are defined in the development phase. If a portal component or service is not assigned a complete security zone in its descriptor file, the portal runtime assigns it to a predefined security zone folder for unspecified components or services. The portal provides default permissions for the standard security zone folders in which the portal applications shipped with the portal's initial content reside. These permissions provide a high level of security for a freshly installed portal. We recommend that you become familiar with the standard security zones created by SAP and also the default permissions assigned to them. If necessary, adjust the default permissions to suit your environment. We highly recommend that you use the security zones structure of SAP for your own content. For your own content, you should make sure that the permissions on the security zones provide appropriate protection against unauthorized access and adjust them if required.

Security zones control access to portal components whether they are accessed by a direct URL or through a role-assigned iView based on that portal component.

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

- **UME Actions**: the User Management Engine (UME) equivalent of portal permissions. The UME verifies that users have the appropriate UME actions assigned to them before granting them access to UME iViews and functions. All other portal services do not use UME actions.

  For more information on UME actions, see UME Actions in the Portal [SAP Library].

  Pay particular attention to the UME action *UME.AclSuperUser*. This action provides *Owner* permissions on all objects in the Portal Content Catalog and should be used very restrictively. It should only be assigned to the *Super Administration* role in the portal. It should not be assigned to any other roles.

  Also be careful to whom you assign the UME.Manage_Roles action. Users with this action can assign themselves the *Administrator* role in the UME Web-based administration tool and thus gain full administrator rights on the J2EE Engine. In particular, DO NOT assign this action to delegated user administrators.

- **AuthRequirement property**: This is a master iView property used in EP 5.0 that defines which users are authorized to access a master iView or Java iViews derived from a master iView. For backward compatibility with iViews developed for EP 5.0, EP 6.0 supports this property.

  For details on the *AuthRequirement* property, see *SAP Enterprise Portal 5.0 Administration Guide → iViews → Master iViews → Master iView Properties → Portal Component Properties*.

4.1 Portal Roles

In the portal, roles are only indirectly linked to authorization. Portal roles group together the portal content required by users with a certain role in the company. In addition, the role structure defines the navigation structure that a user sees in the portal. Users and groups assigned to a role inherit the permissions of the role. By default this is end user permission.

For more information on the roles shipped with the portal, see Pre-configured Roles [SAP Library].

After installation the following pre-configured roles are assigned to the following standard users/groups:

Role	Assigned to Users	Assigned to Groups
Super Administration		Administrators
Standard User		Administrators

Super Administration Role
The *Super Administration* role has access to all content and objects in the portal and these permissions cannot be deleted or modified. Because this role has such extensive permissions, we recommend not to use users assigned to this role for normal daily administration. We recommend that only one user account should be assigned to this role. All other administrator users should be assigned a subset of administrative tasks and these users should be used for daily administration. For more information on delegating administrative tasks to a number of users, see Super Administration [SAP Library] and Delegated Administration [SAP Library].

Standard User Role
We recommend that after installation you assign the *Standard User* role to the default group *Everyone*. If this group does not have a role assigned to it, some users may not have a role assigned to them and, as a result, see a blank page when they log on to the portal.

5 Network and Communication Security

This section covers:

- Communication Channel Security [Page 14]: Describes the communication channels used in a portal system-landscape and provides recommendations for how to secure these channels.
- Network Security [Page 19]: Provides a recommendation for a secure network architecture for your portal installation.

5.1 Communication Channel Security

Protecting the information transferred between the client and the Portal Server and between the internal components of the SAP Enterprise Portal is important. The data transferred contains authentication credentials and possibly other sensitive data that must not be known to third parties. This kind of data must be encrypted using secure communication protocols such as Secure Sockets Layer (SSL) or Secure Network Communications (SNC).

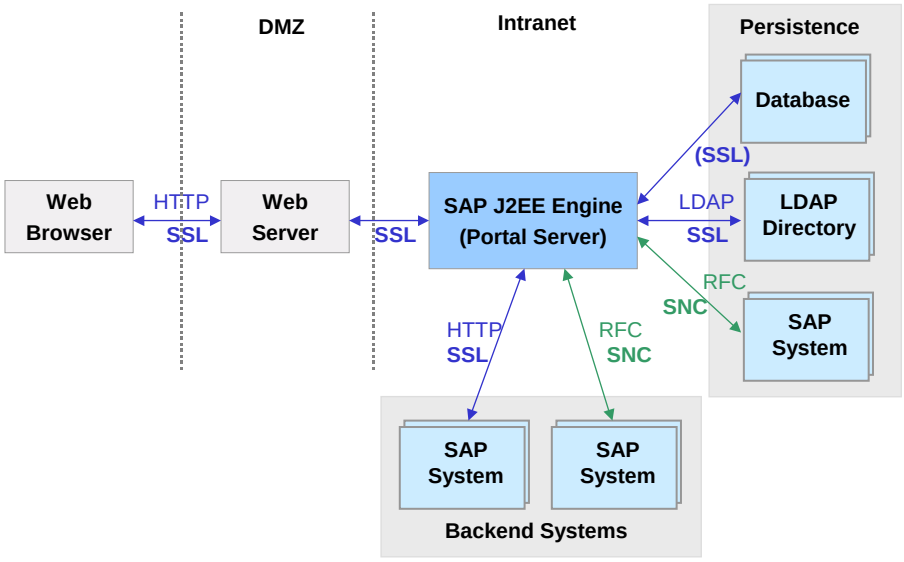
We strongly recommend that you protect all communication channels used during normal operation of the SAP Enterprise Portal.

See also:

- Communication Between Internal Components [Page 15]
- Communication with Backend Systems [Page 16]

5.1.1 Communication Between Internal Components

The following diagram provides an overview of the communication channels between the components of the Enterprise Portal.



This diagram displays a secure network architecture where a Web server is placed in a demilitarized zone (DMZ) in front of the Portal Server. It is also possible to have a network architecture in which the client communicates directly with the Portal Server.

The Portal Server uses a database to store portal-related data such as content objects. It can use any combination of database, LDAP server and SAP System to store user management data. As user-related data is sensitive data, you should protect all communication channels to user data stores.

There are also communication channels between the Portal Server and any backend systems used for providing content to display in the portal. Depending on the nature of the data passed from the backend systems to the Portal Server, these communication channels should also be protected. For example, the Portal Server can connect to SAP Systems using the remote function call (RFC) protocol. These connections can be secured using Secure Network Communications (SNC).

The following table gives you a quick overview of where to find detailed documentation on securing the communication channels shown in the diagram.

Connection	Secure Protocol	Documentation
Web browser ↔ SAP J2EE Engine	Secure Sockets Layer (SSL)	See the document Configuring the Use of SSL on the SAP J2EE Engine [SAP Library] or, if you are using an intermediary server such as an IIS, see Using SSL With an Intermediary Server [SAP Library].
Portal Server ↔ Database	SSL	No documentation currently available.
Portal Server (UME) ↔ LDAP Directory	SSL	Configuring SSL Between the UME and an LDAP Directory [SAP Library]
Portal Server (UME) ↔ ABAP-based SAP system	Secure Network Communications (SNC)	Configuring SNC Between the UME and an ABAP-Based System [SAP Library]

5.1.2 Communication with Backend Systems

We also recommend that you configure secure communications to application servers accessed in the back end by SAP Enterprise Portal components. For example, if an iView accesses a backend ERP System via HTTP, you need to configure Secure Sockets Layer (SSL) on this connection.

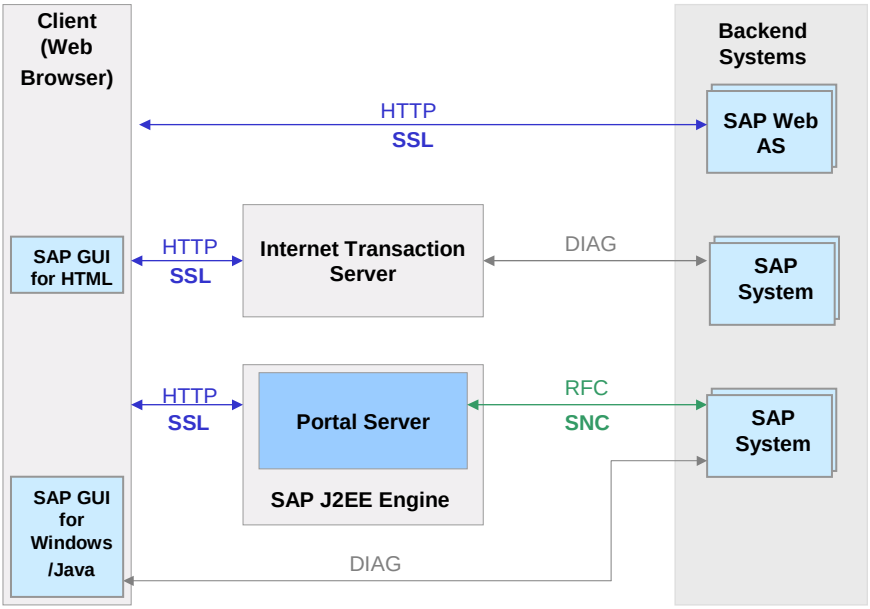
Communication with SAP Systems in the Back End

The portal's iView technology allows you to integrate a broad range of SAP applications, such as:

- SAP transactions
- Business Server Pages (BSPs)
- Business Warehouse (BW) reports
- Internet Application Components (IACs)
- MiniApps

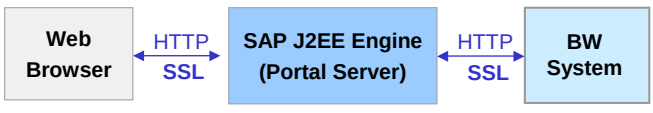
In each of these cases, the portal needs to connect to the SAP system in the back end to retrieve the required data and (in some cases) user interface.

The following diagram illustrates how SAP Enterprise Portal connects to SAP systems.



For most iViews that integrate SAP applications, the corresponding SAP systems are accessed via HTTP or HTTPS connections. This is the case for BSPs, IACs, MiniApps, BW reports, and SAP transactions that use SAP GUI for HTML. For example, if the browser sends a request to the portal server with a URL for an iView that integrates an IAC, the portal server converts the URL into a URL to the Internet Transaction Server (ITS) containing all the parameters that the ITS requires, such as the ID of the SAP system, the ID of the IAC, user information, and so on. It sends this URL to the browser, which redirects the URL to the ITS. The ITS then gets the data that it requires from the SAP system through a DIAG connection and finally sends a HTTP(S) response to the browser. There is no direct connection between the portal server and the SAP system in the backend.

If the portal is set up to run BW reports in caching mode, then the process is slightly different. When the portal server receives a request for a BW report, it sends a request via HTTP to the BW system. When the BW system sends its response, the portal server caches it, before sending it to the browser. In this case, there is a direct HTTP connection between the portal server and the BW system. This is illustrated in the following diagram.



In the case of iViews that integrate SAP transactions using SAP GUI for Windows or SAP GUI for Java, the browser accesses the SAP system using a DIAG connection.

If SAP systems are accessed through iViews that use the SAP Java Connector (JCo) to access the SAP System, the system is accessed via remote function calls (RFC).

If sensitive data, such as passwords, financial information, or data that underlies particular legal protection, is being sent over these connections, we recommend that you secure the connection. The following table provides an overview of the communication channels and where to find the relevant documentation.

Connection	Protocol	Documentation
Web browser ↔ Web Application Server	HTTP or HTTPS	Configuring the Use of SSL on the SAP J2EE Engine [SAP Library]
Web browser ↔ Internet Transaction Server	HTTP or HTTPS	SNC User's Guide [Page 21]
Portal Server ↔ SAP System	RFC or Secure Network Communication (SNC)	Configuring SNC (SAP J2EE Engine → ABAP Engine) [SAP Library] and Configuring SNC Between a Java iView and an ABAP System [SAP Library]
SAP GUI for Windows/Java ↔ SAP System	DIAG – can be protected using SNC	SNC User's Guide [Page 21]

If you have set up a network architecture with one or more firewalls and your portal integrates iViews for BSPs, IACs, MiniApps, BW reports, and so on, you need to set up a direct access in the firewall between the client machine and the ITS or WAS.

Communication with Databases in the Back End

The portal provides an iView wizard framework for creating iViews over database applications via a JDBC provider. The wizard enables you to build a data query based on a function predefined in the database, or based on a customized query.

If the database in the back end is a Microsoft SQL server, it must be set up for authentication based on SQL *Server and Windows NT* mode (mixed mode). If it is set up for *Windows only* mode, the connection does not work.

5.2 Network Security

We strongly recommend using firewalls to control network traffic in the portal system landscape. A 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.

The network architecture that you require for your specific portal installation depends on how sensitive the data and applications are that you can access through the portal. Many different constellations are possible. For our recommendation for a portal installation that requires a medium level of security or higher, see Using Multiple Network Zones [SAP Library]. In this network architecture, the portal server and its underlying SAP Web Application Server Java would be located in the inner DMZ. Any backend systems such as SAP systems would be located in the high security area. User persistence stores such as a corporate LDAP directory server or an ABAP-based SAP system would also be located in the high security area.

If you are using Search and Classification (TREX) with your portal installation, we suggest that you install the TREX server on a separate host to the portal server and separate the two servers with a packet-filtering firewall. For optimum security, the TREX server should only be accessible by the portal and not by normal users. For more information on TREX security, see Search and Classification (TREX) Security Guide [SAP Library].

6 Operating System Security

If the underlying operating system of your portal installation is not sufficiently secured, attackers can exploit existing vulnerabilities at operating system level. For this reason the operating systems on all machines of your portal installation (Portal Server machine, persistence layer machine, and so on) should be hardened. Hardening the operating system means to configure it as securely as possible and includes the following:

- Apply all available patches to the operating system before using it for the portal.
- Deactivate or de-install any service that is not needed for the operation of the portal.

7 Dispensable Functions with Impacts on Security

ActiveX Controls

The portal uses ActiveX controls to display content in the portal catalog. As security weaknesses in ActiveX controls can be exploited, you may wish to disable them on your clients. By making the corresponding settings on your clients and on the portal server, you can deactivate ActiveX controls while still keeping the full functions of the portal.

If you disable ActiveX controls, the performance of your portal installation decreases. This is because the portal has to emulate the tasks of the ActiveX controls.

For more information on how to deactivate ActiveX controls in your portal, see Enabling an ActiveX-Free Portal [SAP Library]. This is supported on all supported Microsoft Internet Explorer versions.

8 Other Security-Relevant Information

Secure Installation

For Windows platforms, we recommend that you install the J2EE Engine and the portal on a different drive than the operating system. If possible, no other software should be installed on the drive with the portal and the J2EE Engine. This is a defense-in-depth measure to reduce the impact of directory traversal attacks for both the portal application and user-written iViews.

9 Trace and Log Files

The User Management Engine (UME) used by the portal logs important security events, for example, user logon or changes to a user's permissions. For more information, see Logging and Tracing [SAP Library]. For details on which information is logged, see What is Logged? [SAP Library].

10 Appendix

Related Security Guides

You can find more information about the security of SAP applications on SAP Service Marketplace at **`service.sap.com/security`**. Security guides are available at **`service.sap.com/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
Master guides, installation guides, upgrade guides, solution management guides for SAP NetWeaver 04	*Instguidesnw04*
SAP Notes	*notes*
Released platforms	*pam*
Network security	*network* *securityguide*
Technical infrastructure	*ti*
SAP Solution Manager	*solutionmanager*
NetWeaver documentation, including How-To Guides and SAP Notes	*nw04doc*
Information about SAP Enterprise Portal	*nw-ep*
SNC User's Guide	**`service.sap.com/security`** → *Security in Detail* → *Secure System Management* → *SNC User's Guide*