

Security Guide for SAP Portfolio and Project Management 5.0



Copyright

© Copyright 2011 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, Excel, Outlook, and PowerPoint are registered trademarks of Microsoft Corporation.

IBM, DB2, DB2 Universal Database, System i, System i5, System p, System p5, System x, System z, System z10, System z9, z10, z9, iSeries, pSeries, xSeries, zSeries, eServer, z/VM, z/OS, i5/OS, S/390, OS/390, OS/400, AS/400, S/390 Parallel Enterprise Server, PowerVM, Power Architecture, POWER6+, POWER6, POWER5+, POWER5, POWER, OpenPower, PowerPC, BatchPipes, BladeCenter, System Storage, GPFS, HACMP, RETAIN, DB2 Connect, RACF, Redbooks, OS/2, Parallel Sysplex, MVS/ESA, AIX, Intelligent Miner, WebSphere, Netfinity, Tivoli and Informix are trademarks or registered trademarks of IBM Corporation.

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

Adobe, the Adobe logo, Acrobat, PostScript, and Reader are either trademarks or registered trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Oracle and Java are registered trademarks of Oracle.

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.

SAP, R/3, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP BusinessObjects Explorer, StreamWork, SAP HANA, 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 other countries.

Business Objects and the Business Objects logo, BusinessObjects, Crystal Reports, Crystal Decisions, Web Intelligence, Xcelsius, and other Business Objects products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of Business Objects Software Ltd. Business Objects is an SAP company.

Sybase and Adaptive Server, iAnywhere, Sybase 365, SQL Anywhere, and other Sybase products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of Sybase, Inc. Sybase is an SAP company.

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/instguides`

Icons in Body Text

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*.

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.

Security Guide Template	6
History of Changes	6
SAP Project and Portfolio Management Security Guide	7
Introduction.....	7
Before You Start	10
Technical System Landscape	12
Security Aspects of Data, Data Flow and Processes	13
User Administration and Authentication.....	16
User Management.....	16
Integration into Single Sign-On Environments.....	18
Authorizations.....	19
Session Security Protection	23
Network and Communication Security.....	24
Communication Channel Security.....	25
Network Security	27
Communication Destinations	32
Internet Communication Framework Security	33
Data Storage Security.....	34
Security for Additional Applications	35
Dispensable Functions with Impacts on Security.....	36
Enterprise Services Security	37
Other Security-Relevant Information	38
Security-Relevant Logging and Tracing.....	41
Services for Security Lifecycle Management	44
Appendix	46



History of Changes

Date	Topic	Description of Change
April 2010	1.0	First version of the Security Guide for SAP Portfolio and Project Management 5.0
December 2010	1.1	Updated version of the Security Guide for SAP Portfolio and Project Management 5.0 according to the new template
November 2011	Security-Relevant Logging and Tracing	Update of Subchapter <i>Reports Logging to the Application Log</i>
January 2014	Virus Scan	Enhancements in chapter <i>Other Security-Relevant Information</i>



SAP Portfolio and Project Management Security Guide



Introduction



This guide is available in English only. It does not replace the daily operations handbook that we recommend customers create for their specific productive operations.

Target Audience

- Technology consultants
- Security 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, whereas the Security Guides provide information that is relevant for all life cycle phases.

Why Is Security Necessary?

With the increasing use of distributed systems and the Internet for managing business data, demands on security are also on the rise. When using a distributed system, you need to be sure that your data and processes support your business needs without allowing unauthorized access to critical information. User errors, negligence, or attempted manipulation on your system should not result in loss of information or processing time. These demands on security also apply to the SAP Portfolio and Project Management Security Guide. We provide this guide to assist you in securing SAP Portfolio and Project Management.

About this Document

The Security Guide provides an overview of the security-relevant information that applies to SAP Portfolio and Project Management.

Overview of the Main Sections

The Security Guide comprises the following main sections:

- **Before You Start**
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.
- **Technical System Landscape**
This section provides an overview of the technical components and communication paths that are used by SAP Portfolio and Project Management.
- **Security Aspects of Data, Data Flow and Processes**
This section provides an overview of security aspects involved throughout the most widely-used processes within SAP Portfolio and Project Management.
- **User Administration and Authentication**

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

- Recommended tools to use for user management
- Overview of how integration into Single Sign-On environments is possible

- **Authorizations**

This section provides an overview of the authorization concept that applies to SAP Portfolio and Project Management.

- **Session Security Protection**

This section provides information about activating secure session management, which prevents JavaScript or plug-ins from accessing the SAP logon ticket or security session cookie(s).

- **Network and Communication Security**

This section provides an overview of the communication paths used by SAP Portfolio and Project Management and the security mechanisms that apply. It also includes our recommendations for the network topology to restrict access at the network level.

- **Internet Communication Framework Security**

This section provides an overview of the Internet Communication Framework (ICF) services that are used by SAP Portfolio and Project Management.

- **Data Storage Security**

This section provides an overview of any critical data that is used by SAP Portfolio and Project Management and the security mechanisms that apply.

- **Security for Third-Party or Additional Applications**

This section provides security information that applies to third-party or additional applications that are used with SAP Portfolio and Project Management.

- **Dispensable Functions with Impacts on Security**

This section provides an overview of functions that have impacts on security and can be disabled or removed from the system.

- **Other Security-Relevant Information**

This section contains information about:

- Documents (including Virus Scanner)
- Activating HTTP-Based Document Management
- MS Project Integration
- Definition of Security Lists for OfficeControls
- Export to PDF and MS Excel
- Gantt Chart
- Import from Microsoft Excel

- **Security-Relevant Logging and Tracing**

This section provides an overview of the trace and log files that contain security-relevant information, for example, so you can reproduce activities if a security breach does occur.

- **Services for Security Lifecycle Management**

This section provides an overview of services provided by Active Global Support that are available to assist you in maintaining security in your SAP systems on an ongoing basis.

- **Appendix**

This section provides references to further information.



Before You Start

Fundamental Security Guides

SAP Portfolio and Project Management comprises Project Management and Portfolio Management, all of which are based on the SAP NetWeaver Application Server (SAP NetWeaver AS) including SAP Business Foundation Layer (SAP_BS_FND). You should therefore take the security information for the SAP NetWeaver AS into consideration. This guide only describes the security information that differs from it, as well as additional security information.

Fundamental Security Guides

Related Security Guides

Application	Guide	Most Relevant Sections or Specific Restrictions
SAP NetWeaver AS	SAP Security Guide	
SAP NetWeaver Portal	SAP NetWeaver Portal Security Guide	

For a complete list of the available SAP Security Guides, see SAP Service Marketplace at <http://service.sap.com/securityguide>.

Important SAP Notes

The most important SAP Notes that apply to the security of SAP Portfolio and Project Management are shown in the table below.

SAP Note Number	Title
216419	Multi-Level Caching and Content Server Proxies
128447	Trusted/Trusting Systems
517484	Inactive Services in the Internet Communication Framework
1436778	PPM 5.0: Restrictions
1411953	PPM 5.0: Configuration Content
1416519	PPM 5.0: Support Package Schedule
1417134	PPM 5.0: List of all BADIs

For a list of additional security-relevant SAP Hot News and SAP Notes, see also SAP Service Marketplace at <http://service.sap.com/securitynotes>.

Configuration

You can find a summary of the configuration steps for implementing security for SAP Portfolio and Project Management in the *Basic Settings for Project Management* and the *Basic Settings for Portfolio Management* in SAP Solution Manager.

Additional Information

For more information about specific topics, see the Quick Links as shown in the table below.

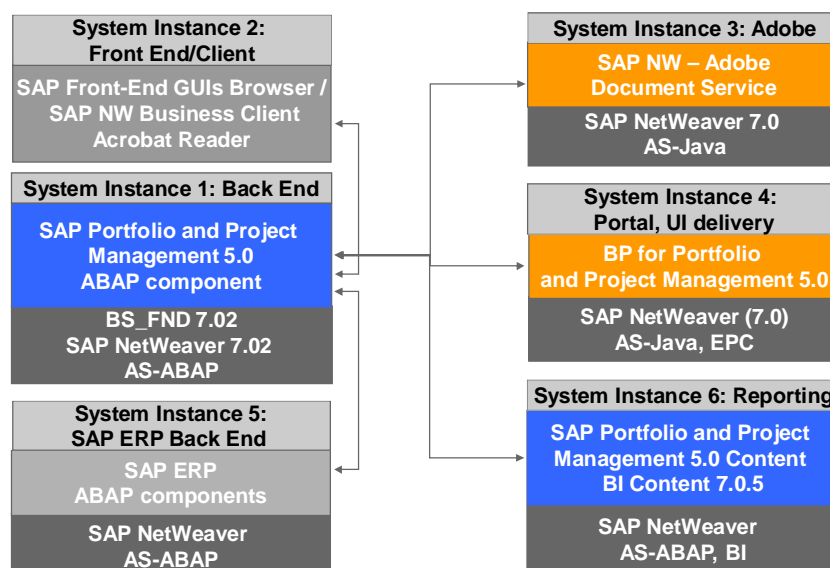
Content	Quick Link on SAP Service Marketplace or SDN
Security	http://sdn.sap.com/irj/sdn/security
Security Guides	http://service.sap.com/securityguide
Related SAP Notes	http://service.sap.com/notes http://service.sap.com/securitynotes
Released platforms	http://service.sap.com/pam
Network security	http://service.sap.com/securityguide
SAP Solution Manager	http://service.sap.com/solutionmanager
SAP NetWeaver	http://sdn.sap.com/irj/sdn/netweaver



Technical System Landscape

Use

The figure below shows an overview of the technical system landscape for SAP Portfolio and Project Management 5.0.



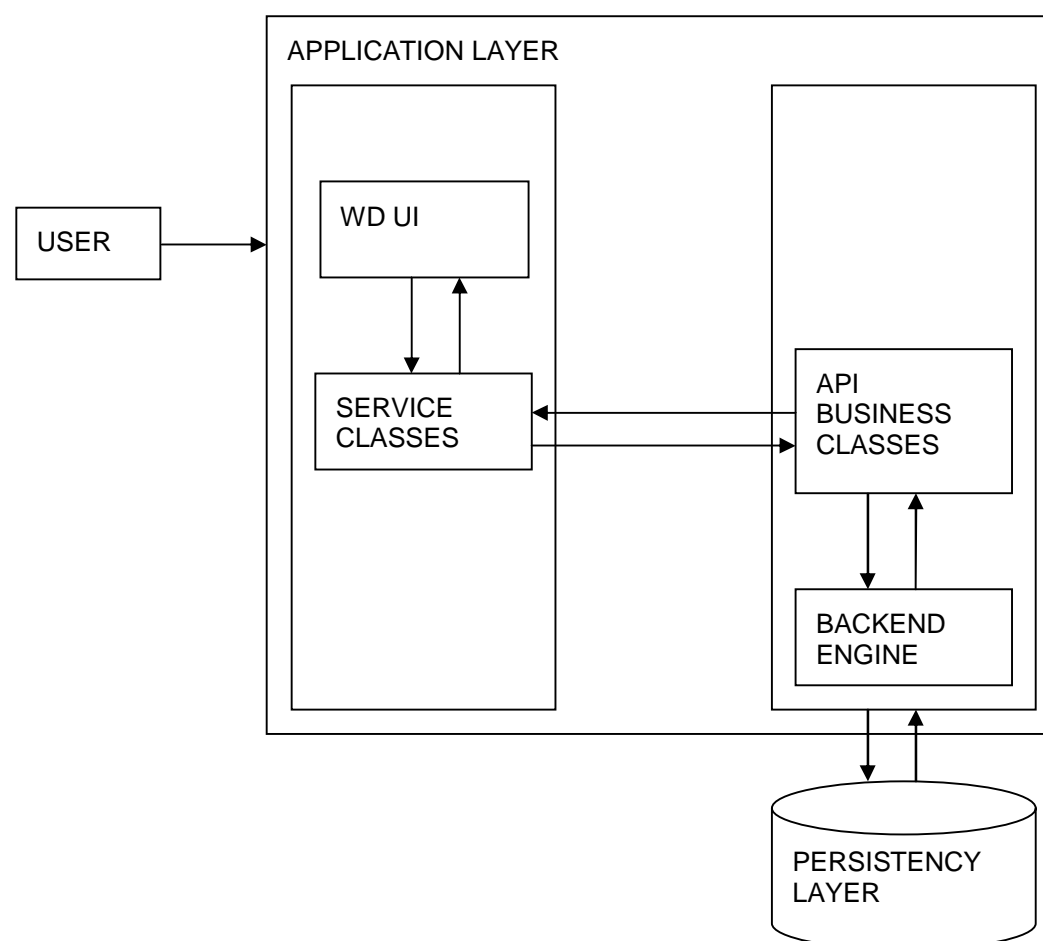
For more information about the technical system landscape, see the resources listed in the table below.

Topic	Guide/Tool	Quick Link on SAP Service Marketplace or SDN
Technical description for SAP Portfolio and Project Management and the underlying components such as SAP NetWeaver	<i>Master Guide</i>	http://service.sap.com/instguides
High availability	<i>High Availability for SAP Solutions</i>	http://sdn.sap.com/irj/sdn/ha
Technical landscape design	See applicable documents	http://sdn.sap.com/irj/sdn/landscapedesign
Security	See applicable documents	http://sdn.sap.com/irj/sdn/security



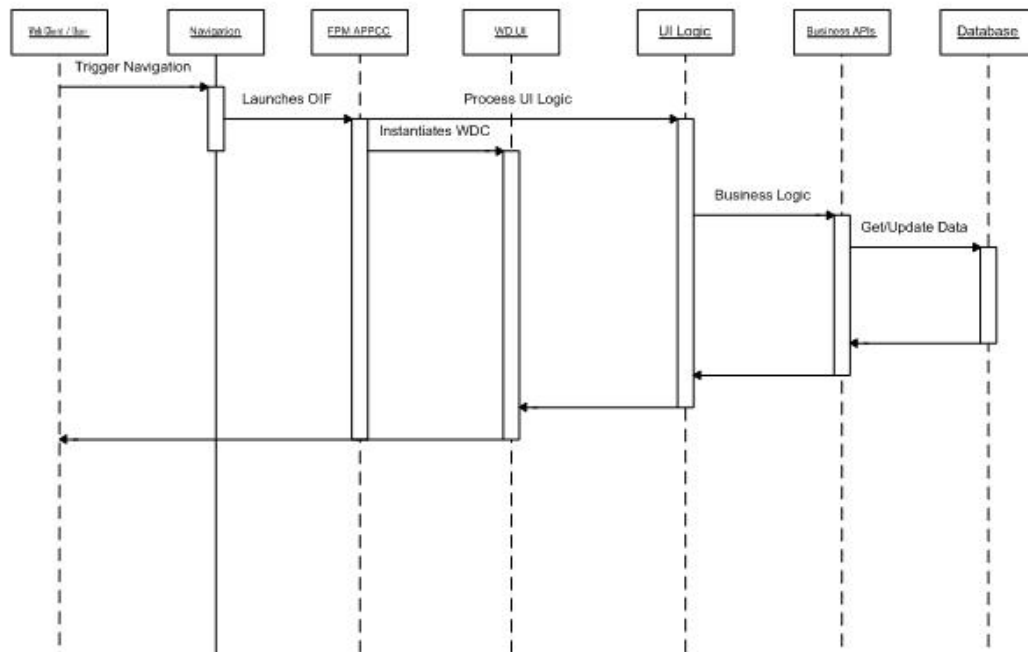
Security Aspects of Data, Data Flow and Processes

The figure below shows an overview of the data flow for SAP Portfolio and Project Management.



Step	Description	Security Measure
1	User logs in to SAP Portfolio and Project Management	User credentials are checked
2	When the user logs on to the application, the data shown on the user interface is retrieved via services classes, which interact with business API classes, which in turn connect with the database.	The system checks the user's application and object level authorization at all levels to retrieve data.
3	When the user updates and saves data, the data flows to service classes, then to business API classes, and from there to the database.	The system checks the user's application and object level authorization at all levels to retrieve data.

The figure below shows an overview of the process for SAP Portfolio and Project Management.



The table below shows the security aspect to be considered for the process step and what mechanism applies.

Step	Description	Security Measure
1	The user logs on to SAP Portfolio and Project Management.	The system checks the user credentials.
2	The user opens any dashboard.	The system fetches the data based on the user, application, and object level authorizations.
3	The user clicks on any object.	The system checks the user authorization for the object again and only then calls up the navigation.
4	The system opens the window.	Based on the parameters available, the system determines and launches the destination window.
5	The system retrieves the data.	The data request flows from the user interface to the logical classes, then to the business APIs, and finally to the database. The data is retrieved according to user authorization.
6	The system displays data on the user interface.	The data flows back from the database to business APIs, then to the logical classes, and then to the user interface.

7	The user modifies and saves the data.	<p>Data flows from the user interface to the logical classes, then to business APIs, and finally to the database.</p> <p>The system updates the data according to the user authorization. The updated data flows back from the database to business APIs, then to the logical classes, and finally to the user interface.</p>
---	---------------------------------------	---



User Administration and Authentication

For an overview of user administration and authentication in SAP Portfolio and Project Management, see the following sections:

- [User Management](#)
- [Integration into Single Sign-On Environments](#)

SAP Portfolio and Project Management uses the user management and authentication mechanisms provided with the SAP NetWeaver platform, in particular the SAP NetWeaver Application Server ABAP and Java. Therefore, the security recommendations and guidelines for user administration and authentication as described in the SAP NetWeaver Application Server ABAP Security Guide and/or SAP NetWeaver Application Server Java Security Guide also apply to SAP Portfolio and Project Management.

For more information, see SAP Help Portal at <http://help.sap.com> → *NetWeaver* → *<Release>* → *SAP NetWeaver Library* → *SAP NetWeaver Security Guide* → *Security Guides for SAP NetWeaver According to Usage Types* → *Security Guide for Usage Type AS* →

- *SAP NetWeaver Application Server ABAP Security Guide.*
- *SAP NetWeaver Application Server JAVA Security Guide.*

In addition to these guidelines, we include information about user administration and authentication that specifically applies to SAP Portfolio and Project Management in the following topics:

- [User Management](#)
- [Integration into Single Sign-On Environments](#)

This topic lists the tools to use for user management.

This topic describes how SAP Portfolio and Project Management supports Single Sign-On mechanisms.



User Management

In SAP Portfolio and Project Management, you use the SAP user administration of the SAP NetWeaver AS to create all users. For more information about creating users in the SAP NetWeaver AS, see SAP Help Portal at <http://help.sap.com> → *SAP NetWeaver* → *<Release>* → *SAP NetWeaver Library* → *SAP NetWeaver by Key Capability* → *Security* → *Identity Management* → *User and Role Administration of AS ABAP*.

In SAP Portfolio and Project Management, you can create users with the SAP Human Resources (SAP HR) integration scenario. You can make the relevant settings in Customizing for *Portfolio Management* under *Global Customizing* → *Global Settings* → *Define Global Settings / Override Default Global Settings*. For more information, see the *Basic Settings for Project Management* and the *Basic Settings for Portfolio Management* in SAP Solution Manager.

You can also use SAP NetWeaver Identity Management to manage users and authorizations in SAP Portfolio and Project Management. For more information, see SAP Help Portal at <http://help.sap.com> → *SAP Business Suite* → *SAP Portfolio and Project Management* → *SAP Portfolio and Project Management 5.0* → *Common Functions* → *SAP Identity Management for SAP Portfolio and Project Management*.

Use

User management for SAP Portfolio and Project Management uses the mechanisms provided with the SAP NetWeaver Application Server ABAP and Java, for example, tools, user types, and password policies. For an overview of how these mechanisms apply for SAP Portfolio and Project Management, see the sections below.

User Administration Tools

The table below shows the tools to use for user management and user administration with SAP Portfolio and Project Management.

User Management Tools

Tool	Detailed Description	Prerequisites
User and role maintenance with SAP NetWeaver AS ABAP (Transactions SU01, PFCG)	For more information, see SAP Help Portal at http://help.sap.com → SAP NetWeaver → <Release> → SAP NetWeaver Library → SAP NetWeaver by Key Capability → Security → Identity Management → User and Role Administration of AS ABAP.	n/a
User Management Engine with SAP NetWeaver AS Java	For more information, see SAP Help Portal at http://help.sap.com → SAP NetWeaver → <Release> → SAP NetWeaver Library → SAP NetWeaver by Key Capability → Security → Identity Management → User Management of the Application Server Java → User Management Engine.	n/a
Identity Management for SAP Portfolio and Project Management	For more information, see SAP Help Portal at http://help.sap.com → SAP Portfolio and Project Management → SAP Portfolio and Project Management 5.0 → Portfolio and Project Management → Common Functions → Identity Management for SAP Portfolio and Project Management.	n/a



Integration into Single Sign-On Environments

SAP Portfolio and Project Management is based on HTTP Internet applications. Therefore, they support the logon mechanisms provided by the SAP NetWeaver AS. This means that they accept SAP logon tickets, as well as X.509 digital certificates.

For more information, see SAP Help Portal at <http://help.sap.com> → *NetWeaver* → *<Release>* → *SAP NetWeaver Library* → *SAP NetWeaver by Key Capability* → *Security* → *SAP NetWeaver Security Guide* → *SAP NetWeaver Application Server ABAP Security Guide* → *User Authentication*.

Use

SAP Portfolio and Project Management supports the Single Sign-On (SSO) mechanisms provided by SAP NetWeaver. Therefore, the security recommendations and guidelines for user administration and authentication as described in the [SAP NetWeaver Security Guide \[External\]](#) also apply to SAP Portfolio and Project Management.

For more information, see SAP Help Portal at <http://help.sap.com> → *NetWeaver* → *<Release>* → *SAP NetWeaver Library* → *SAP NetWeaver Security Guide*.

For more information about the available authentication mechanisms, see SAP Help Portal at <http://help.sap.com> → *NetWeaver* → *<Release>* → *SAP NetWeaver Library* → *Administrator's Guide* → *SAP NetWeaver Security Guide* → *User Authentication and Single Sign-On*.



Authorizations

Authorizations

In Project Management and Portfolio Management, authorizations are controlled in the following ways:

- ABAP authorization objects and roles

This is the standard method for controlling access to transactions and programs in an SAP ABAP system. Authorizations are combined in an authorization profile that is associated with a role. User administrators can then assign the corresponding roles via the user master record, so that the user can access the appropriate transactions for his or her tasks.

For more information, see SAP Help Portal at <http://help.sap.com> → *SAP NetWeaver* → <Release> → *SAP NetWeaver Library* → *SAP NetWeaver by Key Capability* → *Security* → *SAP NetWeaver Security Guide* → *SAP NetWeaver Application Server ABAP Security Guide* → *SAP Authorization Concept*.

- Access control lists

These allow you to add another level of security by controlling authorization at object level. For example, you can control who has authorization to change a particular project definition or collaboration.

You can define the menu options in the navigation area using portal content adjustments or PFCG role Customizing.

In **Project Management only**, you can use the following additional authorization mechanisms:

- System administrators can grant access to objects by choosing *Portfolio and Project Administration* → *Project Authorization Administration* in the application. This is an exception to the normal process and is only used if the administrator of the object is not available due to illness, for example. The system sends the "new" and "old" administrators an e-mail to inform them of the new authorization holder. For more information, see the *Granting Administration Authorization for an Object* section of the *Basic Settings for Project Management* in SAP Solution Manager.

Authorizations regarding BAPIs, reports, and (RFC-enabled) function modules:

In SAP Portfolio and Project Management 5.0, multiple BAPIs, reports and (RFC-enabled) function modules are available to create, read, change, edit, update, and delete the data of SAP Portfolio and Project Management. Additionally, via (RFC-enabled) function modules and reports data is read from the (optional) ERP system. Therefore, using these BAPIs, reports, and function modules access to and manipulation of Portfolio and Project Management data as well as read access to ERP data is possible. Thus, the authorization for using these BAPIs, reports, and function modules (via transactions, for example), should be restricted to users who are intended to have these authorizations and the corresponding access to data. For more information about creation of roles and the authorization concept, see SAP Help Portal at <http://help.sap.com> → *SAP NetWeaver* → <Release> → *SAP NetWeaver Library* → *SAP NetWeaver by Key Capability* → *Security* → *Identity Management* → *User and Role Administration of AS ABAP* → *AS ABAP Authorization Concept*.

Authorizations regarding search results

You can use the BAdI *BADI_DPR_SEARCH* to modify search results. You can filter the result set implementing this BAdI depending on the specified search helps which exist for each Portfolio and Project Management object. Thus, you can, for example, hide all results for

which the user does not have read authorization from the result list. In the standard, these results are displayed in the result list, but the user cannot open or display these objects.

Authorizations regarding KM

You can define authorizations in KM so that users can only access documents for which he or she has authorization. For more information, see SAP Note 599425.

Use

SAP Portfolio and Project Management uses the authorization concept provided by the SAP NetWeaver AS ABAP or AS Java. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide ABAP and SAP NetWeaver AS Security Guide Java also apply to SAP Portfolio and Project Management.

The SAP NetWeaver authorization concept is based on assigning authorizations to users based on roles. For role maintenance, use the profile generator (transaction PFCG) on the AS ABAP and the User Management Engine's user administration console on the AS Java.



For more information about how to create roles, see SAP NetWeaver Library → SAP NetWeaver by Key Capability → Security → Identity Management → User and Role Administration of AS ABAP → Configuration of User and Role Administration → Role Administration.

Role and Authorization Concept for SAP Portfolio and Project Management

For SAP Portfolio and Project Management, SAP delivers one portal role (Portfolio and Project Management). For more information about this role, see SAP Help Portal at <http://help.sap.com> → *SAP Business Suite* → *SAP Portfolio and Project Management* → *SAP Portfolio and Project Management 5.0* → *Business Package for SAP Portfolio and Project Management 5.0*.



In SAP Portfolio and Project Management, you carry out Customizing activities in the SAP NetWeaver AS. Only system administrators, that is, users with the authorization profile SAP_ALL, are authorized to carry out Customizing for SAP Portfolio and Project Management.

You can maintain the following role authorizations in Project Management and Portfolio Management using the SAP Profile Generator.

Project Management Roles

The following single roles are delivered with Project Management:

Role	Authorization
SAP_CPR_PROJECT_ADMINISTRATOR	Create projects (project definitions).
SAP_CPR_TEMPLATE_ADMINISTRATOR	Create, change, read, and delete all templates in Project Management.

SAP_CPR_USER	Use Project Management, but no authorization to perform any activities in a particular project. To do this users need project-specific authorizations, which can be distributed either directly via ACLs or through their assignment to a role. This role must be included in every Project Management composite role.
SAP_CPR_BCV_USER	Project-Management-specific authorization for using BCV content in resource management.
SAP_BPR_PPM	SAP Portfolio and Project Management PFCG role for NW BC

The following composite roles are delivered with Project Management:

Role	Authorization
SAP_CPR_DECISION_MAKER	Decision maker in Project Management. Contains the role SAP_CPR_USER.
SAP_CPR_INTERESTED	Interested party in Project Management. Contains the role SAP_CPR_USER.
SAP_CPR_MEMBER	Team member in Project Management. Contains the role SAP_CPR_USER.
SAP_CPR_PROJECT_LEAD	Project manager in Project Management. Contains the role SAP_CPR_PROJECT_ADMINISTRATOR and SAP_CPR_USER
SAP_CPR_BCV_USER_COMP	Composite role containing the general role for using BCV (SAP_BCV_USER) and the Project Management specific role (SAP_CPR_BCV_USER).
SAP_CPR_TEMPLATE_RESPONSIBLE	Project Management template responsible. Contains the roles SAP_CPR_TEMPLATE_ADMINISTRATOR and SAP_CPR_USER

You can use these SAP standard roles or create your own. For more information, see the *Activating Single Roles for Project Management* section and the *Creating Roles for the Project-Specific Authorization Checks* section of the *Basic Settings for Project Management* in SAP Solution Manager.

Portfolio Management Roles

For Portfolio Management SAP delivers the following roles:

Roles	Authorization
SAP_XRPM_ADMINISTRATOR	Superuser authorization in Portfolio Management. Used to create new portfolios. This role also provides the assigned user full access to all Portfolio Management business objects in the system.

SAP_XRPM_USER	General user in Portfolio Management. All users should be assigned this role. Has general authorizations to use Portfolio Management, but no specific object access. This access must be assigned to the user via ACLs.
SAP_RPM_BCV_USER	Portfolio Management specific authorization for BCV content in Portfolio Management
SAP_RPM_BCV_USER_COMP	Composite role containing the general role for using BCV (SAP_BCV_USER) and the Portfolio Management specific role (SAP_RPM_BCV_USER).
SAP_BPR_PPM	PFCG role for NWBC in SAP Portfolio and Project Management

You can use these SAP standard roles or create your own. For more information about roles in Portfolio Management, see the *Activating Single Roles for Portfolio Management (PFCG)* section and the *Creating Roles for the Portfolio-Specific Authorization Checks* section of the *Basic Settings for Portfolio Management* in SAP Solution Manager.



Session Security Protection

To increase security and prevent access to the SAP logon ticket and security session cookie(s), we recommend activating secure session management.

We also highly recommend using SSL to protect the network communications where these security-relevant cookies are transferred.

Session Security Protection on the AS ABAP

To activate session security on the AS ABAP, set the corresponding profile parameters and activate the session security for the client(s) using the transaction SICF_SESSIONS.

For more information, a list of the relevant profile parameters, and detailed instructions, see SAP Help Portal at <http://help.sap.com> → NetWeaver → <Release> → SAP NetWeaver Library → SAP NetWeaver by Key Capability → Security → User Authentication and Single Sign-On → Authentication on the AS ABAP → Using SAML 2.0 → Activating HTTP Security Session Management on AS ABAP.

Session Security Protection on the AS Java

AS Java is optional for SAP Portfolio and Project Management 5.0. It is needed for:

- Usage of ADS (ADS can be installed on the same server as SAP Portfolio and Project Management 5.0 but also on a separate server). For more information, see SAP Service Marketplace at <http://service.sap.com/instguides> → SAP Business Suite Applications → SAP PLM → using SAP Portfolio and Project Management 5.0 → Master Guide - SAP Portfolio and Project Management / Upgrade Master Guide - SAP Portfolio and Project Management → Adobe in SAP Portfolio and Project Management.
- Usage of SAP Portfolio and Project Management in SAP NetWeaver Portal (optional).
- Usage of the optional JAVA component PPM_KM. It is only relevant for Portfolio Management and only required if KM document management is used.

On the AS Java, set the properties described in *Session Security Protection* using the Visual Administrator. For more information, see SAP Help Portal at <http://help.sap.com> → NetWeaver → <Release> → SAP NetWeaver Library → Administrator's Guide → SAP NetWeaver Security Guide → Security Guides for SAP NetWeaver According to Usage Types → Security Guide for Usage Type AS → SAP NetWeaver Application Server Java Security Guide → Other Security Relevant Information → Session Security Protection.



Network and Communication Security

Your network infrastructure is extremely important in protecting your system. Your network needs to support the communication necessary for your business needs without allowing unauthorized access. A well-defined network topology can eliminate many security threats based on software flaws (at both the operating system and application level), or network attacks such as eavesdropping. If users cannot log on to your application or database servers at the operating system or database layer, then there is no way for intruders to compromise the machines and gain access to the backend system's database or files. Additionally, if users are not able to connect to the server LAN (local area network), they cannot exploit well-known bugs and security holes in network services on the server machines.

The network topology for SAP Portfolio and Project Management is based on the topology used by the SAP NetWeaver Application Server. Therefore, the security guidelines and recommendations described in the SAP NetWeaver AS Security Guide also apply to SAP Portfolio and Project Management. Details that specifically apply to SAP Portfolio and Project Management are described in the following topics:

- [Communication Channel Security](#)
This topic describes the communication paths and protocols used by SAP Portfolio and Project Management
- [Network Security](#)
This topic describes the recommended network topology for SAP Portfolio and Project Management. It shows the appropriate network segments for the various client and server components and where to use firewalls for access protection. It also includes a list of the ports needed to operate SAP Portfolio and Project Management.
- [Communication Destinations](#)
This topic describes the information needed for the various communication paths, for example, which users are used for which communications.

For more information, see the following sections in the SAP NetWeaver Security Guide on SAP Help Portal at <http://help.sap.com> → *NetWeaver* → *<Release>* → *SAP NetWeaver Library* → *Administrator's Guide* → *SAP NetWeaver Security Guide*:

- *Network and Communication Security*
- *Security Guides for Connectivity and Interoperability Technologies*



Communication Channel Security

Use

Communication Channel Security

SAP Portfolio and Project Management Communication Channel Security

Communication Channel	Communication Technology	Data Transferred	Comment/Security Recommendation
SAP Portfolio and Project Management front end (browser) to the SAP NW Application Server (SAP NetWeaver AS)	HTTP(S)	Files, metadata, and user data (passwords, user names)	
WebDAV interface	HTTP(S) with WebDAV extension	Files and metadata	WebDAV interface is used to connect the KM repository, and also front-end WebDAV clients In Portfolio Management, the WebDav interface is only relevant for the initiative.
Project Management front end (browser) to content or cache servers	HTTP(S)	Files	
SAP NetWeaver AS to content or cache servers	HTTP(S)	Metadata, files	
SAP NetWeaver AS to other application servers (for example, SRM, HR, CO)	RFC	Metadata, files	SAP Portfolio and Project Management communicates with 3rd party or SAP systems to obtain or create information on object links between SAP Portfolio and Project Management and objects located in the 3rd party/SAP system. Possible SAP systems are: SAP R/3 4.6C and higher. The communication to 3rd party systems has to be implemented at the customer site. The 3rd party/SAP system never calls

			back. For more information, see the <i>Setting Up Object Links</i> section of the <i>Basic Settings for Project Management</i> and the <i>Basic Settings for Portfolio Management</i> in SAP Solution Manager.
Project Management NetWeaver AS to SRM via SAP XI	HTTP(S)	Metadata	
SAP Portfolio and Project Management on the NetWeaver AS to SAP PLM PS	RFC	Files, metadata	
SAP Portfolio and Project Management on the NetWeaver AS to SAP HCM	SAP ALE RFC	Files, metadata	

For information about security measures when using HTTP(S) in SAP Portfolio and Project Management, see [Network Security](#).



In SAP Portfolio and Project Management, there is no fixed port for communication and the firewall settings described in the SAP NetWeaver AS Security Guide apply. For more information, see SAP Help Portal at <http://help.sap.com> → SAP NetWeaver → <Release> → SAP NetWeaver Library → SAP NetWeaver by Key Capability → Security → SAP NetWeaver Security Guide → SAP NetWeaver Application Server ABAP Security Guide → Protecting Your Productive System (Change and Transport System).

DIAG and RFC connections can be protected using Secure Network Communications (SNC). HTTP connections are protected using the Secure Sockets Layer (SSL) protocol.



We strongly recommend using secure protocols (SSL, SNC) whenever possible.

For more information, see *Transport Layer Security* in the SAP NetWeaver Security Guide on SAP Help Portal at <http://help.sap.com> → NetWeaver → <Release> → SAP NetWeaver Library → Administrator's Guide → SAP NetWeaver Security Guide → Network and Communication Security → Transport Layer Security.



Network Security

SAP supports the following installation variant for SAP Portfolio and Project Management:

- **Installation of SAP Portfolio and Project Management within the intranet**
For internal collaboration only.

Installation Scenarios

Scenarios A and B can be used for SAP Portfolio and Project Management:

- [Scenario A: No Content Server](#)
- [Scenario B: One Hidden Content Server](#)

Installation scenario B, with one hidden content server, is the installation scenario with the highest level of security.

Ports

SAP Portfolio and Project Management runs on SAP NetWeaver and uses the ports from the AS ABAP or AS Java. For more information, see the topics for *AS ABAP Ports* and *AS Java Ports* in the corresponding SAP NetWeaver Security Guides. For other components, for example, SAPinst, SAProuter, or the SAP Web Dispatcher, see also the document *TCP/IP Ports Used by SAP Applications*, which is located on SAP Developer Network at <http://sdn.sap.com/irj/sdn/security> under *Infrastructure Security* → *Network and Communications Security*.

For more information, see SAP Help Portal at <http://help.sap.com> → *SAP NetWeaver* → *<Release>* → *SAP NetWeaver Library* → *SAP NetWeaver by Key Capability* → *Security* → *SAP NetWeaver Security Guide* → *Security Guides for SAP NetWeaver According to Usage Types* → *Security Guide for Usage Type AS* →

- *SAP NetWeaver Application Server ABAP Security Guide* → *Network Security for SAP Web AS ABAP* → *AS ABAP Ports*.
- *SAP NetWeaver Application Server Java Security Guide* → *Network Security* → *AS Java Ports*.

Use

SAP Portfolio and Project Management is an Internet scenario, therefore, the base server must be available not only to intranet (or internal) users, but also to Internet (or external) users all over the world. To protect the base server from malicious attacks and distorted requests, several standard Internet security components can be installed in front of the server, forming an Internet gateway. Some of these components, such as the SAP Web Dispatcher or the built-in features in the SAP NetWeaver Application Server (SAP NetWeaver AS), are from SAP, while other components like reverse proxies or hardware load balancers are non-SAP products. There are many components such as these in existence, which can be used alone or in conjunction with one another. This makes it impossible to recommend the best solution: it always depends on company policy, the existing server landscape, and individual security requirements.

In general, Internet gateway architecture consists of the following:

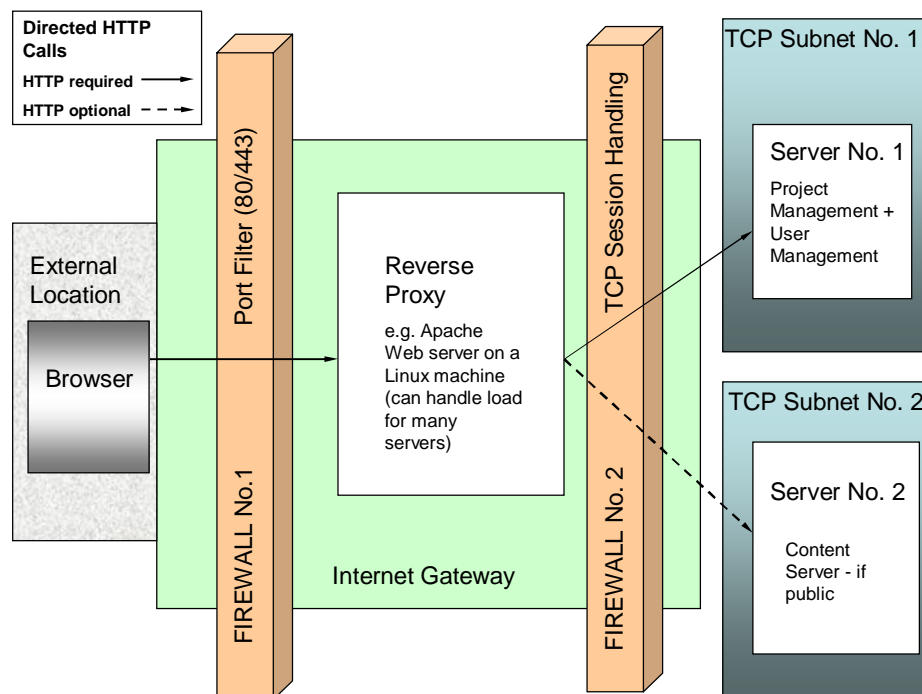
- **Outer firewall:** restricts HTTP requests to allowed ports and protocols, for example, only HTTPS requests on port 443 are allowed, everything else is blocked.

- Application proxies: servers without their own built-in logic, which accept requests, analyze them in terms of security rules, and route the requests towards the real application server. Reverse proxies or the SAP Web Dispatcher are types of application proxies.
- Inner firewall: restricts connections at IP level and checks the communication on TCP/IP low-level session handling.

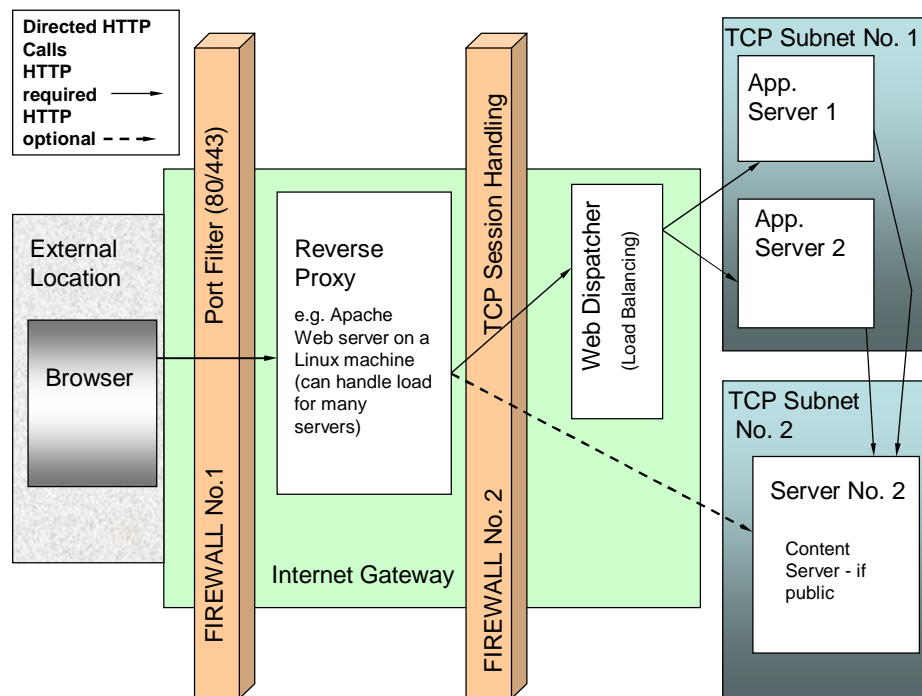
The following figures show two typical types of Internet gateway. The first one consists completely of non-SAP components, the second introduces the SAP Web Dispatcher for load-balancing purposes (this is unnecessary if there is only one application server).



These or similar types of Internet gateways must be placed in front of every HTTP server that can be accessed from the Internet. However, one Internet gateway can be used for several servers because the load on the Internet gateway is not high.



Internet Gateway Architecture with Non-SAP Components

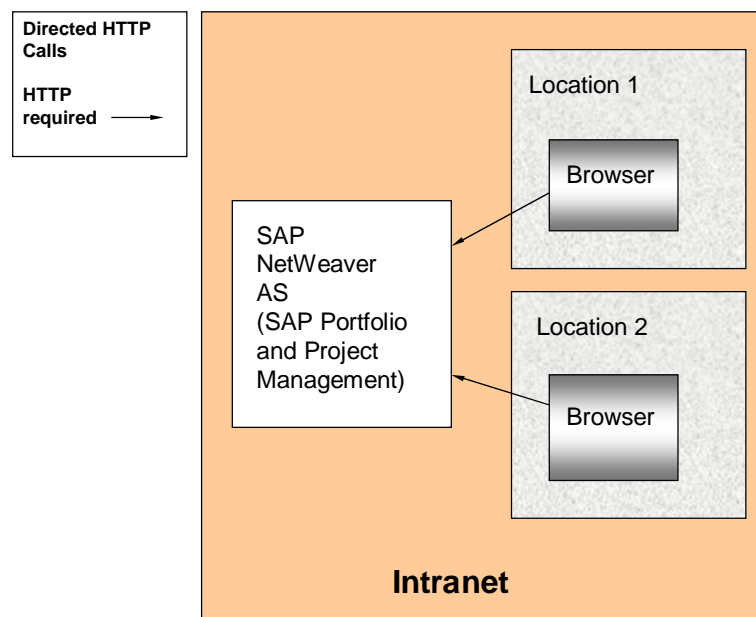


Internet Gateway Architecture with the SAP Web Dispatcher

Scenario A: No Content Server

In scenario A, the complete installation consists only of SAP Portfolio and Project Management server (SAP NetWeaver AS).

- The server is located in the intranet.



Scenario A: No Content Server

Definition of a Subnet

A subnet is an IP address range from which no other IP or Domain Name System (DNS) addresses that are located outside the network segment of the subnet can be reached. The implied consequences of this are as follows:

- You cannot reach external addresses from inside the subnet without the explicit use of proxy technology.
- With proxies between the subnet and external addresses, each access can be controlled at IP number level. This means that you can explicitly allow communication between IP 111.111.111.111 from inside the subnet to the address 222.222.222.222 outside the subnet, but to no other address worldwide.
- In particular, you can ensure that even if a server inside the subnet is hacked and conquered by an external hacker and this server is under complete control of the external hacker, the hacker cannot influence any other system outside the subnet. If there is no other server inside the subnet, it is impossible to gain access to any other system.



An important rule for network security states that HTTP calls should only be allowed from network areas with a high security level to network areas with the same or a lower security level, never the other way around.

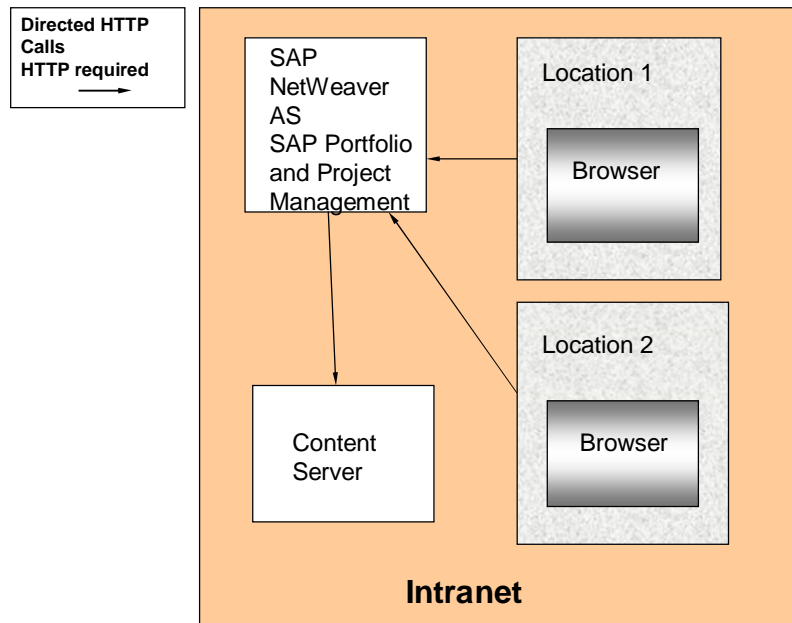
This means that a call from the intranet (high security) to a server in the DMZ (lower security) is acceptable. Without the subnet, however, the rule would be violated for the external user, because the extranet has the lowest security level. The introduction of the IP subnet is therefore recommended because it creates an isolated IP range that can be considered as an artificial area with an even lower level of security.

You can ensure that the transferred metadata and files are secure by using Secure Sockets Layer (SSL) technology. The SAP NetWeaver AS can be configured in such a way that it only allows HTTPS connections, and no HTTP connections. This is a requirement for the external user. The internal user could use HTTP, but in this case, you must ensure that the external user can only use the HTTPS address and not the HTTP address. You can achieve this by configuring the external firewall to allow access only via HTTPS to the IP addresses of the subnet in which the server is located.

Scenario B: One Hidden Content Server

In the second type of installation, one content server is added to the network environment.

- For SAP Portfolio and Project Management, the SAP NetWeaver AS and the content server are both located in the intranet.



Scenario B: One Hidden Content Server



Communication Destinations

Use

For the default SAP Portfolio and Project Management scenarios, no RFC destination pointing to external systems is required. However, if you are using the cFolders or Project Management application programming interfaces (APIs) via the SOAP wrapper, the APIs consist of RFC function modules.

SAP Portfolio and Project Management

- FI/CO integration / Accounting Integration
- Adobe Document Services (ADS)
- Knowledge management integration
- SAP NetWeaver Portal
- Object links to SAP R/3 or SAP ERP or xPD
- SAP HR integration

In the following areas, Portfolio Management RFCs are called from an external application:

- Project integration

The Project Management APIs are required for:

- cFolders integration
- SRM Integration
- Portfolio Management Integration
- If a user needs to use the APIs they must have the basic RFC authorization for the relevant API function modules. The SOAP wrapper adheres to the authorization rules that apply if the RFC module is called directly. The function group name for Project Management is CPR_API

To view the application-specific and basis authorization objects used in SAP Portfolio and Project Management, see [Role and Authorization Concept for SAP Portfolio and Project Management](#).

.

For more information about authorization objects and roles, see SAP Help Portal at <http://help.sap.com> → SAP NetWeaver → <Release> → SAP NetWeaver Library → SAP NetWeaver by Key Capability → Security → SAP NetWeaver Security Guide → SAP NetWeaver Application Server ABAP Security Guide → SAP Authorization Concept.



Internet Communication Framework Security

You should only activate those services that are needed for the applications running in your system. For more information about the services that are needed for SAP Portfolio and Project Management, see the *Activating Services* section of the *Basic Settings for Project Management* and the *Basic Settings for Portfolio Management* in SAP Solution Manager.

Use the transaction SICF to activate these services.

If your firewall(s) use URL filtering, also note the URLs used for the services and adjust your firewall settings accordingly.

For more information, see SAP Help Portal at <http://help.sap.com> → SAP NetWeaver → <Release> → SAP NetWeaver Library → SAP NetWeaver by Key Capability → Application Platform by Key Capability → Platform-Wide Services → Connectivity → Components of SAP Communication Technology → Communication Between ABAP and Non-ABAP Technologies → Internet Communication Framework → Development → Server-Side Development → Creating and Configuring an ICF Service → Activating and Deactivating ICF Services.

For more information about ICF security, see SAP Help Portal at <http://help.sap.com> → SAP NetWeaver → <Release> → SAP NetWeaver Library → SAP NetWeaver by Key Capability → Security → SAP NetWeaver Security Guide Security Guides for Connectivity and Interoperability Technologies → RFC/ICF Security Guide.



Data Storage Security

Data Storage



In the default setting for SAP Portfolio and Project Management, data is protected using the ACL concept already described in [Authorizations](#). A Web browser is required for both scenarios. However, no cookies are used to store data on the front end.

Data Protection

In SAP Portfolio and Project Management, data is mainly stored on the SAP NetWeaver Application Server (SAP NetWeaver AS) database. An exception to this is when files are checked out for editing. In this case, files are stored locally on the user's hard drive and it is their responsibility to protect the files according to company security policy.

Depending on which installation scenario you have chosen for SAP Portfolio and Project Management, files might also be stored on content servers. For information about security measures to be taken in this case, see [Network Security](#).



Security for Additional Applications

SAP Portfolio and Project Management

You can only (import or) export data to Microsoft Project if you have the required authorizations, see *Access Control Lists – Import and Export*. The protection of this downloaded data is not part of the Project Management security model. When the user saves the project to his or her hard drive, the system does not perform an authorization check if somebody else opens the project again in Microsoft Project.

For more information, see [Other Security-Relevant Information – Microsoft Project Integration](#).



Dispensable Functions with Impacts on Security

Use

Portfolio and Project Management

The minimal installation for Project Management is [Scenario A: No Content Server](#)

- Adobe Document Services: see the *Preparing Printing* section of the *Basic Settings for Project Management*
- Microsoft Project integration: see Customizing for *SAP Portfolio and Project Management* under *Common Functions* → *Import and Export of Project Data* → *Microsoft Project Integration* → *Assign Fields for Import to Project Management*.
- Object links: See the *Preparing Object Links to Other Systems* section and the *Setting Up Object Links* section of the *Basic Settings for Project Management* in SAP Solution Manager.
- RFC access. For more information, see section *Communication Destinations*. To allow a user to access these functions it is necessary to assign the authorization object S_RFC in his or her user profile. To allow a user to access these functions, you have to assign the authorization object S_RFC to the user profile.
- HTTP-Based Document Management: see the *Activating HTTP-Based Document Management* of the *Basic Settings for Project Management* and the *Basic Settings for Portfolio Management* in SAP Solution Manager.

Project Management

- CATS integration: see the *Distributing SAP HR Master Data via ALE to Project Management* section of the configuration documentation for *Resource and Time Management with Project Management* business process in SAP Solution Manager.
- WFM Core integration: see the *Connecting Workforce Management Core* section of the configuration documentation for the *Resource and Time Management with Project Management* business process in SAP Solution Manager
- cFolders integration: see the *Preparing Integration with cFolders* section of configuration documentation for the *Project Execution with Project Management* business process in SAP Solution Manager.
- Accounting integration: see the *Defining Settings for Accounting Integration* section of the configuration documentation for the *Project Accounting with Project Management* business process in SAP Solution Manager
- SRM Integration: see the *Preparing Integration with Supplier Relationship Management* section of the *Basic Settings for Project Management* in SAP Solution Manager.
- Portfolio Management Integration: see the *Making Settings for Portfolio Management Integration* section of the *Basic Settings for Project Management* in SAP Solution Manager.

Portfolio Management

You can activate the following optional functions:

- Project Management integration
- SAP PLM PS integration
- Financial and Controlling (FI/CO) integration
- KM document management
- SAP HR integration: This integration is only relevant in context with Project Management

For more information with regards to the minimal installation, see the *SAP Portfolio and Project Management 5.0 Master Guide* on SAP Service Marketplace at service.sap.com/instguides → *Installation & Upgrade Guides* -> *SAP PLM* -> using *SAP Portfolio and Project Management 5.0*.



Other Security-Relevant Information

Documents (including Virus Scanner)

SAP Portfolio and Project Management uses standard SAP NetWeaver (NetWeaver) technology for uploading and downloading documents (Web Dynpro ABAP controls, Internet Communication Framework (ICF) services, and so on). These documents are checked into the defined storage system (content repository) using the Knowledge Provider (KPro).

Using the standard NetWeaver technology, you can use the standard NetWeaver virus scan interface (VSI) to check documents (including attachments) for viruses. To do this, you must have installed and configured a virus scanner. It is highly recommended to integrate a virus scanner. SAP Portfolio and Project Management uses the standard scan profile /SCMS/KPRO_CREATE (see SAP Note 1764839). For more information, see SAP Help Portal at <http://help.sap.com> → *NetWeaver* → *<Release>* → *SAP NetWeaver Library* → *SAP NetWeaver by Key Capability* → *Security* → *SAP NetWeaver Security Guide* → *Security Guides for SAP NetWeaver According to Usage Types* → *SAP NetWeaver Application Server ABAP Security Guide* → *Security Issues for Web Dynpro ABAP* → *Virus Scan Interface*.

Portfolio Management

For more information about security with regards to Knowledge Management, see SAP Service Marketplace at service.sap.com/securityguide → *SAP Knowledge Management Security Guides*.

Activating HTTP-Based Document Management

For more information about the prerequisites, see [Definition of Security Lists for OfficeControls](#). SAP Portfolio and Project Management supports HTTP-based check-in and check-out of documents. Therefore, OfficeControl UI elements for the check-in and check-out of documents are used. For more information, see the *Definition of Security Lists* for OfficeControls section of the *Basic Settings for Project Management* in SAP Solution Manager.

You can activate the HTTP-based document management in Customizing for *SAP Portfolio and Project Management* under *Portfolio Management* → *Global Customizing* → *Global Settings* → *Override Default Global Settings*. For more information, see the *Activating HTTP-Based Document Management* section of the *Basic Settings* for Project Management in SAP Solution Manager.

To use the HTTP-based check-in and check-out of documents, every user needs to install a Java runtime on his client PC. For more information about the required Java version, see SAP Note 1402912.

Export to PDF and MS Excel

- The Project Management and the Portfolio Management user interface (UI) uses standard NetWeaver Web Dynpro ABAP UI technology including the ABAP list viewer (ALV) control, which allows exporting into the following document types:
 - Portable document format (PDF)
 - MS Excel export
- Additionally, Project Management can export evaluation data to MS Excel using the standard Web Dynpro service.

For more information about security with regards to SAP NetWeaver, see SAP Service Marketplace at service.sap.com/securityguide → *SAP NetWeaver 7.0 Security Guides (Complete)*.

For more information about *Security Issues in Web Dynpro for ABAP*, see SAP Help Portal at <http://help.sap.com> → *NetWeaver* → *<Release>* → *SAP NetWeaver Library* → *SAP NetWeaver by Key Capability* → *Security* → *SAP NetWeaver Security Guide* → *Security Guides for SAP NetWeaver According to Usage Types* → *Security Aspects for Usage Type DI and Other Development Technologies*.

Definition of Security Lists for OfficeControls

SAP Portfolio and Project Management uses OfficeControls for the integration with Microsoft Project and for the HTTP-based check-in and check-out of documents. Since rendered pages are normally displayed in a Web browser connected to the Internet in Web Dynpro, security aspects, such as OfficeControls, must be considered for UI elements.

Therefore, the following security measures have been implemented for OfficeControl:

- OfficeControl communicates only with authorized servers
- Data can be stored only in authorized directories
- Data can be read only from authorized directories
- Only authorized file types can be opened directly with the default application

The authorized servers and directories and the authorized file types are listed in a whitelist for security reasons; an administrator stores this information locally using transactions WDR_ACF_WLIST and ACF_WHITELIST_SETUP. If requests for access to directories or communication with servers are sent using HTTP or HTTPS, the control first checks whether this is allowed at all. It then compares the directories or servers in question with the data in the local whitelist file. It executes the relevant methods only if the authorization is set in the whitelist.

Whitelist certificates can be generated using transaction WDR_ACF_GEN_CERT and need to be installed on all end user PCs. To install the whitelist certificate, go to transaction ACF_WHITELIST_SETUP and choose *Install Certificate*.

For more information, see Customizing for SAP NetWeaver under → *Application Server* → *Web Dynpro ABAP* → *Set Up Whitelist for Active Controls* and *Activate Whitelist for Active Controls*.

For more information about the required Java version for the OfficeControl, see SAP Note 1402912.

MS Project Integration

The *Import* and *Export* UI in both Project Management and Portfolio Management uses the OfficeControl UI element for Microsoft Office Project Integration. For more information, see the *Definition of Security Lists for OfficeControls* section of the *Basic Settings for Project Management* in SAP Solution Manager.

Import and export from or to MS Project is only supported when either Internet Explorer or NWBC for Desktop (with browser rendering from Internet Explorer) are used. It is not supported for Firefox, for example. For supported browsers, see SAP Note 1402912.

The Web Dynpro ABAP OfficeControl uses an ActiveX that does not access any resources on the front end, other than via the MS Project application. The ActiveX is digitally signed with the official SAP signature. With the intact official signature, SAP guarantees that the ActiveX, as provided, has not been changed or modified in any way.



The ActiveX must be installed once only, the first time you use the integration of Microsoft Project. This occurs automatically in the Internet Explorer. Subsequent calls to the integration then reuse the installed ActiveX. However, you can activate or deactivate the download and execution of ActiveX components in the standard Internet Explorer browser settings (local front-end settings). If you cannot use ActiveX, for example, due to company policy, you cannot use the Microsoft Project integration.

For more information about OfficeControl, see SAP Help Portal at <http://help.sap.com> → *SAP NetWeaver* → *<Release>* → *SAP NetWeaver Library* → *SAP NetWeaver by Key Capability* → *ABAP Technology* → *UI Technology* → *Web UI Technology* → *Web Dynpro ABAP* → *Reference* → *User Interface Elements*.

Gantt Chart

In the graphical view in Project Management, the timeline monitor and portfolio structure graphic in Portfolio Management, the Web Dynpro ABAP Gantt chart control is used, which uses a JAVA applet. For the supported Java versions, see SAP Note 1402912.

Import from Microsoft Excel

You can import projects from a Microsoft Excel file to Project Management. This enables you to transfer mass data in a quick and easy manner.

If you want to restrict the import function, you have to make sure that only allowed users receive authorization for transaction DPR_DX_PROJECT and report DPR_DX_PROJECT.

Moreover, you can import financial and/or capacity data from a Microsoft Excel file to financial and capacity planning in Portfolio Management. To use this function, you require an ERP system, an appropriate client, user, and password. This import is only allowed if the required authorization has been granted.



Security-Relevant Logging and Tracing

Use

Floorplan Manager Message Logging to the Application Log

The Web Dynpro ABAP UI of SAP Portfolio and Project Management 5.0 uses the Floor Plan Manager (FPM). The FPM Message Manager has a connection to the ABAP application log and offers the option to write error messages occurring in the FPM Message Manager also to the application log in the backend. To activate this feature, go to transaction SAAB and activate the check point group FPM_RUNTIME_MESSAGES for your user or for all users in the server.

For more information about FPM, see <http://www.sdn.sap.com/irj/sdn/nw-ui> -> Custom UI Development -> Web Dynpro ABAP -> Floorplan Manager (FPM) -> Developer's Guide.

For more information about security in the ABAP area, see SAP Help Portal at:

- <http://help.sap.com> → NetWeaver → <Release> → SAP NetWeaver Library → SAP NetWeaver by Key Capability → Security → SAP NetWeaver Security Guide → SAP NetWeaver Application Server ABAP Security Guide.
- <http://help.sap.com> → NetWeaver → <Release> → SAP NetWeaver Library → SAP NetWeaver by Key Capability → Application Platform by Key Capability → ABAP Technology → Web UI Technology → Web Dynpro ABAP → Security Issues for Web Dynpro ABAP.

Reports Logging to the Application Log

SAP Portfolio and Project Management 5.0 logs application errors for background reports to transaction SLG1. Background reports are executed in the areas of financial integration, migration, import from Microsoft Excel, versioning, and replace user and resource. You can display these application logs via the objects RPM_DOCUMENT, RPM_DX, RPM_INTEGRATION, RPM_MIGRATION, RPM_PLANNING, RPM_UC, RPM_VERSIONING, DPR_DX, DPR_REPLACE_USER_BP.

Logon Attempts

For more information about logon attempts, see SAP Help Portal at <http://help.sap.com> → NetWeaver → <Release> → SAP NetWeaver Library → SAP NetWeaver by Key Capability → Security → SAP NetWeaver Security Guide → Auditing and Logging → The Security Audit Log.

Change Document

You can use change document to track changes of objects of Project Management and Portfolio Management. If the function is active, the system also records changes to dependent objects. You can activate the change document function for the following objects:

- **Project Management**
 - Checklist templates
 - Project templates
 - Projects
 - Control plans
 - Control plan templates

You can activate this function in Customizing for *Project Management* under *Basic Settings* → *Activate Change Documents*.

If the function is active for one of these main objects, changes to dependent objects are also recorded. For example, if you select the indicator for the object category project, the system records all changes to the project as well as to the following objects:

- Project definitions
- Phases
- Tasks
- Mirrored tasks
- Checklists
- Checklist items
- Documents
- Object links
- Entity links
- Control plans
- Business partner favorites
- Business partner links
- Roles
- Approvals
- Qualifications
- Collaborations
- Templates

The system only records changes to database table DPR_DOCUMENT. This table contains unusable document attributes only.

The important attributes of the documents and files (such as name, location, and size) as well as the file content are saved to the KPro storage system without the support of a change document function.

Project Management supports versioning for files instead of the change document function. To track the changes, the user must always create a new document version. However, if he or she always overwrites the existing version, it is not possible to track the changes.

Project Management supports evaluations for the following objects:

- Project definitions
- Phases
- Tasks
- Mirrored tasks
- Checklists
- Checklist items
- Object links
- Entity links
- Business partner links
- Roles

- **Portfolio Management**

- Portfolio
- Bucket
- Initiative
- Item
- Decision point
- Review
- Collection
- What-if scenario
- Relational associations of business objects
- Financial and capacity category for bucket and item

In the standard system, this function is not activated.

You can activate this function in Customizing for *Portfolio Management* under *Global Customizing* → *Process and Service Settings* → *Activate Change Document*.

The system does not record changes to the following objects:

- **Project Management**

- Documents

- **Portfolio Management**

- Long texts
- Comments/notes
- Documents
- Financial and capacity planning values

Use

For more information, see SAP Help Portal at <http://help.sap.com> → *NetWeaver* → *<Release>* → *SAP NetWeaver Library* → *SAP NetWeaver Security Guide* →

- *Security Aspects for System Management* → *Auditing and Logging*.
- *Security Guides for SAP NetWeaver According to Usage Types* → *Security Guide for Usage Type AS* → *SAP NetWeaver Application Server Java Security Guide* → *Tracing and Logging*.



Services for Security Lifecycle Management

The following services are available from Active Global Support to assist you in maintaining security in your SAP systems on an ongoing basis.

Security Chapter in the EarlyWatch Alert (EWA) Report

This service regularly monitors the Security chapter in the EarlyWatch Alert report of your system. It tells you:

- Whether SAP Security Notes have been identified as missing on your system.
In this case, analyze and implement the identified SAP Notes if possible. If you cannot implement the SAP Notes, the report should be able to help you decide on how to handle the individual cases.
- Whether an accumulation of critical basis authorizations has been identified.
In this case, verify whether the accumulation of critical basis authorizations is okay for your system. If not, correct the situation. If you consider the situation okay, you should still check for any significant changes compared to former EWA reports.
- Whether standard users with default passwords have been identified on your system.
In this case, change the corresponding passwords to non-default values.

Security Optimization Service (SOS)

The Security Optimization Service can be used for a more thorough security analysis of your system, including:

- Critical authorizations in detail
- Security-relevant configuration parameters
- Critical users
- Missing security patches.

This service is available as a self-service within SAP Solution Manager, as a remote service, or as an on-site service. We recommend you use it regularly (for example, once a year) and in particular after significant system changes or in preparation for a system audit.

Security Configuration Validation

The Security Configuration Validation can be used to continuously monitor a system landscape for compliance with predefined settings, for example, from your company-specific SAP Security Policy. This primarily covers configuration parameters, but it also covers critical security properties like the existence of a non-trivial Gateway configuration or making sure standard users do not have default passwords.

Security in the RunSAP Methodology / Secure Operations Standard

With the E2E Solution Operations Standard Security service, a best practice recommendation is available on how to operate SAP systems and landscapes in a secure manner. It guides you through the most important security operation areas and links to detailed security information from SAP's knowledge base wherever appropriate.

More Information

For more information about these services, see:

- EarlyWatch Alert: <http://service.sap.com/ewa>
- Security Optimization Service / Security Notes Report:
<http://service.sap.com/sos>
- Comprehensive list of Security Notes:
<http://service.sap.com/securitynotes>
- Configuration Validation: <http://service.sap.com/changecontrol>
- RunSAP Roadmap, including the Security and the Secure Operations Standard:
<http://service.sap.com/runsap> (See the RunSAP chapters 2.6.3, 3.6.3 and 5.6.3)



Appendix

For more information, see SAP Note 1377104 (FAQs - SAP Portfolio and Project Management 5.0).