Component Security Guide for SAP EWM 7.0 Including SAP Enhancement Package 1



SCMEWM_SECGUIDE

Release 2010

Copyright

© Copyright 2010 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 is a registered trademark of Oracle Corporation.

UNIX, X/Open, OSF/1, and Motif are registered trademarks of the Open Group.

Citrix, ICA, Program Neighborhood, MetaFrame, WinFrame, VideoFrame, and MultiWin are trademarks or registered trademarks of Citrix Systems, Inc.

HTML, XML, XHTML and W3C are trademarks or registered trademarks of W3C®, World Wide Web Consortium, Massachusetts Institute of Technology.

Java is a registered trademark of Sun Microsystems, Inc.

JavaScript is a registered trademark of Sun Microsystems, Inc., used under license for technology invented and implemented by Netscape.

SAP, R/3, SAP NetWeaver, Duet, PartnerEdge, ByDesign, Clear Enterprise, SAP BusinessObjects Explorer 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 SAP France in the United States and in other countries.

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

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
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`.

Component Security Guide for SAP EWM 7.0 Including SAP Enhancement Package 1 6
Document History 6
Introduction 7
Before You Start 10
Technical System Landscape 14
Security Aspects of Data, Data Flow and Processes 14
User Administration and Authentication 15
User Management 15
User Data Synchronization 19
Integration into Single Sign-On Environments 20
Authorizations 21
Authorization Objects 22
Maintaining Authorizations 23
Maintaining Authorizations for Integration with SAP Components 23
Maintaining Authorizations for Enterprise Services 24
Session Security Protection 24
Network and Communication Security 25
Communication Channel Security 25
Network Security 27
Communication Destinations 28
Internet Communication Framework Security 30
Data Storage Security 30
Security for Additional Applications 33
Enterprise Services Security 34
Minimal Installation 34
Other Security-Relevant Information 34
User Frontend 35
Data Protection and Privacy 35
Security-Relevant Logging and Tracing 36
Services for Security Lifecycle Management 38
Virus Check of Document Attachments 40
Appendix 40

Component Security Guide for SAP EWM 7.0 Including SAP Enhancement Package 1

Document History

Before you start the implementation, make sure you have the latest version of this document. You can find the latest version at the following location: **`http://service.sap.com/securityguide`**.

The following table provides an overview of the most important document changes.

Date	Topic	Description of Change
September 2010 Context 7010	Overall	Minor adjustments based on feedback.
July 2010 Context 7010	*Security Guide Template* Section *About This Template*	Draft version for SAP Business Suite. Included recommendations about using clickable links or full paths for references. Updated contact information in the *Once You Have Finished* section.
	History of Changes	New topic Note: There is no history of changes for changes made prior to July 2010.
	Introduction Section *About this Document*	Adjusted the overview to include the new topics.
	Before You Start	Rearranged the table columns for *Important SAP Notes* and provided additional recommendations for filling out the table. Included a reference to available CTC templates.
	Security Aspects of Data, Data Flow and Processes	New topic
	Example: Security Aspects of Data, Data Flow and Processes	New topic
	User Management	Improved the instructions for describing the user types.
	Integration into Single Sign-On Environments	Changed the standard text to instruction text. This make it much easier for applications

		that run on SAP NetWeaver and use the standard SAP NetWeaver authentication and single sign-on mechanisms.
	Authorizations	Improved instructions about when to include specific authorizations, authorization objects, and the corresponding field values in the topic. Introduced a section for describing the role or authorization concept in general.
	Session Security Protection	New topic
	Communication Channel Security	Included additional examples.
	Network Security	Adjusted the instructions and standard text to make it easier for applications that run on AS ABAP or AS Java-based systems and use the standard ports.
	Communication Destinations	Included the instruction not to use SAP_ALL as the minimum authorization for communication users.
	Internet Communication Framework Security	New topic (relevant for AS ABAP only)
	Data Storage Security	Minor adjustments mainly to emphasize document security and deleting personal data due to data protection laws.
	Enterprise Services Security	Adjusted links to use for applications that run on AS ABAP or AS Java-based systems.
	Security Logging and Tracing	Minor adjustments to emphasize deleting personal data due to data protection laws.
	Services for Security Lifecycle Management	New topic

Introduction



This guide does not replace the administration or operation guides that are available for 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, the 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, reductions in processing time. These demands on security apply likewise to the SAP Extended Warehouse Management (SAP EWM) component. To assist you in securing your SAP EWM component, we provide this SAP EWM Component Security Guide.



SAP strongly recommends that you also consult the SAP NetWeaver Security Guide, in addition.

About This Guide

This Security Guide provides an overview of the security-relevant information that applies to the SAP EWM 7.0 including SAP enhancement package 1 component. It covers the following parts of the component:

- SAP EWM 7.0 Server including SAP enhancement package 1
  - SAP NetWeaver 7.0 BI CONT ADDON 7.05 (only used and required for analytics in SAP EWM)
- Third party software: PTV eServer for SAP SCM 7.0 including SAP enhancement package 1

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 the SAP EWM component.

- **Security Aspects of Data. Data Flow and Processes**

  This section provides an overview of the security aspects involved throughout the most widely-used processes within the SAP EWM component.

- **User Administration and Authentication**

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

- Recommended tools to use for user management
- User types that are required by the SAP EWM component
- Standard users that are delivered with the SAP EWM component
- Overview of the user synchronization strategy, if several components or products are involved
- Overview of how integration into Single Sign-On environments is possible

- **Authorizations**

  This section provides an overview of the authorization concept that applies to the SAP EWM component.

- **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 the SAP EWM component, 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 the SAP EWM component.

- **Data Storage Security**

  This section provides an overview of any critical data that is used by the SAP EWM component 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 the SAP EWM component.

- **Minimal Installation**

  This section provides information on the minimal installation of SAP EWM.

- **Enterprise Services Security**

  This section provides an overview of the security aspects that apply to the enterprise services delivered with SAP EWM.

- **Other Security-Relevant Information**

  This section provides information on the following:

  - Web browser as a user frontend
  - RF device as user frontend
  - Data protection and privacy

- **Security-Relevant Logging and Tracing**

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

- **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.

- **Virus Check of Document Attachments**

  This section provides information on the virus check functionality of SAP EWM.

- **Appendix**

  This section provides references to further information.



Before You Start

Fundamental Security Guides and Documentation

This Component Security Guide often provides references to other documentation. You can find this security-relevant documentation for the SAP Extended Warehouse Management (SAP EWM) component as follows:

Fundamental Security Guides and Documentation

Guide/Documentation	Path to the Guide/Documentation
SAP NetWeaver Security Guide	**`http://service.sap.com`** → *SAP NetWeaver Security Guides 7.0 (Complete)*
SAP NetWeaver Documentation	**`http://help.sap.com`** → *SAP NetWeaver* → *SAP NetWeaver 7.0 Including EHP1* → *SAP NetWeaver 7.0 Library* → *SAP NetWeaver Library* → *SAP NetWeaver by Key Capability*
SAP EWM Master Guide	**`http://service.sap.com/instguides`** → *Installation & Upgrade Guides* → *SAP Business Suite Applications* → *SAP SCM* → *SAP EWM* → *Using SAP EWM 7.0* → *Master Guide for SAP EWM 7.0* The SAP EWM component is built on further components and/or uses further components. Therefore, the corresponding Security Guides also apply to SAP EWM. The Master guide contains more information regarding the components necessary for business scenarios and processes.
SAP EWM Documentation	**`http://help.sap.com`** →*SAP Business Suite* → *SAP Supply Chain Management* → *SAP Extended Warehouse Management*
SAP EWM Installation Note	SAP Note 1173386 *Installation/Upgrade from SCMEWM 7.0 to ERP 6.0 EHP4*

Related Security Guides

The following table provides an overview of all related security guides for this component. For the Security Guides mentioned below, see SAP Help Portal at **`http://service.sap.com/securityguide`** → *SAP NetWeaver Security Guides 7.0 (Complete)*.

Related Security Guides for SAP NetWeaver Products

Product	See
Operating System and Database Platforms	*Security Guides for Operating System and Database Platforms*
SAP NetWeaver Application Server	*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* • *Security Settings for the SAP Message Server* • *SAP Interactive Forms by Adobe Security Guide* • *SAP Knowledge Warehouse Security Guide* • *Composite Application Framework Core Security Guide* • *Virus Protection and SAP GUI Integrity Checks* • *SAP Web AS with Integrated ITS*
EP Core (EPC) and Enterprise Portal (EP)	*Security Guides for Usage Types EPC and EP*
SAP NetWeaver Business Intelligence (SAP NetWeaver BI)	*Security Guide for Usage Type BI*
SAP NetWeaver Development Infrastructure (NWDI) and other development technologies	*Security Aspects for Usage Type DI and Other Development Technologies*
Mobile Infrastructure (MI)	*Security Guide for Usage Type MI*
Process Integration (PI)	*Security Guide for Usage Type PI*
Security Guides for Standalone Engines, Clients and Tools	• *Search and Classification (TREX) Security Guide* • *SAP Content Server Security Guide* • *Security Aspects for the SAP Web Dispatcher*

Connectivity and Interoperability	*Security Guides for Connectivity and Interoperability*, for example: • *Security Guide RFC / ICF* • *Security Guide for Connectivity with the J2EE Engine* • *Web Services Security*
System Management	*Security Aspects for System Management*, for example: • *Security Guide for the Solution Manager Diagnostics* • *Security Guide for the SAP System Landscape Directory* • *Software Lifecycle Manager (SLM)* • *Auditing and Logging*
SAP NetWeaver Scenarios	*Security Guides for the SAP NetWeaver Scenarios*, for example: • *Running an Enterprise Portal: Security Aspects* • *Enabling Application-to-Application Processes: Security Aspects* • *Enabling Business-to-Business Processes: Security Aspects*

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 the SAP EWM component are shown in the following table.

SAP Note	Title	Comment
25591	Database user passwords	The SAP R3 user password is to be changed.
30724	Data protection and security in SAP systems	
110600	SAP Security Library (SAPSECULIB)	
128447	Setting up Trusted/Trusting System relationship between two SAP systems	Needed for Customizing of trusted/trusting system RFC connections.
138498	Single Sign-On Solutions	Information about Single Sign-On solutions for SAP systems
389220	Certificate request reply cannot be inserted	
447543	APO: Authorizations too	

	comprehensive/not user-specific	
510007	Setting Up SSL on the Web Application Server	
616555	LiveCache password changes	The passwords of the standard liveCache user, the database system administrator, the DBM user, should be changed in the liveCache environment.
637052	Missing authorization object for database views	
662340	SSF Encryption Using the SAPCrytolib	The SAP Cryptographic Library has to be used for encrypting data in the SAP system.
683528	Security gaps in SAP DB	This note provides information about the secure operation of SAP DB/MaxDB and liveCache.
727839	Authorization role for the SAP SCM - SAP R/3 integration	
792366	Subsequent implementation of a security level for documents	Knowledge Provider: what needs to be taken into account, application of the Knowledge Provider (KPro) decides to change the security level for documents for one or more of their PHIO classes.
1320500	Installing or upgrading SCMEWM 7.01 to ERP 6.0 EHP5	
1517416	Collective security note for SAP EWM	This note contains additional security-relevant information and notes for SAP EWM.
1515223	SAP NetWeaver Process Integration: Release Recommendation	This note sets out our recommendation on which release of SAP NetWeaver PI you should use.



For a list of additional security-relevant SAP Hot News and SAP Notes, see also SAP Service Marketplace at:

- **`http://service.sap.com/securitynotes`**
- **`http://service.sap.com/security`** → *SAP NetWeaver* → *SAP NetWeaver in Detail* → *Security* → *SAP Security Notes*.

Additional Information

For more information about specific topics, see the addresses on SAP Service Marketplace as shown in the following table.

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 Net Weaver	**http://sdn.sap.com/irj/sdn/netweaver**



Technical System Landscape

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

Topic	Guide/Tool	Quick Link to SAP Service Marketplace
Technical System Landscape	SAP Extended Warehouse Management (SAP EWM) Master Guide	**http://service.sap.com/instguides** → *Installation & Upgrade Guides* → *SAP Business Suite Applications* → *SAP SCM* → *SAP EWM* → *Using SAP EWM 7.0 including SAP enhancement package 1* → *Master Guide for SAP EWM 7.0 including SAP enhancement package 1*
Technical System Landscape & Installation	SAP SCM Installation Guide(s)	**http://service.sap.com/instguides** → *Installation & Upgrade Guides* → *SAP Business Suite Applications* → *SAP SCM* → *SAP SCM Server* → *Using SAP SCM 7.0 Server including SAP enhancement package 1* → *Installation Documentation - SAP SCM 7.0 including SAP enhancement package 1*
Technical Configuration, High Availability	Technical Infrastructure Guide	**http://service.sap.com/installnw70**
Security	Security Guide	**http://service.sap.com/security**



Security Aspects of Data, Data Flow and Processes

SAP EWM can be installed, distributed and used in multiple different scenarios. This is described in Technical System Landscape [Page 14].

The following table describes some typical processes and communication channels, along with appropriate security measures:

Process	Security Measure
EWM receives data from ERP (such as deliveries and master data) and sends data to ERP (such as	Ensure appropriate user authorizations. For more information, see

confirmations and stock updates). This is typically done using standard qRFC/RFC technology.	Communication Channel Security for SAP EWM [Page 25].
Mobile devices can be connected using HTTP/ITS mobile (it is also possible to use the SAP console). This is done based on the Internet Communication Framework (ICF) service for RFUI.	For details, see Internet Communication Framework Security [Page 30].
For certain scenarios, such as connecting automated physical processes (for example, conveyor systems) via SAP Plant Connectivity, RFCs are used. Depending on the scenario, IDOCs may also be used (for example, when warehouse control units are used).	
SAP EWM offers the possibility for upload and download of data. In many of these transactions it is possible to either choose a local file system (PC) or files on the application server.	Ensure that only a few people can access these transactions, and that access to the application server file system is restricted. You should design logical paths and filenames to restrict the access. For more information, see Data Storage Security for SAP EWM [Page 30].

User Administration and Authentication

The SAP Extended Warehouse Management (SAP EWM) component uses the user management and authentication mechanisms provided with the SAP NetWeaver platform, in particular the SAP NetWeaver Application Server ABAP. Therefore, the security recommendations and guidelines for user administration and authentication as described in the SAP NetWeaver Application Server ABAP Security Guide [External] also apply to the SAP EWM component.

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

- User Management [Page 15]

  This topic lists the tools to use for user management, the types of users required, and the standard users that are delivered with the SAP EWM component.

- User Data Synchronization [Page 19]

  The SAP EWM component shares user data with SAP NetWeaver 7.0. This topic describes how the user data is synchronized with these other sources.

- Integration into Single Sign-On Environments [Page 20]

  This topic describes how the SAP EWM component supports Single Sign-On mechanisms.

User Management

Use

User management for the SAP Extended Warehouse Management (SAP EWM) component uses the mechanisms provided with the SAP NetWeaver Application Server ABAP, for example, tools, user types, and password policies. For an overview of how these mechanisms

apply to the SAP EWM component, see the sections below. In addition, we provide a list of the standard users required for operating the SAP EWM component.



For an overview of the information necessary for securing operations with SAP NetWeaver Identity Management, see the Security Guide on SAP Help Portal at **`http://help.sap.com/nw71`** → *SAP NetWeaver Identity Management 7.1*.

User Administration Tools

The following table shows the tools needed for user management and user administration with the SAP EWM component.

User Management Tools

Tool	Detailed Description
User Management for the ABAP Engine (transaction SU01)	Use the user management transaction SU01 to maintain users in ABAP-based systems.
Profile Generator (transaction PFCG)	Use the Profile Generator to create roles and assign authorizations to users in ABAP-based systems.
Central User Administration (CUA)	Use the CUA to centrally maintain users for multiple ABAP-based systems. Synchronization with a directory server is also supported.
User Management Engine (UME) administration console	Use the Web-based UME administration console to maintain users, roles and authorizations in Java-based systems that use the UME for the user store, for example, the SAP NetWeaver Application Server Java and the Enterprise Portal. The UME also supports various persistency options, such as the ABAP Engine or a directory server.
SAP NetWeaver Application Server Java user management using the Visual Administrator	Use the Visual Administrator to maintain users and roles on the SAP NetWeaver Application Server Java. SAP NetWeaver Application Server Java also supports a pluggable user store concept. The UME is the default user store.



For a detailed description of the user management tools available in SAP NetWeaver, see the SAP NetWeaver Security Guide on SAP Service Marketplace at **`http://service.sap.com/securityguide`** → *SAP NetWeaver 7.0 Security Guides (Complete)* → *SAP NetWeaver Security Guide* → *User Administration and Authentication* → *User Management* in the section *"User Management Tools"*.

User Types

It is often necessary to specify different security policies for different types of users. For example, your policy may specify that individual users who perform tasks interactively have to change their passwords on a regular basis, but the users under whom background processing jobs run do not.

For more information about these user types, see the SAP NetWeaver Application Server ABAP Security Guide on SAP Service Marketplace at

http://service.sap.com/securityguide → *SAP NetWeaver Security Guides 7.0 (Complete)* → *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* → *User Authentication* → *User Types*.

The user types required for SAP EWM include the following:

Users

System	User	Delivered ?	Type	Default Password	Detailed Description
SAP SCM 7.0 Server including SAP enhancement package 1	<sapsid>adm	Yes	SAP System Administrator	To be entered	**http://service.sap.com/instguides** → *Installation & Upgrade Guides* → *SAP Business Suite Applications* → *SAP SCM* → *SAP SCM Server* → *Using SAP SCM 7.0 Server* → *Installation Guides* → *Installation Documentation SAP SCM 7.0 including SAP enhancement package 1* → *Installation Guide - SAP SCM Server 7.0* <OS>:<DB>
SAP SCM 7.0 Server including SAP enhancement package 1	SAPService <sapsid>	Yes	SAP System Service Administrator	To be entered	**http://service.sap.com/instguides** → *Installation & Upgrade Guides* → *SAP Business Suite Applications* → *SAP SCM* → *SAP SCM Server* → *Using SAP SCM 7.0 Server* → *Installation Guides* → *Installation Documentation SAP SCM 7.0 including SAP enhancement package* → *Installation Guide - SAP SCM Server 7.0 including SAP enhancement package* <OS>:<DB>
SAP WebAS	SAP Standard ABAP Users (SAP*, DDIC, EARLYWATCH, SAPCPIC)	Yes	See SAP NetWeaver Security Guide	See SAP NetWeaver Security Guide	**http://service.sap.com/securityguide** → *SAP NetWeaver Security Guides 7.0 (Complete)* → *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* → *User Authentication* → *Protecting Standard Users*
SAP WebAS	SAP Standard J2EE Users (Admini	Yes	See SAP NetWeaver 7.0 Security Guide	See SAP NetWeaver 7.0 Security Guide	**http://service.sap.com/securityguide** → *SAP NetWeaver Security Guides 7.0 (Complete)* → *SAP NetWeaver Security Guide* → *Security Guides for SAP*

	strator, Guest, Emergency)				*NetWeaver According to Usage Types → Security Guide for Usage Type AS → SAP NetWeaver Application Server Java Security Guide → User Administration and Authentication → User Administration and Standard Users → Standard Users* and *Standard User Groups*
SAP J2EE Engine	SAPJSF	Yes	Communication user	To be entered	**http://service.sap.com/instguides** → *Installation & Upgrade Guides → SAP Business Suite Applications → SAP SCM → SAP SCM Server → Using SAP SCM 7.0 Server including SAP enhancement package → Installation Guides → Installation Documentation SAP SCM 7.0 including SAP enhancement package → Installation Guide - SAP SCM Server 7.0 including SAP enhancement package* <OS>:<DB>
SAP EWM 7.0 including SAP enhancement package 1	RFC communication users (you need an RFC communication user for each RFC destination described in section *Communication Destination*)	No	Communication user	The authorizations of the user depend on the business case. For more information, see Authorizations [Page 21] in this Security Guide.	Documentation for SAP EWM 7.0 including SAP enhancement package 1 under Communication Destinations [Page 28] and Authorizations [Page 21]
SAP EWM 7.0 including SAP enhancement	Business processing users (you need a	No	Dialog user	To be entered	Documentation for SAP EWM 7.0 including SAP enhancement package 1 under Authorizations [Page 21]

package 1	user in each component for each employee working with the system)				



For more information about user types, see the SAP NetWeaver Application Server ABAP Security Guide on SAP Service Marketplace at **`http://service.sap.com/securityguide`** → *SAP NetWeaver Security Guides 7.0 (Complete)* → *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*.

For more information about SAP NetWeaver standard users, see the SAP NetWeaver Application Server ABAP Security Guide on SAP Service Marketplace at **`http://service.sap.com/securityguide`** → *SAP NetWeaver Security Guides 7.0 (Complete)* → *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* → *User Authentication* → *Protecting Standard Users.*

For more information about SAP NetWeaver password rules, see SAP NetWeaver Application Server ABAP Security Guide on the SAP Service Marketplace at **`http://service.sap.com/securityguide`** → *SAP NetWeaver Security Guides 7.0 (Complete)* → *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* → *User Authentication* → *Authentication and Single Sign-On* → *Logon and Password Security in the SAP System* → *Password Rules.*



User Data Synchronization

Use

To save administrational effort, you can synchronize user data in your system landscape. As the SAP Extended Warehouse Management (SAP EWM) component is based on SAP NetWeaver 7.0, all the mechanisms for user data synchronization of SAP NetWeaver 7.0 are available for SAP EWM.



For information about user data synchronization, see the SAP NetWeaver Security Guide on SAP Service Marketplace at **`http://service.sap.com/securityguide`** → *SAP NetWeaver Security Guides 7.0 (Complete)* → *SAP NetWeaver Security Guide* → *User Administration and Authentication* → *Integration of User Management in Your System Landscape.*

Integration into Single Sign-On Environments

Use

The SAP Extended Warehouse Management (SAP EWM) component 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 Guides also apply to the SAP EWM component.



For more information about integration into Single Sign-On environments based on SAP NetWeaver, see the SAP NetWeaver Security Guide on SAP Service Marketplace at **`http://service.sap.com/securityguide`** → *SAP NetWeaver 7.0 Security Guides (Complete)* → *SAP NetWeaver 7.0 Security Guide* → *User Administration and Authentication* → *User Authentication and Single Sign-On* in the section *"Integration into Single Sign-On Environments".*

For more information about authentication on the SAP NetWeaver Application Server ABAP, see the SAP NetWeaver Security Guide on SAP Service Marketplace at **`http://service.sap.com/securityguide`** → *SAP NetWeaver 7.0 Security Guides (Complete)* → *SAP NetWeaver 7.0 Security Guide* → *Security Guides for SAP NetWeaver According to Usage Types* → *Security Guide for Usage Types AS* → *SAP NetWeaver Application Server ABAP Security Guide* → *User Authentication*.

The supported mechanisms are listed below.

Secure Network Communications (SNC)

SNC is available for user authentication and provides for an SSO environment when using the SAP GUI for Windows or Remote Function Calls.

For more information, see the SAP NetWeaver Security Guide on SAP Service Marketplace at **`http://service.sap.com/securityguide`** → *SAP NetWeaver 7.0 Security Guides (Complete)* → *SAP NetWeaver 7.0 Security Guide* → *SAP NetWeaver Security Guide* → *Network and Communication Security* → *Transport Layer Security* → *Secure Network Communications (SNC).*

SAP Logon Tickets

The SAP EWM component supports the use of logon tickets for SSO when using a Web browser as the frontend client. In this case, users can be issued a logon ticket after they have authenticated themselves with the initial SAP system. The ticket can then be submitted to other systems (SAP or external systems) as an authentication token. The user does not need to enter a user ID or password for authentication but can access the system directly after the system has checked the logon ticket.

For more information, see the SAP NetWeaver Security Guide on SAP Service Marketplace at **`http://service.sap.com/securityguide`** → *SAP NetWeaver 7.0 Security Guides (Complete)* → *SAP NetWeaver 7.0 Security Guide* → *SAP NetWeaver Security Guide* → *User Administration and Authentication* → *User Authentication and Single Sign-On.*

Client Certificates

As an alternative to user authentication by means of a user ID and passwords, users using a Web browser as a front-end client can also provide X.509 client certificates to use for authentication. In this case, user authentication is performed on the Web server using the Secure Sockets Layer Protocol (SSL Protocol) and no passwords have to be transferred. User authorizations are valid in accordance with the authorization concept in the SAP system.

For more information, see the SAP NetWeaver Security Guide on SAP Service Marketplace at **`http://service.sap.com/securityguide`** → *SAP NetWeaver 7.0 Security Guides*

(Complete) → SAP NetWeaver 7.0 Security Guide → SAP NetWeaver Security Guide → Security Guides for SAP NetWeaver According to Usage Types → SAP NetWeaver Application Server ABAP Security Guide → User Authentication → Authentication and Single Sign-On → Client Certificates.

Authorizations

The authorization concept of the SAP Extended Warehouse Mangement (SAP EWM) component is based on the authorization concept of SAP NetWeaver. This concept protects transactions and programs in SAP systems from unauthorized access. Based on the authorization concept, the administrator assigns authorizations to the users that determine which actions users can execute in the SAP system after they have logged on to the system and authenticated themselves.

To access business objects or execute SAP transactions, a user requires corresponding authorizations, since business objects or transactions are protected by authorization objects. The authorizations represent instances of generic authorization objects and are defined depending on the activity and responsibilities of the employee. The authorizations are combined in an authorization profile that is associated with a role. The user administrators then assign the corresponding roles using the user master record, so that users can use the appropriate transactions for their tasks.



For information about the authorization concept of SAP NetWeaver, see SAP Help Portal at **`http://help.sap.com`** → *SAP NetWeaver → SAP NetWeaver 7.0 Including EHP2 → SAP NetWeaver 7.0 Library → SAP NetWeaver Library → SAP NetWeaver by Key Capability → Security → Identity Management → User and Role Administration of AS ABAP → AS ABAP Authorization Concept* and *User and Role Administration of AS Java → Authorization Concept of the AS Java.*



We recommend that you use the role maintenance functions and the Profile Generator (transaction code PFCG) to maintain your roles, authorizations, and profiles. The role maintenance functions support you in performing your task, by automating various processes and allowing you more flexibility in your authorization plan. You can also use the central user administration functions to centrally maintain your own new roles or those provided by SAP, and to assign the roles to any number of users.

The roles you assign to your users define the user menu that is displayed after the users have logged on to the SAP system. Roles also contain the authorizations to allow users to access the transactions, reports, Web-based applications, and so on, that are contained in the menu.

For information about role maintenance and the Profile Generator, see SAP Help Portal at **`http://help.sap.com`** → *SAP NetWeaver → SAP NetWeaver 7.0 Including EHP2 → SAP NetWeaver 7.0 Library → SAP NetWeaver Library → SAP NetWeaver by Key Capability → Security → Identity Management → User and Role Administration of AS ABAP → AS ABAP Authorization Concept → Organizing Authorization Administration* in the section *Organization if You Are Using the Role Administration Tool*.

With the component SAP EWM, SAP delivers SAP standard roles to cover the most-used business cases. These roles can be used as examples, or as a copy master for your own roles.

You can find the SAP standard roles in the Profile Generator (transaction code `PFCG`) using input help. You can use search terms to restrict the selection to the required standard roles, for example, the search term */SCWM* lists all SAP EWM-relevant SAP standard roles. The role short text helps you find the role covering your business needs. The documentation of the role provides you with a detailed description of the role content.

Alternatively you can also use the transaction `SUIM` to find the PFCG roles for EWM. In transaction `SUIM`, choose *Roles* → *Roles by Complex Selection Criteria*. Then enter /SCWM/* in the *Role* field and execute.



We strongly recommend that you be very conservative (restrictive) in assigning the authorization profiles SAP_ALL and SAP_NEW to users in your production system! Too liberal a use of these profiles can seriously weaken the overall security concept in your production system.

Role and Authorization Concept for SAP EWM

Read-Only Access for Auditors

SAP EWM provides a role for read-only access for all data. For an audit, the auditor needs to be able to read all data. However, the auditor must not be allowed to change any data. This can be achieved by assigning the /SCWM/INFORMATION role to a user.

Standard Roles

For information about roles in SAP EWM, see Roles for Extended Warehouse Management (EWM) [External].

For information about users and roles in SAP NetWeaver, see SAP Help Portal at **`http://help.sap.com`** → *SAP NetWeaver* → *SAP NetWeaver 7.0 Including EHP2* → *SAP NetWeaver 7.0 Library* → *SAP NetWeaver Library* → *SAP NetWeaver by Key Capability* → *Security* → *Identity Management* → *User and Role Administration of AS ABAP* and *User Management of the Application Server Java.*



Authorization Objects

Use

A set of authorization objects is available in SAP Extended Warehouse Management.

Authorization objects enable you to define complex authorizations by grouping up to 10 authorization fields in an AND relationship to check whether a user is allowed to perform a certain action. To pass an authorization test for an object, the user must satisfy the authorization check for each field in the object.



For information about the authorization concept of SAP NetWeaver, see SAP Help Portal at **`http://help.sap.com`** → *SAP NetWeaver* → *SAP NetWeaver 7.0 Including EHP2* → *SAP NetWeaver 7.0 Library* → *SAP NetWeaver Library* → *SAP NetWeaver by Key Capability* → *Security* → *Identity Management* → *Users and Roles (BC-SEC-USR)* → *SAP Authorization Conce*pt.

Activities

To gain an overview of the authorization objects for SAP Extended Warehouse Management proceed as follows:

1. Call the transaction for displaying active authorization objects (AUTH_DISPLAY_OBJECTS).
2. In the overview, expand the *Authorizations Extended Warehouse Management* subtree.

   If you want to display the technical names of the authorization objects, choose *Edit* → *Technical names* → *Technical names on*.
3. If you want to get a detailed description, choose the *Information* pushbutton next to the authorization object you are interested in.

Maintaining Authorizations

Use

Using the SAP Extended Warehouse Management (SAP EWM) component, you can assign users to various standard user roles. For more information, see SAP Help Portal at **`http://help.sap.com`** → *SAP Business Suite* → *SAP Supply Chain Management* → *SAP Extended Warehouse Management (SAP EWM)* → *Roles for Extended Warehouse Management (EWM).*

If you want to display the authorization objects in SAP EWM, on the *SAP Easy Access* screen, choose *Tools* → *ABAP Workbench* → *Development* → *Other Tools* → *Authorization Objects* → *Objects.*

For more information, see SAP Help Portal at **`http://help.sap.com`** → *SAP Business Suite* → *SAP Supply Chain Management* → SAP *Extended Warehouse Management* → *General Functions* → *Authorizations in Extended Warehouse Management.*

Maintaining Authorizations for Integration with SAP Components

Procedure

Maintaining Authorizations for SAP Extended Warehouse Management (SAP EWM) – SAP ERP Integration

Using Standard Roles for SAP EWM – SAP ERP Integration

For the integration of SAP EWM and SAP ERP, use the authorization roles for the RFC destination users.



For more information about these roles, see SAP Help Portal at **`http://help.sap.com`** → *SAP Business Suite* → *SAP Supply Chain Management* → *SAP Extended Warehouse Management (SAP EWM)* → *Roles for Extended Warehouse Management (EWM)*.

Maintaining Authorizations for Data Transfer to SAP NetWeaver Business Intelligence

Limiting Authorizations for Extraction



You can exclude DataSources from the extraction to the SAP NetWeaver Business Intelligence (SAP BI). Data that is stored in the extraction structure of this DataSource cannot be transferred to SAP NetWeaver BI.

1. In Customizing for SAP EWM, choose *Integration with SAP Components* → *Data Transfer to the SAP Business Information Warehouse* → *General Settings* → *Limit Authorizations for Extraction*.
2. Choose *New Entries*.
3. Choose a DataSource that you want to exclude from the extraction.
4. Choose the SAP NetWeaver BI system for which you want no more data for this DataSource to be extracted.
5. In the *Excl. Extr.* field, enter whether or not you want to exclude the DataSource from the extraction.
6. Save your entries.
7. Specify a transport request.

Maintaining Authorizations for Enterprise Services

Use

Accessing SAP functions via Web services follows the standard SAP authorization concept. This concept is based on authorizations for specific authorization objects. The system checks for the required authorization for an authorization object during the execution of a Web service. If a user does not have this authorization, the execution is terminated, and an error message is returned.

Enterprise services use standard authorization objects that are available for SAP Extended Warehouse Manaegment (SAP EWM), including authorization default values for Web services. In addition, you need the authorization S_SERVICE to start external services. To create and consume Web services, you require the authorizations belonging to the role SAP_BC_WEBSERVICE_ADMIN as well as authorization for the Internet Communication Framework (S_ICF_ADMIN).

For more information about authorizations for Web services, see SAP Help Portal at **`http://help.sap.com`** → *SAP NetWeaver* → *SAP NetWeaver 7.0 Including EHP2* → *SAP NetWeaver 7.0 Library* → *SAP NetWeaver Library* → *SAP NetWeaver Developer's Guide* → *Fundamentals* → *Using Java* → *Core Development Tasks* → *Providing and Consuming Web Services* → *Web Service Toolset* → *Web Services Security* → *Authorization*.

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 Activating HTTP Security Session Management on AS ABAP [External] in the AS ABAP security documentation.

Network and Communication Security

Your network infrastructure is 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 back-end 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 the SAP Extended Warehouse Management (SAP EWM) component is based on the topology used by the SAP NetWeaver platform. Therefore, the security guidelines and recommendations described in the SAP NetWeaver Security Guide also apply to the SAP EWM component. Details that specifically apply to the SAP EWM component are described in the following topics:

- Communication Channel Security for SAP EWM [Page 25]

  This topic describes the communication paths and protocols used by the SAP EWM component.

- Network Security [Page 27]

  This topic describes the recommended network topology for the SAP EWM component. 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 the SAP EWM component.

- Communication Destinations [Page 28]

  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:

- Network and Communication Security [External]
- Security Guides for Connectivity and Interoperability Technologies [External]

Communication Channel Security

Since communication channels transfer all kinds of your business data, they should be protected against unauthorized access. SAP offers general recommendations and technologies to protect your system landscape, based on SAP NetWeaver.



You should activate the Secure Network Communication (SNC) within all communication channels in SAP EWM to achieve a secure system landscape.

For more information, see **`http://service.sap.com/security`** → *SAP NetWeaver 7.0 Security Guides (Complete)* → *SAP NetWeaver 7.0 Security Guide* → *Network and Communication Security* → *Transport Layer Security* → *Secure Network Communications (SNC)*.

For a detailed description of all communication channels within the SAP EWM component, see SAP Service Marketplace at **`http://service.sap.com/scm`** → *SAP SCM Technology* → *Architecture Overview*.



For more information about the communication security of SAP NetWeaver, see the SAP NetWeaver Security Guide on SAP Service Marketplace at **`http://service.sap.com/securityguide`** → *SAP NetWeaver 7.0 Security Guides (Complete)* → *SAP NetWeaver 7.0 Security Guide* → *Network and Communication Security*.

For more information about security aspects for connectivity and interoperability of SAP NetWeaver, see the SAP NetWeaver Security Guides on SAP Service Marketplace at **`service.sap.com/securityguide`** → *SAP NetWeaver 7.0 Connectivity Security Guides*.

The following table shows the communication channels used by SAP EWM, the protocol used for each connection, and the type of data transferred.

Communication Channel	Protocol Used	Type of Data Transferred
Front-end client that uses SAP GUI for Windows for the application server	DIAG	All application and customizing data
SAP ERP	RFC and /or IDOC	Master data and transaction data
SAP SCM	RFC	ATP data
SAP SCM	RFC	Master data
SAP GTS	RFC	GTS-relevant data
SAP BI	RFC	Data sources
SAP CRM	RFC and/or IDOC	Billing data, business partners
Warehouse Control Units or PLCs	RFC, IDOC (depending on whether or not SAP plant connectivity is used)	Transaction data
Legacy systems	RFC, IDOC, HTTP, File	Depends on legacy scenario

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 [External] in the SAP NetWeaver Security Guide.

Note that many of the entries depend on the configuration and how SAP EWM is used. For example, usage of SAP GTS, SAP BI, legacy systems and further components is optional and depends on how the system is used. Also if parts of underlying components (SAP SCM Basis, SAP Netweaver) are used they may also offer further communication channels.

For more detailed information about external messages that can be sent to and/or from SAP EWM, see the appendix of the EWM Application Operations Guide at **`http://service.sap.com/instguides`** → *Installation & Upgrade Guides* → *SAP Business Suite Applications* → *SAP SCM* → *SAP EWM* → *Using SAP enhancement package 1 for SAP EWM 7.0* → *Application Operations Guide*.

Core Interface (CIF) – SAP ERP

The integration of SAP EWM and SAP ERP is technically based on CIF. As CIF is technically based on the RFC provided by SAP NetWeaver, we strongly recommend that you consult the SAP NetWeaver Security Guide regarding communication channel security.

You should at least enable Secure Network Communication (SNC) while configuring the RFC destination for your SAP EWM - SAP ERP integration.



For more information about the integration of SAP EWM and SAP ERP, see SAP Help Portal at **`http://help.sap.com`** → *SAP Business Suite* → *SAP Supply Chain Management* → *SAP SCM 7.0 including SAP enhancement package 1*→ *SAP Advanced Planning and Optimization (SAP APO)* → *Integration via Core Interface (CIF)* → *Technical Integration*.

Network Security

Your network infrastructure is important in protecting your system. 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.

We offer general recommendations to protect your system landscape, based on SAP NetWeaver.



For information about network security for SAP NetWeaver, see Network and Communication Security [External].

A minimum security demand for your network infrastructure is the use of a firewall for all your services provided over the Internet.

A more secure variant is to protect your systems (or groups of systems) by locating the different "groups" in different network segments, each protected with a firewall against unauthorized access. External security attacks can also come from "inside", if the intruder has already taken over control of one of your systems.



For more information about the technical components of your SAP Extended Warehouse Management (SAP EWM) component, see SAP Service Marketplace at **`http://service.sap.com/scm`** → *SAP Supply Chain Management* → *SAP SCM Technology***.**

For more information about access control using firewalls, see Using Firewall Systems for Access Control [External].

Ports

SAP EWM runs on SAP NetWeaver and uses the ports from the AS ABAP. For more information, see the topic for AS ABAP Ports [External] 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*.

Communication Destinations

Use



If not implemented and used with care, users and authorizations for connection destinations can cause serious security flaws.

Follow the “Golden Rules” for connection users and authorizations, as follows:

- Choose user *type*: <system>.
- Assign only the minimum required authorizations to the user.
- Choose a secure and secret password for the user.
- Store only connection user log-on data for users of type “system“.
- Choose *trusted system* functionality whenever possible, rather than storing connection user log-on data.

The table below shows an overview of the communication destinations used by the SAP Extended Warehouse Management (SAP EWM) component:

Connection Destinations

Destination	Delivered	Type	User, Authorizations	Description
<EWM name>CLNT<client> EWM → SAP ERP	No	RFC - ERP	Use the Profile Generator (transaction code PFCG) to define an appropriate profile, and see SAP Notes 447543 and 727839.	For more information, see Customizing for SCM Basis under *Integration* → *Basic Settings for Creating the System Landscape* → *Assign RFC Destinations to Various Application Cases*.
EWM → SAP R/3 or SAP ERP	No	RFC – ERP (qRFC)	Use the Profile Generator (transaction code PFCG) to define an appropriate profile, and see SAP Notes 447543 and 727839.	For more information, see Customizing for SAP EWM under *Interfaces* → *ERP Integration* → *General Settings* → *Control for RFC Queue* **and** Customizing for SCM

				Basis under *Integration → Basic Settings for Creating the System Landscape → Assign RFC Destinations to Various Application Cases*.
EWM → SAP APO (APO instance)	No	RFC – ERP	Use the Profile Generator (transaction PFCG) to define an appropriate profile, and see SAP Notes 447543 and 727839.	For more information, see Customizing for SAP EWM under *Goods Receipt Process → Slotting → General Settings → Change Information for APO Instances.*
EWM → Non-SAP Systems	No	RFC – ERP	-	For more information, see Customizing for SAP EWM under *Interfaces → Non-SAP Systems → Connect Subsystem.*
EWM → SAP GTS	No	RFC –	-	For more information, see Customizing for SAP EWM *under Interfaces → GTS Integration → Basic Settings of GTS Integration*.
EWM → SAP Business Warehouse (BW)	No	RFC – ERP	-	For more information, see Customizing for SAP EWM under *Integration with SAP Components → Data Transfer to the SAP Business Information Warehouse* **and** Customizing for SAP EWM under *Interfaces → SAP Business Information Warehouse.*



For more information about communication destinations of SAP NetWeaver, see the SAP NetWeaver Security Guide on SAP Service Marketplace at **`http://service.sap.com/securityguide`** → *SAP NetWeaver 7.0 Security Guides (Complete) → SAP NetWeaver 7.0 Security Guide → Security Guides for Connectivity and Interoperability Technologies*.

Internet Communication Framework Security

You should only activate those services that are needed for the applications running in your system. For SAP EWM the following service is available:

- RFUI
  - Path: /default_host/sap/bc/gui/sap/its/scwm/rfui
  - This service can be used, for example, to allow warehouse workers to use transaction /SCWM/RFUI from mobile applications. The service can be accessed from the SAP console or by using ITS mobile. For more information, see Resource Management Using Radio Frequency [External].

Use the transaction `SICF` to activate this service.

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

For more information, see Activating and Deactivating ICF Services [External] in the SAP NetWeaver Library documentation.

For more information about ICF security, see the RFC/ICF Security Guide [External].

Data Storage Security

Data Storage

The data storage security of SAP NetWeaver and components installed on that database is described in detail in the SAP NetWeaver 7.0 Security Guide.

For more information about the data storage security of SAP NetWeaver, see the SAP NetWeaver Security Guide on SAP Service Marketplace at **`http://service.sap.com/securityguide`** → *SAP NetWeaver 7.0 Security Guides (Complete)* → *SAP NetWeaver 7.0 Security Guides* → *Security Guides for Operating System and Database Platforms*.

In general, all business data of the SAP EWM component is stored in the system database. If SAP liveCache is used, some business data is also stored there. This business data is protected by the authorization concept of SAP NetWeaver and SAP EWM.

In some special cases, business-relevant data is stored elsewhere (for example, in a file system).

Using Logical Path and Filenames to Protect Access to the File System

The SAP EWM component may save data in files in the file system and may read data from the file system. Therefore, it is important to explicitly provide access to the corresponding files in the file system without allowing access to other directories or files (also known as directory traversal). This is achieved by specifying logical paths and file names in the system that map to the physical paths and file names. This mapping is validated at runtime and if access is requested to a directory that does not match a stored mapping, then an error occurs.

In some cases fixed logical file names are also used in applications which cannot be changed.

The following lists show the logical filenames and paths used by SAP EWM and the programs to which they apply.

Logical Filenames and File Paths Used in SAP EWM

The following logical filenames have been created in order to enable the validation of physical filenames:

- EWM_PI_DOWNLOAD

  Transactions/programs using this logical filename:

  - Transaction /SCWM/PI_DOWNLOAD
  - Program /SCWM/R_PI_STOCK_DWNLD

  Parameters and format used in this context:

  - <PARAM_1> = Warehouse number (CHAR4)
  - <PARAM_2> = Counter (NUM2)

  Logical file path used:

  - EWM_GLOBAL_PATH

  Comment:
  The logical filename is fixed and cannot be changed. The logical file contains a physical filename. The logical file path contains a physical path. The validation and alias definition do not apply for this logical filename.

- EWM_PI_UPLOAD
  Transactions/programs using this logical filename:

  - Transaction /SCWM/PI_UPLOAD
  - Program /SCWM/R_PI_FILEUPLD

  Parameters and format used in this context:

  - <PARAM_1> = Warehouse number (CHAR4)
  - <PARAM_2> = Creation Date (DATS8)
  - <PARAM_3> = Counter (NUM2)

  Logical file path used:

  - EWM_GLOBAL_PATH

  Comment:
  The logical filename is fixed and cannot be changed. The logical file contains a physical filename. The logical file path contains a physical path. The validation and alias definition do not apply for this logical filename.

- EWM_STOCK_UPLOAD

  Transactions/programs using this logical filename:

  - Transaction /SCWM/ISU
  - Program /SCWM/R_INITIALSTOCKUPLOAD

  Parameters and format used in this context:

  - <PARAM_1> = Warehouse number (CHAR4)

  Logical file ath used:

- EWM_STOCK_UPLOAD_PATH

- EWM_STOBIN_UPLOAD

  Transactions/programs using this logical filename:

  - Transaction /SCWM/SBUP
  - Program /SCWM/TLAGP_UPLOAD
    - Logical file path used:
  - EWM_STOBIN_UPLOAD_PATH

- EWM_STOBIN_SORT_UPLOAD

  Transactions/programs using this logical filename:

  - Transaction /SCWM/SRTUP
  - Program /SCWM/TLAGPS_UPLOAD

  Logical file path used:

  - EWM_STOBIN_SORT_UPLOAD_PATH

- EWM_MS_RESULT

  Transactions/programs using this logical filename:

  - Transaction /SCWM/MS_RESULT
  - Program /SCWM/R_MS_RESULT_READ

  Parameters and format used in this context:

  - <PARAM_1> = Warehouse number (CHAR4)

  Logical file path used:

  - EWM_GLOBAL_PATH

  Comment:
  The logical filename is fixed and cannot be changed. The logical file contains a physical filename. The logical file path contains a physical path. The validation and alias definition do not apply for this logical file name.

- EWM_ELS_FRML
- EWM_ELS_ST
- EWM_ELS_STE
- EWM_ELS_SEQ
- EWM_ELS_ASS

  Transactions/programs using this logical filename:

  - Transaction /SCWM/ELS_UPLOAD
  - Program /SCWM/ELS_UPLOAD

Logical file path used:

- EWM_GLOBAL_PATH

Comment:

The logical filename is fixed and cannot be changed. The logical file contains a physical filename. The logical file path contains a physical path. The validation and alias definition do not apply for this logical file name.

- EWM_MS_RESULT

  Transactions/programs using this logical filename:

  - Transaction /SCWM/PI_SAMP_UPDATE
  - Program /SCWM/PI_SAMP_UPDATE_RESULT

  Parameters and format used in this context:

  - <PARAM_1> = Warehouse number (CHAR4)

  Logical file path used:

  - EWM_GLOBAL_PATH

  Comment:

  The logical filename is fixed and cannot be changed. The logical file contains a physical filename. The logical file path contains a physical path. The validation and alias definition do not apply for this logical file name.

Activating the Validation of Logical Path and Filenames
Note that this only applies to logical filenames that are not fixed.

These logical paths and filenames are specified in the system for the corresponding programs. For downward compatibility, the validation at runtime is deactivated by default. To activate the validation at runtime, maintain the physical path using the transactions `FILE` (client-independent) and `SF01` (client-specific). To find out which paths are being used by your system, you can activate the corresponding settings in the security audit log.

For more information, see:

- Logical File Names [External]
- Protecting Access to the File System Using Logical Path and File Names [External]
- Security Audit Log [External]



Security for Additional Applications

PTV eServer

The SAP Extended Warehouse Management (SAP EWM) component is delivered with the optional third party software PTV eServer. This software requires an RFC destination on the SAP EWM side. This RFC is described in the Communication Destinations [Page 28] chapter. For any security issues regarding the PTV eServer software, see the third party PTV eServer documentation.

Enterprise Services Security

The following chapters in the SAP NetWeaver Security Guide are relevant for all enterprise services delivered with SAP Extended Warehouse Management:

`http://service.sap.com/securityguide` → *SAP NetWeaver 7.0 Security Guides (Complete)*

- User Administration and Authentification
- Network and Communication Security
- Security Guide for Usage Type PI
- Web Services Security
- Security Guide Communication Interfaces
- Security Guides for Operating System and Database Platforms
- Security Aspects for System Management
- Enabling Application-to-Application Processes: Security Aspects
- Enabling Business-to-Business Processes: Security Aspects

For more information about special security requirements for Web services, see the SAP NetWeaver documentation on SAP Help Portal at **`http://help.sap.com`** → *SAP NetWeaver* → *SAP NetWeaver 7.0 Including EHP2* → *SAP NetWeaver 7.0 Library* → *SAP NetWeaver Library* → *SAP NetWeaver Developer's Guide* → *Fundamentals* → *Using Java* → *Core Development Tasks* → *Providing and Consuming Web Services* → *Web Service Toolset* → *Web Services Security*.

Minimal Installation

Use

In general, you only install and activate the software you really need for your business. Every piece of installed or activated software that you do not use can cause dangerous security flaws (for example, missing Customizing, services that are running but are not monitored, and so on).

Some software needs activated techniques that entail a higher security risk than others. The following is an overview of the minimum activated techniques required to run the specific SAP software components.

Other Security-Relevant Information

Use

You can find other security-relevant information for the following:

- User Frontend [Page 35]
- Data Protection and Privacy [Page 35]

User Frontend

Use

Web Browser as a User Frontend

To use the Web browser as a user frontend, you must first activate Java script (Active Scripting), to ensure a working user interface. This could, however, conflict with your security policy regarding Web services.

Making Browser Settings for Easy Graphics Framework (EGF)

If you work with Microsoft Internet Explorer in the Easy Graphics Framework (EGF), you must have installed Microsoft Internet Explorer version 5 or higher.

For more information about the security settings, see SAP Help Portal at **`http://help.sap.com`** → *SAP Business Suite* → *SAP Supply Chain Management* → *SAP Extended Warehouse Management 7.0 including SAP enhancement package 1* → *SAP Extended Warehouse Management (SAP EWM)* → *Monitoring* → *Easy Graphics Framework.*

RF Device as a User Frontend

To use an RF device as a user frontend, you can use a mobile PC running SAP Front End, or a character-based device using SAP Console. SAP Console is part of the SAP Front End installation. In addition, a third-party Telnet server is necessary. For any security issues regarding the Telnet server software, consult the third-party software documentation.

For more information about SAP Front End, see SAP Service Marketplace at **`http://service.sap.com/instguides`** → *Installation & Upgrade Guides* → *SAP NetWeaver* → *SAP NetWeaver 7.0 (2004s)* → *Installation* → *4 - Installation - Clients* → *SAP Front End Installation Guide*.

Data Protection and Privacy

Use

You can use the RSCRDOMA report with the SAP&DS_USNAM variant to determine all domains that contain person-related data.

You can check which values the variant uses to filter the result.

Activities

You can execute the variant with the following selection criteria to filter the result and display a where-used list for domains in tables:

1. On the *SAP Easy Access* screen, choose *Tools* → *ABAP Workbench* → *Development* → *ABAP Editor*.
2. Enter **`RSCRDOMA`** as the program name.
3. Select the *Variants* subobject and choose *Display*.
4. Enter the **`SAP&DS_USNAM`** variant.
5. Select the *Values* subobject and choose *Display*.

To find the documentation of the RSCRDOMA report, proceed as follows:

1. On the *SAP Easy Access* screen choose *Tools* → *ABAP Workbench* → *Development* → *ABAP Editor*.

2. Enter **RSCRDOMA** as program name.
3. Select the *Source Code* subobject and choose *Display*.



Security-Relevant Logging and Tracing

SAP systems keep a variety of logs for system administration, monitoring, problem solving, and auditing purposes. Audits and logs are important for monitoring the security of your system and to track events, in case of problems.



Auditing and logging for the SAP Extended Warehouse Management (SAP EWM) component is described in detail in the SAP NetWeaver Security Guide. For more information, see Auditing and Logging [External].

Security Audit Log Triggered by Virus Scan Interface (VSI)

The class CL_VSI automatically creates entries in the Security Audit Log for infections and scan errors found, together with the following information:

- Profile
- Profile step allowing the detection of the scanner-group
- Kind of virus found, with internal virus ID of the scan engine, if available
- User name and timestamp

The messages logged are located in the message class VSCAN, using the system log messages BU8 and BU9 (created in SE92). The severities are set to *High* and *Medium*, respectively. The severity of the audit class is set to *Miscellaneous*. For more information, see Customizing for SAP Supply Chain Management under *SAP Web Application Server* → *System Administration* → *Virus Scan Interface.*

Audit Information System (AIS)

Information on auditing and logging for the Audit Information System (AIS) is described in detail in the SAP NetWeaver Security Guide. For more information, see SAP Service Marketplace at **http://service.sap.com** → *NetWeaver 7.0 Security Guides (Complete)* → *SAP NetWeaver 7.0 Security Guides* → *SAP NetWeaver Security Guide* → *Security Aspects for System Management* → *Auditing and Logging* → *The Audit Info System (AIS)*.

SAP EWM

SAP EWM auditing and logging is governed by the transactions and customizing activities listed in the table below.

Auditing and logging in SAP EWM is governed by change documents. Change documents have to be activated in Customizing before they can be used.

When change documents are activated and used in the system, each field in the SCM delivery documents is linked to change documents. The change documents provide information about which fields have been changed and about the old and new values. When you use change documents, you can define that the SCM system creates a log that shows which user has changed data in a delivery document and the specific time at which the change was made.

You can also run reports that retrieve archived documents. The reports are not separate transactions but they are contained in the SCM standard transactions, such as the *Maintain Outbound Delivery Order* transaction (the *Open Advanced Search* pushbutton is used).

The following Customizing activities are relevant for SAP EWM auditing and logging (in SCM Customizing, you can set – per document type of delivery – whether a change document is to be written for each delivery document. You can make these settings for all document categories in SAP EWM. In other words, you can make these settings for all delivery documents in SAP EWM, including posting changes and internal moves).

Customizing Activity	**Path in Customizing for SAP EWM**
Activation of change documents for inbound delivery	*Extended Warehouse Management* → *Goods Receipt Process* → *Inbound Delivery* → *Manual Settings* → *Define Document Types for Inbound Delivery Process* (or: *Extended Warehouse Management* → *Goods Receipt Process* → *Inbound Delivery* → *Use Wizard to Define Document Types for Inbound Delivery Process*). Set the *Change Documents* indicator.
Activation of change documents for expected goods receipt	*Extended Warehouse Management* → *Goods Receipt Process* → *Expected Goods Receipt* → *Manual Settings* → *Define Document Types for Expected Goods Receipt* (or: *Extended Warehouse Management* → *Goods Receipt Process* → *Expected Goods Receipt* → *Use Wizard to Define Document Types for Expected Goods Receipt*). Set the *Change Documents* indicator.
Activation of change documents for outbound delivery	*Extended Warehouse Management* → *Goods Issue Process* → *Outbound Delivery* → *Manual Settings* → *Define Document Types for Outbound Delivery Process* (or: *Extended Warehouse Management* → *Goods Issue Process* → *Outbound Delivery* → *Use Wizard to Define Document Types for Outbound Delivery Process*). Then set the *Change Documents* indicator.
Activation of change documents for posting changes	*Extended Warehouse Management* → *Internal Warehouse Processes* → *Delivery Processing* → *Posting Changes* → *Manual Settings* → *Define Document Types for Posting Change Process* (or: *Extended Warehouse Management* → *Internal Warehouse Processes* → *Delivery Processing* → *Posting Changes* → *Use Wizard to Define Document Types for Posting Change Process*). Set the *Change Documents* indicator.

Activation of change documents for stock transfers	*Extended Warehouse Management* → *Internal Warehouse Processes* → *Delivery Processing* → *Stock Transfers* → *Manual Settings* → *Define Document Types for the Stock Transfer Process* (or: *Extended Warehouse Management* → *Internal Warehouse Processes* → *Delivery Processing* → *Stock Transfers* → *Use Wizard to Define Document Types for the Stock Transfer Process*). Set the *Change Documents* indicator.

The following transactions are relevant for SAP EWM auditing and logging (in each of these transactions, you can use the *Open Advanced Search* button on the screen for that transaction, to retrieve and display archived report data):

Transaction Description	Menu Path in the SAP EWM System
Maintain Inbound Delivery	On the *SAP Easy Access* screen, choose *Extended Warehouse Management* → *Delivery Processing* → *Inbound Delivery* → *Maintain Inbound Delivery*.
Maintain Expected Goods Receipt	On the *SAP Easy Access* screen, choose *Extended Warehouse Management* → *Delivery Processing* → *Inbound Delivery* → *Expected Goods Receipt* → *Maintain Expected Goods Receipt.*
Maintain Outbound Delivery Order	On the *SAP Easy Access* screen, choose *Extended Warehouse Management* → *Outbound Delivery* → *Maintain Expected Goods Receipt*.
Maintain Posting Change	On the *SAP Easy Access* screen, choose *Extended Warehouse Management* → *Delivery Processing* → *Posting Change* → *Maintain Posting Change*.
Maintain Internal Stock Transfer	On the *SAP Easy Access* screen, choose *Extended Warehouse Management* → *Delivery Processing* → *Maintain Internal Stock Transfer*.



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)

Virus Check of Document Attachments

Use

The SAP Extended Warehouse Management (SAP EWM) component provides functionality for checking documents using a virus scanner, before they are uploaded to the SCM system.

Prerequisites

You must have a virus scanner installed and configured correctly.

For more information, see Customizing for SAP EWM under *SAP NetWeaver* → *Application Server* → *System Administration* → *Virus Scan Interface*.

Appendix

Related Security Guides

For more information about the security of SAP applications, see SAP Service Marketplace at **`http://service.sap.com/security`**.

For more information about security guides of SAP applications, see SAP Service Marketplace at **`http://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 SAP Service Marketplace (http://service.sap.com)**
Master Guides, Installation Guides, Upgrade Guides, Solution Management Guides	**`http://service.sap.com/instguides`** **`http://service.sap.com/ibc`**
Related SAP Notes	**`http://service.sap.com/notes`**
Released platforms	**`http://service.sap.com/platforms`**
Network security	**`http://service.sap.com/securityguide`**
Technical infrastructure	**`http://service.sap.com/installnw70`**
SAP Solution Manager	**`http://service.sap.com/solutionmanager`**
SAP Supply Chain Management	**`http://service.sap.com/scm`**